

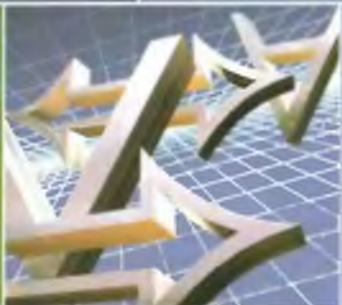
Высшее профессиональное образование

В. И. Игошин

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

2-е издание

Учебное пособие



Педагогические
специальности

В. И. ИГОШИН

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

Допущено

*Министерством образования Российской Федерации
в качестве учебного пособия для студентов высших учебных заведений,
обучающихся по специальности 050201 «Математика»*

2-е издание, стереотипное



Москва
Издательский центр «Академия»
2008

УДК 510.6(075.8)

ББК 22.12я73

И269



Рецензенты:

декан факультета «Прикладная математика» Московского государственного
открытого университета, д-р физ.-мат. наук, проф. *В.Д. Кулиев*;
д-р физ.-мат. наук, проф. *Д.А. Бредихин*

Игошин В.И.

И269 Математическая логика и теория алгоритмов : учеб. пособие для студ. высш. учеб. заведений / В. И. Игошин. — 2-е изд., стер. — М. : Издательский центр «Академия», 2008. — 448 с.
ISBN 978-5-7695-4593-1

Предлагаемое учебное пособие составляет основу комплекта по курсу математической логики и теории алгоритмов, в который также входит сборник задач (*Игошин В.И.* Задачи и упражнения по математической логике и теории алгоритмов). Подробно изложены основы теории, показаны направления проникновения логики в основания алгебры, анализа, геометрии, привлечен материал школьного курса математики для его логического анализа, охарактеризованы взаимосвязи математической логики с компьютерами, информатикой, системами искусственного интеллекта.

Для студентов университетов, технических и педагогических вузов, обучающихся по специальностям «Математика», «Прикладная математика».

УДК 510.6(075.8)

ББК 22.12я73

*Оригинал-макет данного издания является собственностью
Издательского центра «Академия», и его воспроизведение любым способом
без согласия правообладателя запрещается*

ISBN 978-5-7695-4593-1

© Игошин В.И., 2004

© Издательский центр «Академия», 2004

Предисловие

Логика образует такой пласт общечеловеческой культуры, без освоения которого в настоящее время не может состояться ни одна мыслящая личность. Основы логической культуры закладываются в школе и в первую очередь на уроках математики, ибо, как точно подметил еще Л. Н. Толстой, «математика имеет задачей не обучение исчислению, но обучение приемам человеческой мысли при исчислении»¹.

Математическая логика — вершина развития логики, достигнутая ею в XX в. Органично соединив в себе традиционную логику, восходящую к Аристотелю, и методы современной математики, она получила столь глубокие и поразительные результаты, не принимать в расчет которые стало просто невозможно не только тем, кто изучает, преподает и творит математику, но и всем тем, для кого методы рассуждений, обоснований и доказательств являются главными методами деятельности. Результаты, полученные с помощью математической логики, легли в основу проектирования и создания электронно-вычислительных машин (компьютеров) и программного обеспечения к ним, нашли широчайшее применение в областях информатики и систем искусственного интеллекта.

Настоящая книга предназначена для тех, кто изучает математическую логику в высших учебных заведениях. Автор знакомит будущих специалистов с основными понятиями и методами математической логики, показывает взаимосвязи математической логики с математической наукой, со школьным курсом математики, с современными ЭВМ.

В гл. I дано подробное изложение алгебры (логики) высказываний, так как важно, чтобы именно на начальном этапе знакомства с предметом у студента сформировалась требуемая система понятий, составляющих фундамент математической логики. В гл. II рассматриваются, возникшие из алгебры логики булевы функции, которые оказались действенным математическим инструментом для конструирования функциональных и релейно-контактных (переключаемых) схем — элементов современных ЭВМ. В гл. III происходит знакомство с иным подходом к алгебре высказываний: она строится как аксиоматическая теория на базе трех схем аксиом и одного правила вывода. Основная цель гл. IV, в которой

¹ Толстой Л. Н. Педагогические сочинения. — М., 1989. С. 244.

излагается логика предикатов, — привить студентам навыки использования квантора общности и квантора существования, правильного их понимания и умения оперировать выражениями (формулами) с кванторами. В вопросах применения логики предикатов значительное внимание уделяется записям на ее языке различных предложений, строению математических теорем и методам их доказательств. В гл. V рассмотрен аксиоматический метод в математике, изложены его логические основы. На неформальном (содержательном) уровне показано, как математическая логика вторгается в различные разделы математической науки, образуя их фундаментальные аксиоматические основы.

В гл. VI изложение математической логики поднимается на новый качественный уровень: математические теории начинают изучаться с формальной точки зрения. Сначала изучаются свойства формализованного исчисления предикатов: доказываются теоремы Гёделя о существовании модели, о полноте и адекватности этого исчисления, теорема компактности, теорема Лёвенгейма-Сколема. Затем дается обзор формализаций теории множеств, числовых систем, геометрии, математического анализа. Гл. VII посвящена основам теории алгоритмов. Рассматриваются три формализации этого понятия (машины Тьюринга, рекурсивные функции, нормальные алгоритмы Маркова), устанавливается их равносильность. Рассматриваются неразрешимые алгоритмические проблемы. Доказывается теорема Гёделя о неполноте формальной арифметики. Наконец в гл. VIII дан обзор применений математической логики в сферах программного обеспечения компьютеров, информатики и искусственного интеллекта.

Данное пособие задумано в комплекте со сборником задач: *Игошин В. И.* Задачи и упражнения по математической логике и теории алгоритмов. — М.: Изд. центр «Академия», 2004. По ходу изложения теоретического материала автор прибегает к многочисленным ссылкам на конкретные примеры решения тех или иных задач из данного сборника, используя краткое его название — «Задачник». Например, усвоение теоретического материала гл. I закрепляется решением задач § 1 — 3 Задачника, гл. II является теоретической основой для решения задач § 4 — 7 Задачника. После изучения гл. III рекомендуются задачи § 8 Задачника. В процессе изучения гл. IV решаются задачи § 9 — 11, а для закрепления материала гл. VII и гл. VIII предназначены задачи § 12 — 14 Задачника.

Знаки $\Leftrightarrow$ и $\Rightarrow$ почти всегда используются для сокращенной записи оборотов «тогда и только тогда» и «если ..., то ...» соответственно. Исключения составляют § 18 и 19 книги, где первый знак ($\Leftrightarrow$) используется для обозначения равносильности предикатов, а второй ($\Rightarrow$) — для следования предикатов, а также § 32 и 34, где знак $\Rightarrow$ обозначает переход от одного слова к другому в результате применения соответствующего алгоритма. Знак $\equiv$ обо-

значает графическое совпадение (одинаковость) формул (логики высказываний или логики предикатов). Для множеств комплексных, действительных, рациональных, целых и натуральных чисел используются стандартные обозначения: C , R , Q , Z и N соответственно. Конец доказательства отмечается значком $\square$.

Составляющими элементами каждого параграфа являются теоремы, леммы, определения, следствия, замечания, примеры, которым присвоена двойная нумерация для их идентификации: на первом месте указан номер параграфа в книге, на втором — порядковый номер данного элемента в этом параграфе.

В конце книги приведен обширный список рекомендуемой литературы по разделам математики, имеющим отношение к разным системам логического исчисления: числовым и алгебраическим, к смежным вопросам алгебры, к теории алгоритмов и др. Выделена литература по математической логике и информатике и искусственному интеллекту. Сборники задач и книги, рекомендуемые школьникам, также составляют отдельные подразделы списка литературы.

В работе над данной книгой, как и в работе над сборником задач, автором учтен опыт его прежних публикаций по теме, в частности сборника задач (1986) и учебника (1991) по математической логике и теории алгоритмов.

Автор вполне отдаст себе отчет о трудности создания учебного пособия, полностью отвечающего требованиям сегодняшнего дня, однако выражает надежду, что его новые работы, рассчитанные на тех, кто начинает изучать основы математической логики и теории алгоритмов, будут востребованы и оценены должным образом в учебных заведениях различных профилей и уровней.

В. Игошин

МАТЕМАТИЧЕСКАЯ ЛОГИКА В СИСТЕМЕ СОВРЕМЕННОГО ОБРАЗОВАНИЯ

Предварим изучение математической логики кратким введением, в котором попытаемся осознать роль и место логики в мышлении, в науке, в математике и в обучении.

Логика и интуиция. Мыслительная деятельность человека представляет собой сложный и многогранный процесс, происходящий как на сознательном, так и на бессознательном (подсознательном) уровнях. Это высшая ступень человеческого познания, способность к адекватному отражению предметов и явлений действительности, т.е. к нахождению истины.

Логика и интуиция — два противоположных и неразрывно связанных между собой свойства человеческого мышления. Логическое (дедуктивное) мышление отличается тем, что оно от истинных посылок всегда приводит к истинному заключению, не опираясь при этом на опыт, интуицию и другие внешние факторы. Интуиция (от лат. *intuitio* — «пристальное всматривание») представляет собой способность постижения истины путем прямого ее усмотрения без обоснования с помощью логически строгого доказательства. Таким образом, интуиция является своего рода антиподом, противовесом логики и строгости. Логическая часть мыслительного процесса протекает на уровне сознания, интуитивная — на подсознательном уровне.

Развитие науки и особенно математики немыслимо без интуиции. Различают два вида интуиции в научном познании¹: интуицию-суждение и интуицию-догадку. *Интуиция-суждение* (или *философская интуиция-суждение*) характеризуется тем, что в этом случае прямое усмотрение истины, объективной связи вещей осуществляется не просто без логически строгого доказательства, но такого доказательства для данной истины не существует и не может существовать в принципе. Интуиция-суждение осуществляется как единый (единовременный) синтетический целостный акт обобщающего характера. Именно такой характер логически недоказуемых утверждений носят рассматриваемые в теории алгоритмов тезисы Тьюринга, Чёрча и Маркова (см. § 31 — 36). Примером применения интуиции-суждения является установление истинно-

¹ Фейнберг Е.Л. Кибернетика, логика, искусство. — М., 1981.

сти или ложности положений, помещаемых в основание той или иной математической теории, которая затем будет развиваться строгими формально-логическими методами.

Интуиция-догадка, называемая также *психоэвристической интуицией*, характеризуется тем, что происходит прямое внелогическое усмотрение такой истины, такого факта, который впоследствии, по прошествии определенного времени, будет обоснован и доказан строго логическим путем. Такое суждение в значительной мере протекает бессознательно или подсознательно в короткие промежутки времени и проявляется как «озарение», «прозрение». Факт, усмотренный в результате психоэвристической интуиции-догадки, в рамках определенной формально-логической системы может быть логически сведен к некоторым исходным основным положениям, принятым за аксиомы или постулаты. При этом последующее строго логическое доказательство интуитивно усмотренного факта происходит через такой промежуток времени, который абсолютно несопоставим по продолжительности с актом «озарения». Для этого могут понадобиться часы, дни и даже годы.

Вопрос о противопоставлении логического и интуитивного (интеллектуального и чувственного) давно отнесен историей развития процесса познания к проблеме взаимодействия этих двух ипостасей человеческого сознания в ходе данного процесса. Для познания мира — и физического, и духовного — необходимы два совершенно разных метода: с одной стороны, логический, строго доказательный, а с другой — интуитивный, основанный на непосредственном синтетическом суждении, не опирающемся на доказательство. Гипертрофия (преувеличение) роли как строгой логики, так и интуиции — это крайности. «Обе эти крайности, — справедливо считает Я. Стюарт¹, — бьют мимо цели: вся сила математики — в разумном сочетании интуиции и строгости. Контролируемый дух и вдохновенная логика!»

Завершим мысль словами выдающегося математика XX в. А. Пуанкаре: «Таким образом, логика и интуиция играют каждая свою необходимую роль. Обе они неизбежны. Логика, которая одна может дать достоверность, есть орудие доказательства; интуиция есть орудие изобретательства»².

Логика традиционная и математическая логика. Термин «логика» — наука о способах доказательств и опровержений — происходит от греч. λογος (логос), что означает «слово», «понятие», «смысл». Понятие «традиционная или формальная логика» характеризует берущую свое начало от Аристотеля науку, изучающую формы и законы мышления, а также методы, с помощью которых люди в действительности делают выводы, устанавливают связь логических форм с языком. Появление логических форм и категорий, формирование законов мыш-

¹ Стюарт Я. Концепции современной математики. — Минск, 1980. С. 14.

² Пуанкаре А. О науке. — М., 1983. С. 167.

ления — это результат общественной практики. Именно длительная практическая деятельность человека в процессе познания окружающей действительности, миллиарды раз приводя его сознание к повторению одних и тех же логических фигур, откристаллизовала эти фигуры в законы логики. Таким образом, логика представляет собой определенный способ отражения действительности. Логика изучает то общее, что связывает мысли в их движении к познанию истины. Она есть наука о законах и формах правильного мышления. Она изучает формы рассуждений, отвлекаясь от их конкретного содержания; устанавливает, что из чего следует; ищет ответ на вопрос о направлении рассуждений. Специфика логики состоит в том, что изучение и познание объективного мира природы и субъективного мира переживаний и чувств возможно вести эффективными средствами абстрактного мышления человека.

Математическая логика, называемая также *символической* или *теоретической логикой*, выросла из логики традиционной, но составила значительное ее расширение. С одной стороны, эта наука применила математические методы для изучения общих структур (форм) правильного мышления и тем самым оформилась как раздел математики, с другой — математическая логика сделала предмет своего изучения процесс доказательства математических теорем и сами математические теории. Математическая логика явилась, таким образом, инструментом для исследований в области оснований математики. Данный раздел математической логики получил название «теория доказательств» или «метаматематика».

Ни одна из этих двух логик не может в полной мере включать другую как частный случай, но они тесно взаимосвязаны между собой. Математическая логика, являясь более общей и более абстрактной, чем традиционная формальная логика, в то же время является и более конкретной, так как она имеет более широкое применение, дает возможность решать множество конкретных практических задач, не разрешимых средствами традиционной формальной логики. Аппарат исчислений и формальных систем в математической логике гораздо более совершенен, нежели аппарат традиционной логики. Поэтому он может применяться к решению таких сложных задач, которые недоступны для классической логики. Математическая логика способствует более глубокому пониманию логики традиционной, ее сохранению и поднятию на более высокую ступень. Благодаря математической логике логика традиционная достигла определенного уровня совершенства, так как появилась новая возможность использования математики не только по форме, но и по существу.

Немного истории. Основоположителем логики как науки является древнегреческий философ и ученый Аристотель (384 — 322 гг. до н. э.). Он впервые разработал теорию дедукции, т.е. теорию логического вывода. Именно он обратил внимание на то, что в рассуждениях

мы из одних утверждений выводим другие, исходя не из конкретного содержания утверждений, а из определенной взаимосвязи между их формами и структурами.

Древнегреческий математик Евклид (330 — 275 гг. до н. э.) впервые предпринял попытку упорядочить накопившиеся к тому времени обширные сведения по геометрии, взглянув на эту науку с общелогических позиций. Он положил начало осознанию геометрии как аксиоматической теории, а всей математики — как совокупности аксиоматических теорий, впервые на практике реализовав восходящие к Платону и Аристотелю идеи аксиоматической организации всякого научного знания.

На протяжении многих веков различными философами и целыми философскими школами дополнялась, усвершенствовалась и изменялась логика Аристотеля. Это был первый (доматематический) этап развития формальной логики. Второй этап связан с применением в логике математических методов, начало которому положил немецкий философ и математик Г. Лейбниц (1646 — 1716). Он пытался построить универсальный язык, с помощью которого можно было бы решать споры между людьми, а затем и вообще все «идеи заменить вычислениями».

Важный период становления математической логики начинается с появления работ английского математика и логика Джорджа Буля (1815 — 1864) «Математический анализ логики» (1847) и «Исследование законов мышления» (1854). Он применил к логике методы современной ему алгебры — язык символов и формул, составление и решение уравнений. Им была создана своеобразная алгебра — алгебра логики. В этот период она оформилась как алгебра высказываний и была значительно развита в работах шотландского логика А. де Моргана (1806 — 1871), английского логика У. Джевонса (1835 — 1882), американского логика Ч. Пирса (1839 — 1914), немецкого алгебраиста и логика Э. Шрёдера (1841 — 1902), русского математика, астронома и логика П. С. Порецкого (1846 — 1907). Создание алгебры логики явилось заключительным звеном в развитии формальной логики: алгебра логики поставила и решила в самом общем виде те задачи, которые рассматривались в аристотелевой логике. Формальная логика в результате использования в ней развитого символического языка окончательно оформилась как логика символическая.

Значительным толчком к новому периоду развития математической логики послужило создание в первой половине XIX в. великим русским математиком Н. И. Лобачевским (1792 — 1856) и независимо от него венгерским математиком Я. Бояи (1802 — 1860) неевклидовой геометрии. Кроме того, создание анализа бесконечно малых привело к необходимости обоснования понятия числа как фундаментального понятия всей математики. Довершали картину парадоксы (антиномии), обнаруженные в конце XIX в. в те-

ории множеств: они отчетливо показали, что трудности обоснования математики являются трудностями логического и методологического характера. Таким образом, перед математической логикой встали задачи, которые перед логикой Аристотеля не возникали: она должна была исследовать основания математической науки, исследовать математику как совокупность аксиоматических теорий, исследовать аксиоматический метод построения математических теорий. В ходе развития математической логики сформировались три направления обоснования математики, создатели которых по-разному пытались преодолеть возникшие в математике трудности. В каждом из них были получены фундаментальные результаты, оказавшие влияние на развитие не только математической логики, но и всей математики.

Основоположником одного из направлений — *логицизма* — явился немецкий математик и логик Г. Фреге (1848 — 1925). Он стремился всю математику обосновать через логику, применил аппарат математической логики для обоснования арифметики, построив первую формальную логическую систему, включавшую значительную часть арифметики. Кроме того, им и независимо от него Ч. Пирсом были введены в язык логики предикаты, предметные переменные и кванторы, что дало возможность применить этот язык к вопросам обоснования математики. Задачу аксиоматического построения арифметики, геометрии и математического анализа ставил перед собой итальянский математик Дж. Пеано (1858 — 1932). Сведение чистой математики к логике продолжили в своем трехтомном труде «Основания математики» (1910 — 1913) английские математики Б. Рассел (1872 — 1970) и А. Уайтхед (1861 — 1947). Данное направление не увенчалось полным успехом (в частности, оказалось невозможным вывести из чисто логических аксиом существование бесконечного множества), однако был создан богатый логический аппарат, без которого математическая логика не смогла бы оформиться как полноценная математическая дисциплина.

Немецкий математик Д. Гильберт (1862 — 1943) предложил свой путь преодоления трудностей в основаниях математики, базирующийся на применении аксиоматического метода, с помощью которого все математические утверждения записываются в виде логических формул, некоторые из которых выделяются в качестве аксиом, а остальные логически из них выводятся. Это направление получило название *формализм*. Открытие в 1930 — 1931 гг. австрийским математиком К. Гёделем (1906 — 1978) неполноты формализованной арифметики показало ограниченность гильбертовской программы обоснования математики. Тем не менее работы Гильберта и его последователей привели к глубокой разработке аксиоматического метода и окончательному осознанию его фундаментальной роли в математике.

Представители направления, возникшего в начале XX в. благодаря трудам голландского математика Л. Брауэра (1881—1966) и получившего название *интуиционизм*, предложили отказаться от рассмотрения бесконечных множеств как завершённых совокупностей, а также от закона исключённого третьего. Ими признавались только такие математические доказательства, которые конструктивно строили тот или иной объект, и оспаривались чистые доказательства существования. Они построили специфическую математику, имеющую интересные особенности, ещё раз подчеркнули различие между конструктивным и неконструктивным в математике.

XX в. — время бурного развития математической логики, формирования многих ее новых разделов: построены различные аксиоматические теории множеств; на базе математической логики сформирована теория алгоритмов, с помощью которой были выработаны несколько формализаций понятия алгоритма. Теория алгоритмов получила такое развитие, что ее методы стали проникать в другие разделы математической логики и в смежные математические дисциплины. В другие разделы математики стала проникать и сама математическая логика. Примером может быть теория моделей, возникающая на стыке современной алгебры и логики. Следует отметить и нестандартный подход к математическому анализу. Были созданы многочисленные новые неклассические логические системы. Немалый вклад в развитие математической логики внесли и советские математики Н. А. Васильев, И. И. Жегалкин, А. Н. Колмогоров, П. С. Новиков, А. А. Марков, А. И. Мальцев, С. А. Яновская. Кроме того, XX в. — это период начала глубокого проникновения идей и методов математической логики в технику, прежде всего в процесс конструирования и создания ЭВМ, в программирование, кибернетику, вычислительную математику, структурную лингвистику.

Математическая логика — логика или математика? Вопрос о соотношении логики и математики в математической логике издавна интересовал философов, близких к математике, и математиков, близких к философии. Является ли математическая логика в традиционном (философском) понимании логикой, т. е. изучает ли она формы мышления и методы, с помощью которых люди обычно делают выводы, или же она является чисто математической дисциплиной со своим абстрактным аппаратом, не имеющим ничего общего с реальным процессом мышления? Подобные вопросы возникли потому, что посредством математической логики математика впервые проникла в гуманитарную область знаний, в ее святая святых — сферу человеческого мышления, ранее подвластную лишь философии. Это проникновение было столь стремительным и успешным, что многие философы и мыслители сразу не осознали его преимуществ.

Доказанная в 1931 г. австрийским математиком и логиком К. Гёделем (1906—1978) теорема о неполноте формальной арифметики

ки с большой силой показала, что математическая логика — это прежде всего логика и что к человеческому мышлению эта наука имеет самое непосредственное отношение. Пришло понимание того, что совершенно безнадежно рассчитывать на возможность создания полной и непротиворечивой системы аксиом для арифметики или какой-либо теории, содержащей арифметику. (Полнота системы аксиом означает, что, исходя из нее, можно вывести все истинные предложения данной науки.) Из этого следует, что аксиоматический подход к арифметике натуральных чисел не в состоянии охватить всю область истинных арифметических утверждений. Отсюда также вытекает, что то, что обычно интуитивно понимается под процессом математического доказательства, не сводится к использованию аксиоматического метода и законов традиционной и математической логики. Этот самоограничительный закон логики удалось установить только с помощью математической логики, что является убедительнейшим доказательством непосредственного отношения математической логики к мышлению и законам, по которым оно работает.

Известный российский логик П. С. Порецкий точно подметил, что математическая логика по предмету своему есть логика, а по методу — математика.

Математическая логика в обучении математике. Логика и математика в процессе обучения математике взаимодействуют неизбежно. Важно, чтобы это дидактическое взаимодействие не было стихийным, а сознательно организовывалось и направлялось педагогом. В нем можно выделить два аспекта. Во-первых, при обучении математике логика выступает как инструмент педагогики математики, т.е. как инструмент изучения математики. Для педагогики математики логика — это особый инструмент, причем это не метод, не средство и не форма обучения, а именно инструмент. Во-вторых, логика (как своеобразная часть математики) предстает как предмет педагогики математики, т.е. как объект, изучаемый в рамках математики и с помощью математики. Но и в этом своем качестве логика выступает как педагогика математики, ибо изучение логики с помощью математического материала в конечном итоге способствует более осознанному и глубокому изучению самой математики.

Чтобы сделать логику действенным инструментом процесса обучения математике, необходимо соблюдать ряд принципов — тех общих положений, связанных с логикой, которые имеют фундаментальное значение для методики обучения математике. Эти принципы отражают основные направления проникновения логики в методику, и их нарушение или несоблюдение их в процессе обучения математике приведет в итоге к искаженному видению обучаемым как общей картины математики, так и отдельных ее деталей.

1. Принцип обучения строению (структуре) математических утверждений. Здесь в первую очередь необходимо научиться видеть логическую структуру математического утверждения, будь то определение или теорема, отчетливо видеть, где и какие логические связки участвуют в формулировке. При этом, если это определение понятия, то важно установить, какого оно типа — через ближайший род и видовое отличие, индуктивное, рекуррентное, генетическое или аксиоматическое. Если это теорема, то необходимо четко уяснить, что в ней дано и что требуется доказать, каковы структура условий и структура заключения. Важно также понимание сути необходимых и достаточных условий, прямой и обратной теорем и их различных видов. Кроме того, необходимо научиться определять, какие утверждения равносильны каким, т.е. научиться преобразовывать структуру математического утверждения равносильным образом. Чем больше усвоено логических равносильностей, тем выше логическая культура учителя.

2. Принцип обучения понятию доказательства математической теоремы. В этом случае важно уяснить, что доказательство теоремы — это последовательность (цепочка) утверждений, каждое из которых есть либо условие теоремы, либо аксиома, либо получено из двух предыдущих утверждений последовательности по правилу вывода: из утверждений A и $A \rightarrow B$ следует утверждение B . Построив такую цепочку, мы доказываем, что из A выводится B , в результате чего делаем вывод, что справедлива теорема $A \rightarrow B$. Обоснованием этому переходу служит логическая теорема о дедукции. Всякий раз при доказательстве теоремы нужно стремиться к тому, чтобы цепочка последовательных утверждений вырисовывалась в сознании учащегося как можно более отчетливо.

3. Принцип обучения методам доказательства математических теорем. В первую очередь необходимо, научиться методам построения цепочки утверждений $A = A_0, A_1, \dots, A_n = B$ для доказательства теоремы $A \rightarrow B$. Синтетический (или прямой) метод — построение цепочки в прямом направлении, т.е. от A к B . Аналитический метод (или метод восходящего анализа) — построение цепочки в обратном направлении, т.е. от B к A . Далее необходимо уяснить, что для доказательства теоремы $A \rightarrow B$ достаточно доказать теорему $\neg B \rightarrow \neg A$ или $(A \wedge \neg B) \rightarrow \neg A$ или $(A \wedge \neg B) \rightarrow B$ (варианты метода доказательства от противного), вместо теоремы A достаточно доказать теорему $(\neg A \rightarrow (B \wedge \neg B)) \rightarrow A$ (метод приведения к абсурду), а вместо теоремы $A \rightarrow C$ — две теоремы $A \rightarrow B$ и $B \rightarrow C$ (метод цепного заключения) и т.д.

4. Принцип обучения строению математических теорий. Имеется в виду уяснение сути аксиоматического метода при построении математической теории и при ее преподавании, а также уяснение сути первоначальных (неопределяемых) понятий теории, ее аксиом и теорем, вплоть до метатеории (свойств этой теории) —

непротиворечивости, полноты, категоричности, независимости системы аксиом. Важно также знание аксиоматических теорий, лежащих в основе школьных математических курсов: аксиоматических построений геометрии на основе систем аксиом Евклида, Гильберта, Вейля и т.д.; аксиоматической теории числовых систем как основания школьного курса алгебры и начал анализа.

Математическая логика помогает обосновать и облегчает применение указанных логических принципов. Они должны органично войти в сознание всякого преподающего и изучающего математику, так как при несоблюдении данных принципов при обучении математике изучаемый предмет рискует утратить те качества и черты, которые, собственно, и выделяют его из системы прочих наук.

Математическая логика и современные ЭВМ. Широчайшее распространение компьютеров, проникших буквально во все сферы жизни, связано с насущной проблемой развития и поддержания массовой компьютерной культуры, начиная с самого раннего возраста. Важно, чтобы росло понимание возможностей компьютера и умение взаимодействия с ним, чтобы молодые люди развивали свои способности и умение мыслить алгоритмически, т.е. отчетливо и однозначно могли определять последовательность своих действий при решении той или иной задачи. Развитие мышления в области математических наук всегда было в наибольшей степени алгоритмичным по сравнению с прочими науками, тем не менее всеобщая компьютеризация еще более отчетливо выявила эту сторону математического мышления. Математическая логика, в частности ее раздел, посвященный теории алгоритмов, являются важнейшими составляющими теоретических основ алгоритмического мышления. Не менее тесная связь методов математической логики и современных компьютеров прослеживается по следующим двум направлениям. Эти методы используются как при физическом конструировании и создании компьютеров (алгебра высказываний и булевы функции — математический аппарат для конструирования переключательных и функциональных схем, составляющих элементную базу компьютеров), так и при создании математического обеспечения к ним. В основе многочисленных языков программирования лежат теория алгоритмов, теория формальных систем, логика предикатов. Например, название языка ПРОЛОГ означает сокращение от слов «ПРОграммирование ЛОГическое». Кроме того, синтез логики и компьютеров привел к возникновению баз данных и экспертных систем, что явилось важнейшим этапом на пути к созданию искусственного интеллекта — машинной модели человеческого разума.

Понимание всех этих взаимосвязей неотделимо от современного высшего математического, технического и педагогического образования.

АЛГЕБРА ВЫСКАЗЫВАНИЙ

Высказывание — первый важнейший объект изучения математической логики. Алгебра высказываний изучает способы построения высказываний из уже имеющихся высказываний, закономерности таких способов сочетания высказываний. Алгебра высказываний является фундаментом математической логики.

§ 1. Высказывания и операции над ними

Понятие высказывания. Предметом исследования алгебры высказываний являются высказывания. Но алгебра высказываний не ставит целью их всестороннее изучение. Из многочисленных свойств высказывания алгебре высказываний интересует лишь одно: истинно оно или ложно. Именно это и является определяющим свойством высказывания. Итак, под *высказыванием* понимается такое предложение, которое либо истинно, либо ложно. Высказывание не может быть одновременно и истинным, и ложным.

В дальнейшем будем считать, что имеется первоначальная совокупность некоторых простейших высказываний, называемых элементарными или исходными, о каждом из которых точно известно, истинно оно или ложно. Причем в этой совокупности имеются как истинные высказывания, так и ложные. Примеры предложений, являющихся высказываниями, и предложений, таковыми не являющимися, приведены в Задачнике¹, № 1.1.

Договоримся обозначать конкретные высказывания начальными заглавными буквами латинского алфавита $A, B, C, D, \dots$ или теми же буквами с индексами внизу.

Приведем примеры высказываний, которые будут использоваться в дальнейшем:

- A_1 : «Москва — столица России»;
- A_2 : «Саратов находится на берегу Невы»;
- A_3 : «Все люди смертны»;
- A_4 : «Сократ — человек»;
- A_5 : « $7 < 4$ »;

¹ Игошин В. И. Задачи и упражнения по математической логике и теории алгоритмов. — М., 2004.

A_6 : «Волга впадает в Каспийское море»;

A_7 : «А. С. Пушкин — великий русский математик»;

A_8 : «Снег белый».

Обозначив истинное высказывание символом 1, а ложное — 0, введем функцию λ , заданную на совокупности всех высказываний и принимающую значения в двухэлементном множестве $\{0, 1\}$, по следующему правилу:

$$\lambda(P) = \begin{cases} 1, & \text{если высказывание } P \text{ истинно,} \\ 0, & \text{если высказывание } P \text{ ложно.} \end{cases}$$

Функция λ называется *функцией истинности*, а значение $\lambda(P)$ — *логическим значением* или *значением истинности* высказывания P . Для приведенных высказываний имеем логические значения $\lambda(A_1) = 1$, $\lambda(A_2) = 0$, $\lambda(A_3) = 1$, $\lambda(A_4) = 1$, $\lambda(A_5) = 0$, $\lambda(A_6) = 1$, $\lambda(A_7) = 0$, $\lambda(A_8) = 1$.

Отметим, что в литературе имеются следующие обозначения для истинных высказываний: 1, И, t (от англ. *true* — истинный) и для ложных высказываний: 0, Л, f (от англ. *false* — ложный). Из этих обозначений будем использовать 1 и 0. Это обусловлено рядом причин. Во-первых, таблицы истинности для формул алгебры высказываний принимают более лаконичный и стандартизированный вид, так как в этом случае наборы значений пропозициональных переменных (см. § 2) можно расположить в порядке возрастания чисел, которые этими наборами закодированы в двоичной системе счисления. Например, для случая трех пропозициональных переменных X, Y, Z набор значений этих переменных 000 означает двоичную запись десятичного числа 0, набор 001 — двоичную запись десятичного числа 1, набор 010 — двоичную запись десятичного числа 2, 011 — 3, 100 — 4, 101 — 5, 110 — 6, 111 — 7. Во-вторых, более удобный и математически строгий вид принимают многие формулы и алгоритмы алгебры высказываний. В-третьих, обозначение 0 и 1 принято и более целесообразно в приложениях математической логики к компьютерам и информатике.

Из элементарных высказываний с помощью операций над высказываниями или логических связей строят сложные высказывания. Перейдем к точному описанию таких построений.

Отрицание высказывания. *Определение 1.1.*¹ *Отрицанием* высказывания P называется новое высказывание, обозначаемое $\neg P$ (читается: «не P » или «не верно, что P »), которое истинно, если высказывание P ложно, и ложно, если высказывание P истинно. Другими словами, логическое значение высказывания $\neg P$ связа-

¹ В книге принята нумерация всех элементов по параграфам. Так, в обозначении «Определение 1.1» первая цифра указывает на номер параграфа, в котором находится данный элемент, вторая — на порядковый номер элемента в данном параграфе.

но с логическим значением высказывания P , как указано в следующей таблице, называемой *таблицей истинности операции отрицания*:

$\lambda(P)$	$\lambda(\neg P)$
0	1
1	0

Здесь может возникнуть вопрос, почему приписывание истинности или ложности высказыванию $\neg P$ осуществляется именно на основании приведенной таблицы. Конечно, можно ответить, что об определениях не спорят. Но ведь мы желаем построить математическую теорию (алгебру высказываний), которая в какой-то мере отражала бы реально существующий в природе человеческого мышления процесс построения составных высказываний из элементарных и имела бы реальный смысл. Затем мы должны будем развить нашу математическую теорию, а полученные выводы применить в практике мышления и при этом не войти в противоречие с общеизвестными законами мышления. Определение отрицания с помощью приведенной таблицы (как, впрочем, и других логических связей с помощью соответствующих таблиц, о чем речь пойдет далее) появилось как результат длительного опыта, и оно полностью оправдало себя на практике.

Пример 1.2. Применим операцию отрицания к высказыванию A_6 : «Волга впадает в Каспийское море». Данное отрицание можно читать так: «Неверно, что A_6 » т.е. «Неверно, что Волга впадает в Каспийское море». Или же частицу «не» переносят на такое место (чаще всего ставят перед сказуемым), чтобы получилось правильно составленное предложение: «Волга не впадает в Каспийское море». Таблица из определения 1.1 дает для данного высказывания следующее логическое значение: $\lambda(\neg A_6) = \neg \lambda(A_6) = \neg 1 = 0$, т.е. высказывание $\neg A_6$ ложно. Ложность высказывания $\neg A_6$ обусловлена только истинностью исходного высказывания A_6 и определением 1.1, но никак не соображениями смысла (содержания) высказывания $\neg A_6$. Другое дело, что само определение 1.1 потому и имеет такую формулировку, что оно правильно (или, как говорят, адекватно) отражает факты, известные нам из практики.

Конъюнкция двух высказываний. **Определение 1.3.** Конъюнкцией двух высказываний P и Q называется новое высказывание, обозначаемое $P \wedge Q$ или $P \& Q$ (читается: « P и Q »), которое истинно лишь в единственном случае, когда истинны оба исходных высказывания P и Q , и ложно во всех остальных случаях. Другими словами, логическое значение высказывания $P \wedge Q$ связано с логическими значениями высказываний P и Q , как указано в следующей таблице, называемой *таблицей истинности операции конъюнкции*:

$\lambda(P)$	$\lambda(Q)$	$\lambda(P \wedge Q)$
0	0	0
0	1	0
1	0	0
1	1	1

Практика полностью подтвердила, что именно такое распределение значений истинности наиболее соответствует тому смыслу, который придается в процессе мыслительной деятельности связующему союзу «и».

Пример 1.4. Применим операцию конъюнкции к высказываниям A_2 и A_3 . Получим высказывание $A_2 \wedge A_3$: «Саратов находится на берегу Невы, и все люди смертны». Конечно, мы не воспринимаем это высказывание как истинное из-за первой, ложной, его части. К выводу о ложности полученного высказывания также приходим, исходя из логических значений исходных высказываний A_2 и A_3 и определения 1.3 конъюнкции на основании приведенной там таблицы. В самом деле, $\lambda(A_2 \wedge A_3) = \lambda(A_2) \wedge \lambda(A_3) = 0 \wedge 1 = 0$.

Дизъюнкция двух высказываний. Определение 1.5. Дизъюнкцией двух высказываний P и Q называется новое высказывание, обозначаемое $P \vee Q$ (читается « P или Q »), которое истинно в тех случаях, когда хотя бы одно из высказываний P или Q истинно, и ложно в единственном случае, когда оба высказывания P и Q ложны. Другими словами, $P \vee Q$ — такое высказывание, логическое значение которого связано с логическими значениями исходных высказываний P и Q так, как указано в следующей таблице, называемой *таблицей истинности операции дизъюнкции*:

$\lambda(P)$	$\lambda(Q)$	$\lambda(P \vee Q)$
0	0	0
0	1	1
1	0	1
1	1	1

Пример 1.6. Применим операцию дизъюнкции к высказываниям A_3 и A_5 . Получим составное высказывание $A_3 \vee A_5$: «Все люди смертны, или $7 < 4$ ». Несмотря на первоначально кажущуюся странность этого высказывания, нет сомнений в его истинности. К аналогичному заключению приводит также формальное вычисление логического значения данного высказывания по таблице из определения 1.5, исходя из логических значений высказываний A_3 и A_5 : $\lambda(A_3 \vee A_5) = \lambda(A_3) \vee \lambda(A_5) = 1 \vee 0 = 1$. В то же время высказывание

«Саратов находится на берегу Невы, или А. С. Пушкин — великий русский математик», являющееся дизъюнкцией высказываний A_2 и A_7 , безусловно, ложно, что полностью согласуется с формальным вычислением его логического значения по таблице из определения 1.5: $\lambda(A_2 \vee A_7) = \lambda(A_2) \vee \lambda(A_7) = 0 \vee 0 = 0$.

Импликация двух высказываний. Определение 1.7. Импликацией двух высказываний P и Q называется новое высказывание, обозначаемое $P \rightarrow Q$ (читается: «если P , то Q », или «из P следует Q », или « P влечет Q », или « P достаточно для Q », или « Q необходимо для P »), которое ложно в единственном случае, когда высказывание P истинно, а Q — ложно, а во всех остальных случаях — истинно. Другими словами, логическое значение высказывания $P \rightarrow Q$ связано с логическими значениями высказываний P и Q , как указано в следующей таблице, называемой *таблицей истинности операции импликации*:

$\lambda(P)$	$\lambda(Q)$	$\lambda(P \rightarrow Q)$
0	0	1
0	1	1
1	0	0
1	1	1

В высказывании $P \rightarrow Q$ высказывание P называется посылкой или антецедентом, а высказывание Q — следствием или консеквентом.

При определении импликации с еще большей силой встает вопрос, почему именно такое распределение принято в ее таблице истинности. Последние две строки в ней достаточно хорошо согласуются с нашим пониманием выражения «если..., то...». Их обоснованием могут служить следующие соображения. Импликация призвана отразить процесс рассуждения, умозаключения. Общая характеристика этого процесса следующая. Если мы исходим из истинной посылки и правильно (верно) рассуждаем, то мы приходим к истинному заключению (следствию, выводу). Другими словами, если мы исходили из истинной посылки и пришли к ложному выводу, значит, мы неверно рассуждали. В импликации $P \rightarrow Q$ имеется посылка P , следствие Q и процесс рассуждения $\rightarrow$. Процесс рассуждения как раз и моделируется результатом операции $P \rightarrow Q$. Приведенное соображение служит обоснованием результата $1 \rightarrow 0 = 0$, а также результата $1 \rightarrow 1 = 1$.

Определенные сомнения возникают при оценке адекватности первых двух строк в таблице, определяющей импликацию. В первой строке при ложной посылке и ложном следствии импликация признается истинной. Следующие два примера добавляют аргументы в пользу такого определения логического значения импликации в этом случае. Рассмотрим такое высказывание: «Если число делится на 5, то и его квадрат делится на 5». Его истинность не

вызывает сомнения. В частности, мы могли бы сказать: «Если 10 делится на 5, то 10^2 делится на 5» или «Если 11 делится на 5, то и 11^2 делится на 5». В первом из этих высказываний и посылка, и следствие истинны, во втором — и посылка, и следствие ложны. Тем не менее оба этих высказывания истинны. Для большей убедительности второе высказывание можно сформулировать в со-
 слагательной форме: «Если бы 11 делилось на 5, то и 11^2 делилось бы на 5». Есть утверждения такого типа и в житейской речи, которые признаются вполне нормальными. Например, «Если ты можешь переплыть Черное море, то я — турецкий султан».

В пользу второй строки таблицы, когда импликация остается истинной при ложной посылке и истинном следствии, говорит такой пример. Высказывание «Если первое слагаемое делится на 5 и второе слагаемое делится на 5, то и сумма делится на 5», несомненно, истинно. Но, в частности, мы могли бы сказать: «Если 10 делится на 5 и 20 делится на 5, то 30 делится на 5» или «Если 12 делится на 5 и 13 делится на 5, то 25 делится на 5». В первом из этих высказываний и посылка истинна (как конъюнкция двух истинных выражений), и следствие истинно. Во втором же высказывании посылка ложна (как конъюнкция двух ложных высказываний), а следствие истинно. Тем не менее, как мы уже отметили, оба этих высказывания признаются истинными.

Пример 1.8. Высказывание $A_6 \rightarrow A_5$: «Если Волга впадает в Каспийское море, то $7 < 4$ » ложно, так как $\lambda(A_6 \rightarrow A_5) = \lambda(A_6) \rightarrow \lambda(A_5) = 1 \rightarrow 0 = 0$. Высказывание «Если Саратов находится на берегу Невы, то А. С. Пушкин — великий русский математик», являющееся импликацией высказываний A_2 и A_7 , истинно, так как $\lambda(A_2 \rightarrow A_7) = \lambda(A_2) \rightarrow \lambda(A_7) = 0 \rightarrow 0 = 1$.

Эквивалентность двух высказываний. Определение 1.9. Эквивалентностью двух высказываний P и Q называется новое высказывание, обозначаемое $P \leftrightarrow Q$ (читается: « P эквивалентно Q », или « P необходимо и достаточно для Q », или « P тогда и только тогда, когда Q », или « P , если и только если Q »), которое истинно в том и только в том случае, когда одновременно оба высказывания P и Q либо истинны, либо ложны, а во всех остальных случаях — ложно. Другими словами, логическое значение высказывания $P \leftrightarrow Q$ связано с логическими значениями высказываний P и Q , как указано в следующей таблице, называемой *таблицей истинности операции эквивалентности*:

$\lambda(P)$	$\lambda(Q)$	$\lambda(P \leftrightarrow Q)$
0	0	1
0	1	0
1	0	0
1	1	1

Пример 1.10. Высказывание « $7 < 4$ тогда и только тогда, когда снег белый», являющееся эквивалентностью высказываний A_5 и A_8 , ложно, так как $\lambda(A_5 \leftrightarrow A_8) = \lambda(A_5) \leftrightarrow \lambda(A_8) = 0 \leftrightarrow 1 = 0$. Напротив, высказывание «Саратов находится на берегу Невы, если и только если А. С. Пушкин — великий русский математик» истинно, так как оно является эквивалентностью двух ложных высказываний.

Союзы языка и логические операции (язык и логика). Итак, каждая из введенных логических операций является неким математическим образом, моделью соответствующего логического союза нашего языка. Эти понятия призваны отразить на языке нулей и единиц соответствующие союзы нашего мышления, которыми человечество пользуется в течение тысячелетий. Вне всякого сомнения, язык нулей и единиц значительно беднее человеческого языка, и это отражение достаточно грубо и несовершенно. Тем не менее какие-то основные черты (существенные аспекты процессов мышления) понятия логических операций все же отражают. Так, отрицание, конъюнкция и эквивалентность достаточно точно передают суть логических союзов «не», «и», «тогда и только тогда, когда» соответственно. Хуже обстоит дело с дизъюнкцией, призванной отразить языковой союз «или». Следует отметить, что кроме рассматриваемой так называемой *дизъюнкции в не исключающем смысле* (она истинна тогда и только тогда, когда по меньшей мере один ее член истинен) некоторые авторы рассматривают дизъюнкцию в *исключающем смысле* (или строгую дизъюнкцию): она истинна тогда и только тогда, когда истинен точно один ее член.

Наименее адекватным соответствующему союзу языка является понятие импликации, которое призвано отразить логический союз «если... , то...». Это и понятно: на этом союзе основан один из сложнейших умственных процессов — процесс построения выводов, умозаключений. Импликация остается все же самой «коварной» из всех логических операций, и ее определение при всех приведенных доводах оставляет в нас чувство незавершенности. И это неспроста. Наиболее наглядно эта неадекватность определения языку проявится в ходе развития алгебры высказываний, когда мы, например, придем к тому, что тавтологией окажется следующая формула: $(P \rightarrow Q) \vee (Q \rightarrow P)$. Это означает, что какие бы ни были высказывания P и Q , по меньшей мере одно из высказываний $P \rightarrow Q$ или $Q \rightarrow P$ непременно будет истинным. Этот факт уже не согласуется с общепринятой практикой, и он еще раз подтверждает, что понятие импликации лишь весьма условно и приблизительно переводит на язык нулей и единиц тот смысл, который имеется в виду при построении фразы типа «если..., то...».

Из приведенного следует вывод о том, что тонкое и многообразное человеческое мышление не так легко поддается научному

осмыслению и изучению и что алгебра высказываний — всего лишь одно из приближений, всего лишь шаг на пути к познанию человеческого мышления.

По поводу происхождения терминов отметим, что «конъюнкция» происходит от лат. *conjunctio* — соединение, дизъюнкция — от лат. *disjunctio* — разъединение, импликация от лат. *implicatio* — сплетение и *implico* — тесно связываю.

Общий взгляд на логические операции. Еще раз отметим, что только логические значения или значения истинности, а не их содержание интересуют нас в развиваемой теории. Поэтому каждое из введенных определений (1.1, 1.3, 1.5, 1.7, 1.9) операций над высказываниями можно рассматривать как определение некоторого действия над символами 0 и 1, т.е. как определение некоторой операции на двухэлементном множестве $\{0, 1\}$. Например, отрицание задает следующие правила действия с этими символами: $\neg 0 = 1$, $\neg 1 = 0$, конъюнкция — следующие: $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 0 = 0$, $1 \wedge 1 = 1$, импликация — следующие: $0 \rightarrow 0 = 1$, $0 \rightarrow 1 = 1$, $1 \rightarrow 0 = 0$, $1 \rightarrow 1 = 1$ и т.д.

Учитывая два правила действия с символами 0 и 1, определяемые отрицанием, можно записать равенство для вычисления логического значения высказывания $\neg P$:

$$\lambda(\neg P) = \neg \lambda(P). \quad (1.1)$$

Указанные четыре правила действия с символами 0 и 1, определяемые конъюнкцией, позволяют записать равенство для вычисления логического значения высказывания $P \wedge Q$:

$$\lambda(P \wedge Q) = \lambda(P) \wedge \lambda(Q). \quad (1.2)$$

Аналогично, правила действия с символами 0 и 1, сформулированные в определениях 1.5, 1.7, 1.9, дают возможность записать равенства для вычисления логических значений высказываний $P \vee Q$, $P \rightarrow Q$ и $P \leftrightarrow Q$ соответственно:

$$\lambda(P \vee Q) = \lambda(P) \vee \lambda(Q); \quad (1.3)$$

$$\lambda(P \rightarrow Q) = \lambda(P) \rightarrow \lambda(Q); \quad (1.4)$$

$$\lambda(P \leftrightarrow Q) = \lambda(P) \leftrightarrow \lambda(Q). \quad (1.5)$$

Равенства (1.2) ... (1.5) можно записать в виде одного соотношения: $\lambda(P * Q) = \lambda(P) * \lambda(Q)$, где значок «*» обозначает один из символов логических операций $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$. Равенства (1.1) — (1.5) фактически использовались при вычислениях логических значений высказываний $\neg A_6$, $A_2 \wedge A_3$, $A_3 \vee A_5$, $A_2 \vee A_7$, $A_6 \rightarrow A_5$, $A_2 \rightarrow A_7$, $A_5 \leftrightarrow A_8$, которые были проделаны выше в качестве примеров применения операций над высказываниями.

§ 2. Формулы алгебры высказываний

Конструирование сложных высказываний. С помощью логических операций, рассмотренных в § 1, из простейших высказываний можно строить высказывания более сложные. Например, из высказываний A_2, A_3, A_7 можно построить такое высказывание: «Если Саратов находится на берегу Невы и все люди смертны, то А. С. Пушкин — великий русский математик». Построенное высказывание символически записывается так: $(A_2 \wedge A_3) \rightarrow A_7$. Конечно, оно звучит несколько странно, поскольку соединяет в себе столь разнородные понятия, которые обычно существуют раздельно друг от друга. Но нас, еще раз подчеркиваем, интересует не содержание этого высказывания, а его логическое значение. Оно может быть определено, исходя из логических значений исходных высказываний A_2, A_3, A_7 и той схемы, по которой из исходных высказываний построено сложное высказывание. Так как $\lambda(A_2) = 0, \lambda(A_3) = 1, \lambda(A_7) = 0$, то, пользуясь соотношения (1.4), (1.2) и определения 1.7, 1.3, находим: $\lambda[(A_2 \wedge A_3) \rightarrow A_7] = \lambda(A_2 \wedge A_3) \rightarrow \lambda(A_7) = (\lambda(A_2) \wedge \lambda(A_3)) \rightarrow \lambda(A_7) = (0 \wedge 1) \rightarrow 0 = 0 \rightarrow 0 = 1$. Итак, высказывание $(A_2 \wedge A_3) \rightarrow A_7$ истинно.

Для конструирования данного сложного высказывания из простейших высказываний A_2, A_3 и A_7 нужно применить операцию конъюнкции к первым двум высказываниям, а затем к полученному высказыванию и к третьему исходному высказыванию применить операцию импликации. Это словесное описание схемы конструирования данного сложного высказывания можно заменить описанием символическим: $(X \wedge Y) \rightarrow Z$, где X, Y, Z — некоторые символы (переменные), вместо которых можно подставить любые конкретные высказывания. Такая схема конструирования составного высказывания может быть применена к различным конкретным высказываниям, а не только к высказываниям A_2, A_3, A_7 . Например, по этой схеме из высказываний A_4, A_8, A_5 построим высказывание «Если Сократ — человек и снег — белый, то $7 < 4$ ». Находим его логическое значение: $\lambda[(A_4 \wedge A_8) \rightarrow A_5] = \lambda(A_4 \wedge A_8) \rightarrow \lambda(A_5) = (\lambda(A_4) \wedge \lambda(A_8)) \rightarrow \lambda(A_5) = (1 \wedge 1) \rightarrow 0 = 1 \rightarrow 0 = 0$. Таким образом, та же самая схема построения составного высказывания привела к ложному высказыванию. Однако ввиду разнородности понятий, которыми оперируют исходные высказывания A_4, A_8, A_5 , трудно на интуитивной основе судить об истинности высказывания $(A_4 \wedge A_8) \rightarrow A_5$.

По рассматриваемой схеме построено и следующее высказывание: «Если 100 делится на 5 и 100 делится на 2, то 100 делится на 10». Формальное вычисление логического значения данного высказывания показывает, что оно истинно, с чем вполне согласуются наши интуитивные представления об этом высказывании.

Итак, символическая запись $(X \wedge Y) \rightarrow Z$ является своего рода формулой. Конечно, более привычны формулы типа $S = \pi r^2$ (фор-

мула площади круга), $E = mgh$ (формула потенциальной энергии тела) и им подобные. Тем не менее выражение $(X \wedge Y) \rightarrow Z$ также можно считать формулой — формулой схемы конструирования составных высказываний из более простых.

Понятие формулы алгебры высказываний. В формулу $(X \wedge Y) \rightarrow Z$ вместо переменных X, Y, Z можно подставлять конкретные высказывания, после чего вся формула будет превращаться в некоторое составное высказывание. Переменные, вместо которых можно подставлять высказывания, т.е. переменные, пробегающие множество высказываний, называют *пропозициональными переменными*, или высказывательными переменными, или переменными высказываниями. Будем обозначать пропозициональные переменные заглавными буквами латинского алфавита P, Q, R, S, X, Y, Z или такими же буквами с индексами $P_1, P_2, \dots, Q_1, Q_2, \dots, X_1, X_2, \dots, Y_1, Y_2, \dots$. Теперь дадим точное определение *формулы алгебры высказываний*.

Определение 2.1

1. Каждая отдельно взятая пропозициональная переменная есть формула алгебры высказываний.

2. Если F_1 и F_2 — формулы алгебры высказываний, то выражения $\neg F_1, (F_1 \wedge F_2), (F_1 \vee F_2), (F_1 \rightarrow F_2), (F_1 \leftrightarrow F_2)$ также являются формулами алгебры высказываний.

3. Никаких других формул алгебры высказываний, кроме получающихся согласно п. 1 и 2, нет.

Определения такого типа называются индуктивными. В них имеются прямые пункты (в данном случае п. 1 и п. 2), где задаются объекты, которые в дальнейшем именуются определяемым термином (в данном случае — формулами алгебры высказываний), и косвенный пункт (в данном случае п. 3), в котором говорится, что такие объекты исчерпываются объектами, заданными в прямых пунктах. Среди прямых пунктов имеются базисные пункты (в данном случае п. 1), где указываются некоторые конкретные объекты, именуемые в дальнейшем определяемым термином, и индуктивные пункты (в данном случае п. 2), где даются правила получения определяемых объектов, в частности из объектов, перечисленных в базисных пунктах.

В настоящей главе формулы алгебры высказываний будем называть просто формулами. Есть и другие названия для понятия формулы: правильно построенная формула или правильно построенное выражение, но они представляются менее предпочтительными. Само определение формулы, носящее индуктивный характер, на первых порах кажется непривычным. Определения такого типа вам ранее не встречались. Лучшее понимание этого определения наступит, когда вы научитесь применять его для определения того, является или не является формулой последовательность символов (слово), составленная из пропозициональных переменных, символов логических операций и скобок.

К этому полезно добавить следующее. Для каждой формулы должна существовать конечная последовательность всех ее подформул, т. е. такая конечная последовательность, которая начинается с входящих в данную формулу пропозициональных переменных, заканчивается самой этой формулой, и каждый член этой последовательности, не являющийся пропозициональной переменной, есть либо отрицание уже имеющегося члена этой последовательности, либо получается из двух уже имеющихся членов этой последовательности их соединением с помощью одного из знаков $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ и заключением полученного выражения в скобки. Такую последовательность всех подформул данной формулы иногда называют *порождающей последовательностью* для данной формулы. Наличие такой последовательности у логического выражения служит критерием того, что выражение является формулой. Это свойство отличает формулы.

Приведем примеры формул. На основании п. 1 определения 2.1 формулами будут пропозициональные переменные: $P, Q, R, X, Y, Z; P_1, P_2, \dots, Q_1, Q_2, \dots, X_1, X_2, \dots$. Далее на основании п. 2 того же определения из этих формул построим следующие: $\neg P, \neg Q, \neg X, \neg Y, \neg Z, (P \vee R), (X \wedge Y), (X \rightarrow Z), (Q \leftrightarrow R), (Y \vee Z)$. Из построенных формул также на основании п. 2 строим еще более сложные формулы: $(\neg P \wedge \neg Q), (P \wedge \neg P), ((X \wedge Y) \rightarrow Z), ((X \rightarrow Z) \wedge (Y \vee Z)), ((P \vee R) \rightarrow (Q \leftrightarrow R)), ((X \rightarrow Z) \rightarrow Y)$. Ясно, что процесс построения все более сложных формул может продолжаться безгранично.

Приведем примеры выражений, не являющихся формулами. Это в каком-то смысле нелепые выражения. К примеру, выражение $((XY) \rightarrow Z)$ было бы формулой на основании п. 2 определения 2.1, если бы формулами были выражения (XY) и Z . Выражение Z есть пропозициональная переменная и потому на основании п. 1 определения 2.1 является формулой. Рассмотрим выражение (XY) . Оно было бы формулой, если бы между формулами X и Y стоял один из знаков логических связок. Но такого знака нет. Следовательно, выражение (XY) не формула, и исходное выражение $((XY) \rightarrow Z)$ формулой также не является.

Таким образом, индуктивный характер определения 2.1 дает возможность эффективно решать для каждого выражения, является оно формулой алгебры высказываний или нет.

Вот еще примеры выражений, не являющихся формулами (убедитесь в этом самостоятельно): $((P \neg Q) \wedge (P \rightarrow \neg R)), (P \wedge Q \vee R), ((X \rightarrow) \wedge Z), (X \vee \neg Y) \rightarrow (\neg X \wedge \neg Y)$.

То, что последнее выражение не является формулой, может сначала вызвать недоумение. Но после сопоставления его с п. 2 определения 2.1 отмечаем, что в последнем выражении недостает внешних скобок для того, чтобы считать его формулой. Действительно, если бы мы сочли данное выражение формулой, то на

основании п. 2 формулой было бы и выражение $((X \vee \neg Y) \rightarrow \rightarrow (\neg X \wedge \neg Y) \leftrightarrow Z)$. Но оно бессмысленно, потому что неопределенно: неизвестно, какую операцию нужно выполнять первой, импликацию или эквивалентность. А от этого, как можно проверить (проверьте!), будет зависеть логическое значение составного высказывания (см. п. 3), получающегося из последнего выражения, если его превратить в формулу указанием последовательности действий и придать пропозициональным переменным X , Y и Z конкретные значения (высказывания). Если бы в исходном выражении стояли внешние скобки, т. е. если бы оно было формулой $((X \vee \neg Y) \rightarrow (\neg X \wedge \neg Y))$, то сделанное в предыдущем абзаце построение привело бы к формуле $((X \vee \neg Y) \rightarrow (\neg X \wedge \neg Y)) \leftrightarrow Z$.

Итак, требование внешних скобок у формулы не является излишним формализмом. Тем не менее внешние скобки придают формуле громоздкость и, если данная формула не входит составной частью в более сложную формулу, не несут никакой информации и смысловой нагрузки. Поэтому внешние скобки в окончательно записанной формуле договариваются опускать. Например, формулу $((X \wedge Y) \rightarrow Z)$ будем записывать в виде $(X \wedge Y) \rightarrow Z$, а вместо формулы $((X \vee \neg Y) \rightarrow (\neg X \wedge \neg Y))$ будем писать $(X \vee \neg Y) \rightarrow \rightarrow (\neg X \wedge \neg Y)$. Но если данная формула должна будет войти составной частью в более сложную формулу, то сначала заключаем ее во внешние скобки и только потом отправляем в процедуру построения новой формулы.

Логическое значение составного высказывания. Если в формулу алгебры высказываний $F(X_1, X_2, \dots, X_n)$ вместо пропозициональных переменных $X_1, X_2, \dots, X_n$ подставить конкретные высказывания $A_1, A_2, \dots, A_n$ соответственно, то получится некоторое новое составное высказывание $F(A_1, A_2, \dots, A_n)$. Оно называется *конкретизацией* формулы $F(X_1, X_2, \dots, X_n)$ на выборе высказываний $A_1, A_2, \dots, A_n$. Как определить логическое значение $\lambda(F(A_1, A_2, \dots, A_n))$ полученного составного высказывания, если известны логические значения $\lambda(A_1), \lambda(A_2), \dots, \lambda(A_n)$ исходных высказываний $A_1, A_2, \dots, A_n$?

Прежде чем сформулировать в следующей теореме ответ на поставленный вопрос, введем одно понятие. В § 1 отмечалось, что только логические значения высказываний, а не их содержание рассматриваются в алгебре высказываний. Это дает возможность несколько упростить обозначения и терминологию. Так, каждое ложное высказывание можно рассматривать как элемент 0, а каждое истинное — как элемент 1 двухэлементного множества $\{0, 1\}$, и писать вместо $\lambda(P) = 0$ или $\lambda(P) = 1$ лишь только $P = 0$ или $P = 1$ соответственно. Далее, если формула $F(X_1, X_2, \dots, X_n)$ при подстановке вместо ее пропозициональных переменных $X_1, X_2, \dots, X_n$ высказываний $A_1, A_2, \dots, A_n$ с логическими значениями $\lambda(A_1) = \alpha_1,$

$\lambda(A_2) = \alpha_2, \dots, \lambda(A_n) = \alpha_n$ превращается в высказывание $F(A_1, A_2, \dots, A_n)$ с логическим значением $\lambda(F(A_1, A_2, \dots, A_n)) = \alpha$, то будем говорить, что формула $F(X_1, X_2, \dots, X_n)$ принимает значение α , если ее переменные $X_1, X_2, \dots, X_n$ принимают значения $\alpha_1, \alpha_2, \dots, \alpha_n$ соответственно, и писать $X_1 = \alpha_1, X_2 = \alpha_2, \dots, X_n = \alpha_n$ и $F(\alpha_1, \alpha_2, \dots, \alpha_n) = \alpha$, где $\alpha_1, \alpha_2, \dots, \alpha_n, \alpha \in \{0, 1\}$. Для нахождения значения $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ нужно подставить в формулу $F(X_1, X_2, \dots, X_n)$ вместо пропозициональных переменных $X_1, X_2, \dots, X_n$ значения $\alpha_1, \alpha_2, \dots, \alpha_n$ соответственно и в полученном выражении последовательно проделать все действия с нулями и единицами, предписываемые правилами таблиц из определений 1.1, 1.3, 1.5, 1.7, 1.9. В результате получим 0 или 1. Полученное значение будем обозначать $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ и называть *значением* данной формулы $F(X_1, X_2, \dots, X_n)$ на данном наборе нулей и единиц $\alpha_1, \alpha_2, \dots, \alpha_n$. Например, вычислим значение формулы $F(X_1, X_2, X_3) \equiv (X_1 \rightarrow \neg X_2) \wedge (X_2 \leftrightarrow (X_1 \vee \neg X_3))$ на наборе 0, 1, 1: $F(0, 1, 1) = (0 \rightarrow \neg 1) \wedge (1 \leftrightarrow (0 \vee \neg 1)) = (0 \rightarrow 0) \wedge (1 \leftrightarrow (0 \vee 0)) = 1 \wedge (1 \leftrightarrow 0) = 1 \wedge 0 = 0$.

Теорема 2.2. *Логическое значение составного высказывания $F(A_1, A_2, \dots, A_n)$ равно значению формулы $F(X_1, X_2, \dots, X_n)$ на наборе $\lambda(A_1), \lambda(A_2), \dots, \lambda(A_n)$ логических значений составляющих высказываний $A_1, A_2, \dots, A_n$, т.е.*

$$\lambda(F(A_1, A_2, \dots, A_n)) = F(\lambda(A_1), \lambda(A_2), \dots, \lambda(A_n)).$$

Доказательство. Докажем утверждение методом полной математической индукции по числу символов логических операций, входящих в формулу $F(X_1, X_2, \dots, X_n)$.

Если формула $F(X_1, X_2, \dots, X_n)$ содержит 0 символов логических операций, то она представляет собой просто пропозициональную переменную, скажем, X_1 , т.е. $F(X_1, X_2, \dots, X_n) \equiv X_1$ (знак $\equiv$ обозначает абсолютную тождественность двух формул, графическую одинаковость левой и правой частей). Тогда доказываемое соотношение сводится к тривиальному равенству: $\lambda(A_1) = \lambda(A_1)$.

Если формула $F(X_1, X_2, \dots, X_n)$ содержит лишь один символ логической операции, то она является одной из следующих формул: $\neg X_1, X_1 \wedge X_2, X_1 \vee X_2, X_1 \rightarrow X_2, X_1 \leftrightarrow X_2$. В этих случаях доказываемое равенство есть одно из равенств (1.1) — (1.5).

Предположим теперь, что утверждающееся в теореме равенство верно для всех формул алгебры высказываний, содержащих не более k символов логических операций. Докажем, что оно верно для формулы $F(X_1, X_2, \dots, X_n)$, содержащей $k + 1$ символов логических операций. На основании определения 2.1 формула F имеет один из следующих видов: $\neg F_1, F_1 \wedge F_2, F_1 \vee F_2, F_1 \rightarrow F_2, F_1 \leftrightarrow F_2$, где F_1, F_2 — некоторые формулы, каждая из которых содержит уже не более k символов логических операций. Нужно провести доказательство для всех пяти случаев. Но в силу принци-

пиальной идентичности этих доказательств проделаем его, например, для случая $F \equiv F_1 \wedge F_2$. Вычисляем: $\lambda(F(A_1, A_2, \dots, A_n)) = \lambda(F_1(A_1, A_2, \dots, A_n) \wedge F_2(A_1, A_2, \dots, A_n)) = \lambda(F_1(A_1, A_2, \dots, A_n)) \wedge \lambda(F_2(A_1, A_2, \dots, A_n)) = F_1(\lambda(A_1), \dots, \lambda(A_n)) \wedge F_2(\lambda(A_1), \dots, \lambda(A_n)) = F_1(\lambda(A_1), \dots, \lambda(A_n))$. В проделанных вычислениях второе равенство основано на определении 1.3 логической операции конъюнкции. Третье равенство основано на предположении индукции о том, что для формул F_1 и F_2 соотношение теоремы выполняется. Наконец четвертое равенство записано на основании того, что $F \equiv F_1 \wedge F_2$.

Аналогичным образом соотношение теоремы доказывается и во всех остальных случаях конструирования формулы F из формул F_1 и F_2 .

Следовательно, утверждение теоремы верно для любой формулы F алгебры высказываний. $\square$

Итак, здесь необходимо понять, что логическое значение составного высказывания по существу является значением некоторого (логического) выражения при некотором наборе конкретных значений всех входящих в него (пропозициональных) переменных. При этом пропозициональные переменные могут принимать значения 0 или 1, само выражение принимает значение 0 или 1, и вычисляется это значение (в силу теоремы 2.2) посредством применения к значениям 0 и 1 предписываемых данным выражением логических действий. Логические действия над величинами 0 и 1 выполняются по правилам, определяемым таблицами истинности этих действий (операций) — отрицания, конъюнкции, дизъюнкции, импликации и эквивалентности. Таким образом, мы фактически начинаем иметь дело с некой новой (логической) алгеброй, или алгеброй логики, которая как бы «параллельна» привычной школьной алгебре. Сравним компоненты этих двух алгебр с помощью следующей таблицы:

Компонента	Школьная алгебра	Алгебра логики
Базисное множество	R — множество вещественных чисел	$\{0, 1\}$ — двухэлементное множество
Операции над элементами базисного множества	$+, -, \cdot, :$	$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
Переменные	Вещественные $a, b, c, \dots, x, y, z, \dots$	Пропозициональные $P, Q, R, \dots, X, Y, Z, \dots$
Формулы (правильно построенные выражения)	$ax + by + cz, ax^2 - bx + c$ и т.д.	$(\neg P \wedge Q) \leftrightarrow \neg R, \neg(P \rightarrow \rightarrow Q) \vee R$ и т.д.

Аналогия со школьной алгеброй будет продолжена в § 4 при рассмотрении равносильных преобразований в алгебре логики.

Составление таблиц истинности для формул. На основании теоремы 2.2 можно для данной формулы F алгебры высказываний найти логические значения всех тех высказываний, в которые формула превращается при подстановке вместо всех ее пропозициональных переменных различных конкретных высказываний. При этом говорят о логическом значении самой формулы и о логических значениях ее пропозициональных переменных. При нахождении логических значений формулы, соответствующих всевозможным наборам значений ее пропозициональных переменных, удобной формой записи является табличная форма. Рассмотрим примеры.

Пример 2.3. Составим таблицу истинности для формулы $(X \rightarrow Y) \vee (Y \rightarrow X)$. В первых двух столбцах таблицы выпишем всевозможные пары логических значений, которые могут принимать пропозициональные переменные X и Y (точнее, те высказывания, которые могут быть подставлены в формулу вместо пропозициональных переменных X и Y). В последующих столбцах выписываем логические значения формул $X \rightarrow Y$, $Y \rightarrow X$ и $(X \rightarrow Y) \vee (Y \rightarrow X)$, образующих так называемую *порождающую последовательность* для данной формулы. Руководствуемся при этом определениями логических операций импликации и дизъюнкции. В результате получаем таблицу:

$\lambda(X)$	$\lambda(Y)$	$\lambda(X \rightarrow Y)$	$\lambda(Y \rightarrow X)$	$\lambda((X \rightarrow Y) \vee (Y \rightarrow X))$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	1
1	1	1	1	1

Первые два столбца и последний столбец составленной таблицы задают соответствия между логическими значениями исходных высказываний и логическим значением составного высказывания, получаемого по данной формуле. Эти три столбца и образуют *таблицу истинности данной формулы*. Остальные два столбца (для логических значений $\lambda(X \rightarrow Y)$ и $\lambda(Y \rightarrow X)$) носят вспомогательный, промежуточный характер.

Пример 2.4. Составим таблицу истинности для формулы $F(P, Q, R) \equiv (P \wedge Q) \rightarrow (P \leftrightarrow \neg R)$. Она содержит три пропозициональные переменные, для которых имеются точно восемь различных наборов значений истинности. Таблица истинности для рассматриваемой формулы вместе с промежуточными столбцами выглядит следующим образом:

$\lambda(P)$	$\lambda(Q)$	$\lambda(R)$	$\lambda(P \wedge Q)$	$\lambda(\neg R)$	$\lambda(P \leftrightarrow \neg R)$	$\lambda(F)$
0	0	0	0	1	0	1
0	0	1	0	0	1	1
0	1	0	0	1	0	1
0	1	1	0	0	1	1
1	0	0	0	1	1	1
1	0	1	0	0	0	1
1	1	0	1	1	1	1
1	1	1	1	0	0	0

Таблицу истинности формулы можно составлять в сокращенном виде.

Пример 2.5. Составим, например, такую таблицу для формулы: $(X \wedge \neg Y) \leftrightarrow (\neg X \vee Y)$ (внешние скобки у формулы, согласно договоренности, опущены). В первой строке таблицы выпишем данную формулу. Под переменными X и Y выписываем всевозможные наборы их логических значений. Далее столбец под первым знаком $\neg$ заполним логическими значениями формулы $\neg Y$, исходя из соответствующих значений переменной Y , а столбец под знаком $\wedge$ — логическими значениями формулы $(X \wedge \neg Y)$, исходя из соответствующих логических значений формул X и $\neg Y$. Затем заполняем столбец под вторым знаком $\neg$ значениями формулы $\neg X$ и столбец под знаком $\vee$ — значениями формулы $(\neg X \vee Y)$. Наконец заполняем столбец под знаком $\leftrightarrow$ логическими значениями данной формулы. В итоге получаем

$(X \wedge \neg Y) \leftrightarrow (\neg X \vee Y)$						
0	0	1	0	1	1	0
0	0	0	0	1	1	1
1	1	1	0	0	0	0
1	0	0	0	0	1	1

Выделенные жирным шрифтом табулированные значения представляют собой столбец логических значений данной формулы.

Практика составления довольно большого числа таблиц истинности есть наилучший способ прочно запомнить определения логических связок (отрицания, конъюнкции, дизъюнкции, импликации, эквивалентности) и довести до автоматизма выдачу значений любой из этих операций. Это знание необходимо для решения более содержательных задач алгебры высказываний.

Классификация формул алгебры высказываний. Формулы алгебры высказываний подразделяются на следующие типы: выполнимые, тавтологии, опровержимые и тождественно ложные.

Формула алгебры высказываний $F(X_1, X_2, \dots, X_n)$ называется *выполнимой*, если некоторая ее конкретизация является истинным высказыванием, т. е. существуют такие конкретные высказывания $A_1, A_2, \dots, A_n$, которые, будучи подставленными в эту формулу вместо переменных $X_1, X_2, \dots, X_n$ соответственно, превращают ее в истинное высказывание. Таким образом, $F(X_1, X_2, \dots, X_n)$ выполнима, если существуют такие конкретные высказывания $A_1, A_2, \dots, A_n$, что $\lambda(F(A_1, A_2, \dots, A_n)) = 1$. Выполнимой формулой является, в частности, формула, рассмотренная в примере 2.4. Она превращается в истинное высказывание, если, например, вместо пропозициональных переменных P, Q, R подставить ложные высказывания. Выполнима также формула $(X \wedge Y) \rightarrow Z$, конкретизация которой рассмотрена в начале § 2 (см. с. 23).

Формула $F(X_1, X_2, \dots, X_n)$ называется *тавтологией*, или *тождественно истинной*, если она превращается в истинное высказывание при всякой подстановке вместо переменных конкретных высказываний $A_1, A_2, \dots, A_n$, т. е. если $\lambda(F(A_1, A_2, \dots, A_n)) = 1$ для любых высказываний $A_1, A_2, \dots, A_n$. Формула из примера 2.3 является тавтологией. Для обозначения тавтологии используется знак $\equiv$, который ставится перед формулой, являющейся тавтологией. Таким образом, запись $\equiv F(X_1, X_2, \dots, X_n)$ означает, что формула $F(X_1, X_2, \dots, X_n)$ является тавтологией. В частности, для указанного примера можем записать $\equiv (X \rightarrow Y) \vee (Y \rightarrow X)$.

Формула $F(X_1, X_2, \dots, X_n)$ называется *опровержимой*, если существуют такие конкретные высказывания $A_1, A_2, \dots, A_n$, которые превращают данную формулу в ложное высказывание $F(A_1, A_2, \dots, A_n)$, т. е. $\lambda(F(A_1, A_2, \dots, A_n)) = 0$. Другими словами, опровержимые формулы — это формулы, не являющиеся тавтологиями. Опровержимой является формула, рассмотренная в примере 2.4. Она обращается в ложное высказывание лишь тогда, когда вместо всех переменных P, Q, R подставлены истинные высказывания. Формула $(X \wedge Y) \rightarrow Z$ также опровержима.

Наконец, формула $F(X_1, X_2, \dots, X_n)$ называется *тождественно ложной*, или *противоречием*, если $\lambda(F(A_1, A_2, \dots, A_n)) = 0$ для любых конкретных высказываний $A_1, A_2, \dots, A_n$. Другими словами, тождественно ложные формулы — это такие формулы, которые не являются выполнимыми.

Примеры формул различных типов приведены в Задачнике (см. № 1.26 — 1.28). При решении задач на классификацию формул полезно отказаться от механического составления таблиц истинности и научиться решать их методом анализа структуры формулы и нахождения тех отдельных наборов значений переменных, в случае которых формула принимает определяющее значение.

Мышление и математическая логика. В заключение следует отметить, что мы приступили к фундаментальному процессу исследования математическими методами такой сферы, как область

человеческого мышления. Начало процессу математизации логики положено математизацией языка. Фактически построена своеобразная знаковая система (*символический язык логики высказываний*), с помощью которой можно попытаться отразить человеческую мысль и проследить оформление мыслительного процесса. Этот язык основывается на алфавите, состоящем из следующих символов:

- 1) пропозициональных букв: $P, Q, R, \dots$;
- 2) символов логических операций: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$;
- 3) технических знаков: $(,)$.

Словами построенного языка являются формулы логики высказываний. Предложения обычного (русского) языка могут быть «переведены» на символический язык логики высказываний, где они представляются формулами логики высказываний (см. Задачник, № 1.13, 1.14, и, особенно, § 3). Следует иметь в виду, что при таком переводе сохраняются логическое содержание, логическая структура предложения, но конечно же теряются его языковая красота и психологические оттенки. Формула представляет собой формальную последовательность знаков, составленную по строгим правилам, нарушение которых недопустимо. Такой перевод высказывания естественного языка на символический язык называется его *формализацией*. В частности, перевод высказывания на символический язык логики высказываний есть его формализация в рамках символической логики высказываний. Получаемая формула показывает способ соединения простых высказываний в составное при помощи логических союзов. Она представляет как бы в «чистом виде» логическую структуру составного высказывания.

Формула логики высказываний сама по себе не имеет никакого содержания. В частности, она не является ни истинной, ни ложной. Она превращается в высказывание, истинное или ложное, при всякой постановке вместо всех ее пропозициональных переменных любых конкретных высказываний. Такой процесс постановки называется *интерпретацией* данной формулы алгебры высказываний.

Таким образом, имеются два взаимно-обратных процесса (две процедуры): формализация и интерпретация. Если имеется формула F и высказывание A есть результат ее интерпретации, то сама формула F будет формализацией высказывания A . Обратно, если имеется высказывание A и формула F есть его формализация, то высказывание A будет одной из интерпретаций формулы F . Итак, формализация — это переход от высказывания естественного языка к формуле логики высказываний, а интерпретация — переход от формулы логики высказываний к высказыванию естественного языка. Таблица истинности или таблица значений формулы логики высказываний — это таблица, которая указывает логическое значение формулы при любой ее интерпретации.

Осознание этих понятий исключительно важно на данном этапе, поскольку они являются ключевыми для изучения в дальнейшем более глубоких разделов математической логики. На данном этапе делается первый шаг на пути формализации — важнейшего метода математической логики.

§ 3. Тавтологии алгебры высказываний

О значении тавтологий. Тавтологии представляют собой схемы построения истинных высказываний, независимо от содержания и истинности составляющих высказываний. Так, если для установления того, истинны или нет высказывания «Саратов основан в 1590 году», «Солнце вращается вокруг Земли», необходимо обладать специальными знаниями или заглянуть в специальную литературу, то для выяснения значения истинности высказываний «Треугольник ABC прямоугольный, или треугольник ABC не прямоугольный», «Неверно, что информация о наследственных признаках хранится в генах, и эта информация в генах не хранится» уже не нужно обладать знаниями ни в математике, ни в генетике. Вывод об истинности последних высказываний делаем, исходя не из их содержания, а из их формы, структуры. Структура первого из последних высказываний выражается формулой $X \vee \neg X$, второго — формулой $\neg(X \wedge \neg X)$. Легко убедиться в том, что обе эти формулы суть тавтологии. Данные формулы дают две схемы построения всегда истинных высказываний. И такова каждая формула, являющаяся тавтологией. Но главное значение тавтологий не в этом.

Основное значение тавтологий состоит в том, что некоторые из них предоставляют правильные способы построения умозаключений, т.е. такие способы, которые от истинных посылок всегда приводят к истинным выводам. А ведь именно такие рассуждения углубляют наши знания и обогащают их истинными сведениями. В частности, любая тавтология алгебры высказываний вида $F \rightarrow G$ соответствует некоторой общей схеме логического умозаключения. Поясним сказанное на примере следующей тавтологии указанного вида (внешние скобки опущены): $((\neg X \rightarrow Y) \wedge (\neg X \rightarrow \neg Y)) \rightarrow X$. (Проверьте, действительно ли данная формула является тавтологией.) Попытаемся выяснить, какой схеме логического умозаключения она соответствует. Схема логического умозаключения, описываемая данной тавтологией, часто используется в математических доказательствах. Она состоит в следующем. Допустим, что требуется доказать истинность некоторого утверждения A . Предполагается, что истинно его отрицание $\neg A$. Затем доказывается, что имеется некоторое такое утверждение B , для которого истинными являются оба утверждения $\neg A \rightarrow B$ и $\neg A \rightarrow \neg B$. Доказательства истинности этих импликаций зависят от содержания высказываний A и B и

устанавливаются на основании методов и законов той математической теории, к которой они относятся. Считаем, что истинность утверждений $\neg A \rightarrow B$ и $\neg A \rightarrow \neg B$ установлена. Одновременный вывод двух утверждений B и $\neg B$ — противоречие, абсурд. Тогда утверждаем, что истинно высказывание A . Такой метод доказательства называется *методом приведения к абсурду*.

Термин «тавтология» имеет греческое происхождение, составлен из двух слов $\tau\alpha\upsilon\tau\omicron\varsigma$ (то же самое) и $\lambda\omicron\gamma\omicron\varsigma$ (слово) и означает повторение одного и того же определения, суждения иными, близкими по смыслу словами. В тавтологиях, относящихся к математической логике, заключительной логической связкой является эквивалентность $\leftrightarrow$. Например, тавтология $(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R))$ выражает одинаковость форм (формул) в ее левой и правой частях, т.е. имеется в виду семантическая одинаковость, выражаемая разными словами — формами (формулами). Совершенно аналогично в этом смысле арифметическое тождество $x(y + z) = xy + xz$, которое отражает ту же внутреннюю сущность посредством разных слов. И каждое из этих двух выражений является объективным законом, действующим каждый в своей сфере: первый — в сфере мыслительных процессов, второй — в сфере чисел. Каждый из этих законов несет объективную информацию об определенной части окружающего нас мира. Труднее в этом смысле истолковать тавтологии вида $P \vee \neg P$, $P \rightarrow P$, $P \rightarrow (Q \rightarrow P)$ и т.п., но на них данный термин просто распространяется.

Основные тавтологии. Приведем некоторые основные тавтологии, выражающие свойства логических операций, а также тавтологии, на которых основаны некоторые схемы математических доказательств.

Теорема 3.1. Следующие формулы алгебры высказываний являются тавтологиями:

- а) закон исключенного третьего $P \vee \neg P$;
- б) закон отрицания противоречия $\neg(P \wedge \neg P)$;
- в) закон двойного отрицания $\neg\neg P \leftrightarrow P$;
- г) закон тождества $P \rightarrow P$;
- д) закон контрапозиции $(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$;
- е) закон силлогизма (правило цепного заключения)
 $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R)$;
- ж) закон противоположности $(P \leftrightarrow Q) \leftrightarrow (\neg P \leftrightarrow \neg Q)$;
- з) правило добавления антецедента («истина из чего угодно»)
 $P \rightarrow (Q \rightarrow P)$;
- и) правило «из ложного что угодно» $\neg P \rightarrow (P \rightarrow Q)$;
- к) правило «модус поненс» (*modus ponens*) $(P \wedge (P \rightarrow Q)) \rightarrow Q$;
- л) правило «модус толленс» (*modus tollens*) $((P \rightarrow Q) \wedge \neg Q) \rightarrow \neg P$;
- м) правило перестановки посылок
 $(P \rightarrow (Q \rightarrow R)) \leftrightarrow (Q \rightarrow (P \rightarrow R))$;

н) правило объединения (и разведения) посылок

$$(P \rightarrow (Q \rightarrow R)) \leftrightarrow ((P \wedge Q) \rightarrow R);$$

о) правило разбора случаев

$$((P \rightarrow R) \wedge (Q \rightarrow R)) \leftrightarrow ((P \vee Q) \rightarrow R);$$

п) правило приведения к абсурду

$$((\neg P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q)) \rightarrow P, (\neg P \rightarrow (Q \wedge \neg Q)) \rightarrow P.$$

Доказательство. Отметим, что непосредственно из определений логических операций вытекает тождественная истинность формул а), б), в), г); для формулы д) доказательство имеется в Задачнике (см. № 1.28, д). Установим тождественную истинность формул л) и н) (для остальных проверьте самостоятельно).

л) Изучая тавтологии, важно уяснить, что имеется простой и надежный алгоритм (общий метод), позволяющий для *любой* формулы логики высказываний дать ответ на вопрос, является она тавтологией логики высказываний или нет — этот алгоритм состоит в построении ее таблицы истинности. Составим таблицу истинности данной формулы:

$\lambda(P)$	$\lambda(Q)$	$\lambda(P \rightarrow Q)$	$\lambda(\neg Q)$	$\lambda((P \rightarrow Q) \wedge \neg Q)$	$\lambda(\neg P)$	$\lambda(F)$
0	0	1	1	1	1	1
0	1	1	0	0	1	1
1	0	0	1	0	0	1
1	1	1	0	0	0	1

Последний столбец таблицы, состоящий из значений истинности данной формулы, содержит лишь единицы. Это означает, что данная формула — тавтология.

н) Доказательство тождественной истинности формул с помощью составления их таблиц истинности проходит автоматически. Приведем следующее доказательство, рассуждая о тех значениях, которые формула может принимать.

Покажем, что левая часть данной эквивалентности обращается в ложное высказывание тогда и только тогда, когда в ложное высказывание обращается формула, стоящая в правой части эквивалентности. Действительно, формула $P \rightarrow (Q \rightarrow R)$ превращается в ложное высказывание, если и только если $\lambda(P) = 1$, $\lambda(Q \rightarrow R) = 0$. В свою очередь, $\lambda(Q \rightarrow R) = 0$ тогда и только тогда, когда $\lambda(Q) = 1$ и $\lambda(R) = 0$. Итак, $\lambda(P \rightarrow (Q \rightarrow R)) = 0$ в том и только в том случае, когда $\lambda(P) = 1$, $\lambda(Q) = 1$, $\lambda(R) = 0$. С другой стороны, формула $(P \wedge Q) \rightarrow R$ обращается в ложное высказывание, если и только если $\lambda(P \wedge Q) = 1$ и $\lambda(R) = 0$. В свою очередь, $\lambda(P \wedge Q) = 1$ тогда и только тогда, когда $\lambda(P) = 1$ и $\lambda(Q) = 1$. Итак, $\lambda((P \wedge Q) \rightarrow R) = 0$ в том и только в том случае, когда $\lambda(P) = 1$, $\lambda(Q) = 1$ и $\lambda(R) = 0$. Доказанное означает, что правая и левая части эквивалентности одновременно превращаются либо в истинные высказывания, либо

в ложные. Следовательно, по определению эквивалентности вся формула всегда превращается в истинное высказывание, т.е. является тавтологией. $\square$

Тавтологии, собранные в теореме 3.1, лежат в основе многих математических рассуждений, что уже обсуждалось в начале § 3 относительно тавтологии теоремы 3.1, n (см. с. 33). Применение некоторых других тавтологий в процессе математических рассуждений рассмотрено в § 7. Тавтологии последующих теорем данного параграфа выражают свойства логических операций.

Теорема 3.2 (свойства конъюнкции и дизъюнкции). *Следующие формулы алгебры высказываний являются тавтологиями:*

а) законы идемпотентности $(P \wedge P) \leftrightarrow P, (P \vee P) \leftrightarrow P$;

б) законы упрощения $(P \wedge Q) \rightarrow P, P \rightarrow (P \vee Q)$;

в) законы коммутативности

$$(P \wedge Q) \leftrightarrow (Q \wedge P), (P \vee Q) \leftrightarrow (Q \vee P);$$

г) законы ассоциативности

$$(P \wedge (Q \wedge R)) \leftrightarrow ((P \wedge Q) \wedge R), (P \vee (Q \vee R)) \leftrightarrow ((P \vee Q) \vee R);$$

д) законы дистрибутивности

$$(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R)),$$

$$(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R));$$

е) законы поглощения

$$(P \wedge (P \vee Q)) \leftrightarrow P, (P \vee (P \wedge Q)) \leftrightarrow P;$$

ж) законы де Моргана

$$\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q), \neg(P \vee Q) \leftrightarrow (\neg P \wedge \neg Q).$$

Доказательство. Докажем для примера, что первый закон де Моргана (см. формулу 3.2, ж)) является тавтологией. Пусть A и B — произвольные конкретные высказывания. Рассмотрим два составных высказывания $\neg(A \wedge B)$ и $\neg A \vee \neg B$, получающиеся из частей данной эквивалентности при замене пропозициональных переменных P и Q конкретными высказываниями A и B соответственно. Предположим, во-первых, что высказывание $\neg(A \wedge B)$ истинно. Тогда конъюнкция $A \wedge B$ ложна; следовательно, по меньшей мере одно из высказываний A или B ложно. Но в таком случае хотя бы одно из высказываний $\neg A$ или $\neg B$ истинно, следовательно, их дизъюнкция $\neg A \vee \neg B$ истинна. Предположим, во-вторых, что высказывание $\neg(A \wedge B)$ ложно. Тогда конъюнкция $A \wedge B$ истинна. Следовательно, оба высказывания A и B истинны, а их отрицания $\neg A$ и $\neg B$ оба ложны, т.е. дизъюнкция $\neg A \vee \neg B$ ложна. Таким образом, для любых двух высказываний значения частей рассматриваемой эквивалентности совпадают. Следовательно, формула тождественно истинна. $\square$

Рекомендуется доказать самостоятельно тождественную истинность остальных формул теоремы 3.2, а также формул следующих далее теорем 3.3 и 3.4.

Теорема 3.3 (свойства импликации и эквивалентности). *Следующие формулы алгебры высказываний являются тавтологиями:*

- а) $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R));$
- б) $P \rightarrow (Q \rightarrow (P \wedge Q));$
- в) $(P \rightarrow R) \rightarrow ((Q \rightarrow R) \rightarrow ((P \vee Q) \rightarrow P));$
- г) $(P \rightarrow Q) \rightarrow ((P \rightarrow \neg Q) \rightarrow \neg P);$
- д) $(\neg Q \wedge (P \rightarrow Q)) \rightarrow \neg P;$
- е) $(\neg P \wedge (P \vee Q)) \rightarrow Q;$
- ж) $(P \rightarrow Q) \rightarrow ((P \vee R) \rightarrow (Q \vee R));$
- з) $(P \rightarrow Q) \rightarrow ((P \wedge R) \rightarrow (Q \wedge R));$
- и) $(P \rightarrow Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \rightarrow R));$
- к) $(P \rightarrow Q) \vee (Q \rightarrow P);$
- л) $(\neg Q \rightarrow \neg P) \rightarrow ((\neg Q \rightarrow P) \rightarrow Q);$
- м) $((P \rightarrow Q) \wedge (R \rightarrow Q)) \leftrightarrow ((P \vee R) \rightarrow Q);$
- н) $((P \rightarrow Q) \wedge (P \rightarrow R)) \leftrightarrow (P \rightarrow (Q \wedge R));$
- о) $P \leftrightarrow P;$
- п) $(P \leftrightarrow Q) \leftrightarrow (Q \leftrightarrow P);$
- р) $((P \leftrightarrow Q) \wedge (Q \leftrightarrow R)) \rightarrow (P \leftrightarrow R).$

Теорема 3.4 (выражение одних логических операций через другие).

Следующие формулы алгебры высказываний являются тавтологиями:

- а) $(P \rightarrow Q) \leftrightarrow (\neg P \vee Q);$
- б) $(P \rightarrow Q) \leftrightarrow \neg(P \wedge \neg Q);$
- в) $(P \wedge Q) \leftrightarrow \neg(\neg P \vee \neg Q);$
- г) $(P \wedge Q) \leftrightarrow \neg(P \rightarrow \neg Q);$
- д) $(P \vee Q) \leftrightarrow \neg(\neg P \wedge \neg Q);$
- е) $(P \vee Q) \leftrightarrow (\neg P \rightarrow Q);$
- ж) $(P \leftrightarrow Q) \leftrightarrow ((P \rightarrow Q) \wedge (Q \rightarrow P)).$

Основные правила получения тавтологий. Опишем два правила, которые позволяют получать новые тавтологии из уже имеющихся.

Теорема 3.5 (правило заключения). Если формулы F и $F \rightarrow H$ являются тавтологиями, то формула H также тавтология. Другими словами, из $\models F$ и $\models F \rightarrow H$ следует $\models H$.

Доказательство. Пусть $\models F(X_1, \dots, X_n)$ и $\models F(X_1, \dots, X_n) \rightarrow H(X_1, \dots, X_n)$. Предположим, что формула $H(X_1, \dots, X_n)$ не является тавтологией. Это означает, что существуют такие конкретные высказывания $A_1, \dots, A_n$, что $\lambda(H(A_1, \dots, A_n)) = 0$. Поскольку $F(X_1, \dots, X_n)$ — тавтология, то для $A_1, \dots, A_n$ имеем $\lambda(F(A_1, \dots, A_n)) = 1$. Вычисляем, пользуясь соотношением (1.4): $\lambda(F(A_1, \dots, A_n) \rightarrow H(A_1, \dots, A_n)) = \lambda(F(A_1, \dots, A_n)) \rightarrow \lambda(H(A_1, \dots, A_n)) = 1 \rightarrow 0 = 0$, что противоречит тождественной истинности формулы $F \rightarrow H$. Следовательно, предположение неверно. Тогда $\models H$, что и требовалось доказать. $\square$

Правило заключения называется также *правилом отделения* или *правилом «modus ponens»* (*modus ponens*).

Второе правило получения тавтологий носит название правила подстановки. Пусть в формуле F содержится пропозициональная переменная X (а возможно, и другие пропозициональные переменные), и H — любая формула. Если в формулу F вместо символа X везде, где он входит в F , вставить формулу H , то получим но-

вую формулу. Она обозначается $S_X^H F$ и называется *формулой, полученной из F в результате подстановки в нее формулы H вместо пропозициональной переменной X* . Например, если в формулу $((X \vee Y) \rightarrow (X \wedge \neg Y))$ вместо переменной Y подставить формулу $(X_1 \wedge X_2)$, то получим $((X \vee (X_1 \wedge X_2)) \rightarrow (X \wedge \neg(X_1 \wedge X_2)))$. Если в ту же формулу вместо переменной Y подставить формулу Z , то произойдет просто замена переменной, в результате которой получится формула $((X \vee Z) \rightarrow (X \wedge \neg Z))$.

Если формула F содержит две пропозициональные переменные X и Y (а возможно, и еще несколько), то можно определить одновременную подстановку двух формул H и G в формулу F вместо пропозициональных переменных X и Y соответственно как одновременную замену символа X всюду, где он входит в F , формулой H и символа Y всюду, где он входит в F , формулой G . Получающуюся формулу обозначают $S_{X,Y}^{H,G} F$. Например, подстановка в формулу $(X \rightarrow (X \wedge Y))$ вместо переменной X формулы $(X_1 \vee X_2)$, а вместо переменной Y формулы $\neg Z$ приводит к формуле $((X_1 \vee X_2) \rightarrow ((X_1 \vee X_2) \wedge \neg Z))$.

Аналогично определяется одновременная подстановка в формулу F и большего числа формул (трех, четырех и т.д.).

Теорема 3.6 (правило подстановки). *Если формула F , содержащая пропозициональную переменную X , является тавтологией, то подстановка в формулу F вместо переменной X любой формулы H снова приводит к тавтологии. Другими словами, из $\models F$ следует $\models S_X^H F$.*

Доказать это. Так как $\models F(X, Y, \dots)$, то формула $F(X, Y, \dots)$ превращается в истинное высказывание при подстановке вместо всех пропозициональных переменных $X, Y, \dots$ любых конкретных высказываний. Истинность получаемого высказывания не зависит от структуры подставляемых вместо $X, Y, \dots$ высказываний. В частности, вместо X может быть подставлено высказывание, которое само является конкретизацией формулы $H(Z_1, \dots, Z_k)$ на некотором наборе конкретных высказываний. Но это и означает, что тавтологией будет формула $F(H(Z_1, \dots, Z_k), Y, \dots)$, т.е. $\models S_X^H F$, что и требовалось доказать. $\square$

Например, если в тавтологии $(X \rightarrow (Y \rightarrow X))$ выполнить подстановку формулы $(X_1 \wedge \neg X_2)$ вместо переменной X , то получим тавтологию $((X_1 \wedge \neg X_2) \rightarrow (Y \rightarrow (X_1 \wedge \neg X_2)))$.

Замечание 3.7. Отметим, что правило подстановки позволяет рассматривать каждую из тавтологий, приведенных в теоремах 3.1 — 3.4, не как отдельно взятую тавтологию, а как схему образования тавтологий. Значит, каждая из пропозициональных переменных в данных формулах может рассматриваться не как переменная, а как произвольная формула алгебры высказываний. Например, тавтология б) из теоремы 3.3 предоставляет бесконечное множество тавтологий вида $\models F_1 \rightarrow (F_2 \rightarrow (F_1 \wedge F_2))$, где F_1, F_2 — произвольные формулы алгебры высказываний.

Два рассмотренных правила образования тавтологий — «модус поненс» и правило подстановки — будем называть *основными*. Существуют и другие правила (см. § 6), которые будем называть *вторичными* или *производными* правилами.

§ 4. Логическая равносильность формул

Понятие равносильности формул. *Определение 4.1.* Формулы $F(X_1, X_2, \dots, X_n)$ и $H(X_1, X_2, \dots, X_n)$ алгебры высказываний называются *равносильными* (*эквивалентными*), если при любых значениях входящих в них пропозициональных переменных логические значения получающихся из формул F и H высказываний совпадают. Для указания равносильности формул используют обозначение $F \equiv H$. Определение равносильности формул можно записать символически:

$$F \equiv H \Leftrightarrow \lambda(F(A_1, A_2, \dots, A_n)) = \lambda(H(A_1, A_2, \dots, A_n)) \quad (4.1)$$

для любых конкретных высказываний $A_1, A_2, \dots, A_n$.

Не следует думать, что в обе формулы F и H непременно входят одни и те же переменные. Некоторые из переменных $X_1, X_2, \dots, X_n$ могут фактически отсутствовать в любой из них. Проверим, например, равносильность формул $\neg X_1$ и $\neg X_2 \wedge (X_2 \vee \neg X_1)$. Для этого составим таблицы истинности обеих формул и убедимся, что значения истинности получающихся из них высказываний одинаковы для любых одинаковых наборов значений пропозициональных переменных X_1 и X_2 :

$\lambda(X_1)$	$\lambda(X_2)$	$\lambda(\neg X_1)$	$\lambda(X_2 \vee \neg X_1)$	$\lambda(\neg X_1 \wedge (X_2 \vee \neg X_1))$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	0

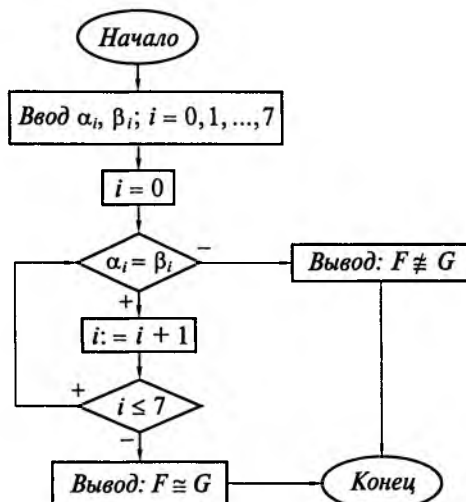
Проверьте самостоятельно справедливость равносильностей $X_1 \vee \neg X_1 \equiv X_2 \vee \neg X_2$, $X_1 \wedge \neg X_1 \equiv X_2 \wedge \neg X_2$.

Выписывание в предыдущем определении в формулах F и H одних и тех же пропозициональных переменных обусловлено стремлением сделать записи и рассуждения более краткими и лаконичными. Это замечание следует иметь в виду и далее (например, при изучении § 6).

Для лучшего усвоения понятия равносильности формул алгоритм проверки на равносильность двух формул $F(X, Y, Z)$ и $G(X, Y, Z)$ можно представить в виде условной схемы (приведена в тексте). Формулы $F(X, Y, Z)$ и $G(X, Y, Z)$ заданы своими таблицами значений:

X	Y	Z	$F(X, Y, Z)$	$G(X, Y, Z)$
0	0	0	α_0	β_0
0	0	1	α_1	β_1
0	1	0	α_2	β_2
0	1	1	α_3	β_3
1	0	0	α_4	β_4
1	0	1	α_5	β_5
1	1	0	α_6	β_6
1	1	1	α_7	β_7

Алгоритм проверки формул на равносильность



Проанализируйте работу данного алгоритма и сопоставьте ее с определением понятия равносильности формул.

Признак равносильности формул. Сущность признака состоит в выявлении тесной связи между понятием равносильности формул и понятием тавтологии.

Теорема 4.2 (признак равносильности формул). *Две формулы F и H алгебры высказываний равносильны тогда и только тогда, когда формула $F \leftrightarrow H$ является тавтологией.*

$$F \equiv H \Leftrightarrow F \leftrightarrow H. \quad (4.2)$$

Доказательство. Если $F \equiv H$, то по определению 4.1 $\lambda(F(A_1, \dots, A_n)) = \lambda(H(A_1, \dots, A_n))$ для любых высказываний $A_1, \dots, A_n$. Тогда (по определению 1.9 операции эквивалентности) $\lambda(F(A_1, \dots, A_n)) \leftrightarrow \lambda(H(A_1, \dots, A_n)) = 1$, откуда на основании соотношения (1.5) заключаем, что $\lambda(F(A_1, \dots, A_n) \leftrightarrow H(A_1, \dots, A_n)) = 1$ для любых $A_1, \dots, A_n$.

Последнее означает по определению тавтологии, что $\models F \leftrightarrow H$. Обратными рассуждениями доказывается утверждение: если $\models F \leftrightarrow H$, то $F \equiv H$. Теорема доказана. $\square$

Отметим, что равносильность формул — это *не* (логическая) операция над формулами, а *отношение* между формулами логики высказываний. Это означает, что если F и G — формулы, то выражение $F \equiv G$ уже не является формулой алгебры высказываний; оно — утверждение о некотором взаимоотношении между формулами F и G , лишь сокращенная (символическая) запись утверждения (высказывания) « F равносильна G » об этих формулах. Это утверждение либо истинно, либо ложно, т.е. F и G либо находятся в отношении равносильности, либо нет. В приведенном далее следствии из теоремы 4.2 устанавливаются некоторые свойства этого отношения между формулами алгебры высказываний.

Следствие 4.3. *Отношение равносильности между формулами алгебры высказываний:*

а) *рефлексивно*: $F \equiv F$;

б) *симметрично*: если $F_1 \equiv F_2$, то $F_2 \equiv F_1$;

в) *транзитивно*: если $F_1 \equiv F_2$ и $F_2 \equiv F_3$, то $F_1 \equiv F_3$,

т.е. отношение равносильности является отношением эквивалентности.

Доказательство. Рефлексивность следует непосредственно из тавтологии теоремы 3.3, *о* и теоремы 4.2.

Для доказательства симметричности отношения $\equiv$ предположим, что $F_1 \equiv F_2$, т.е. на основании признака равносильности (теорема 4.2) $\models F_1 \leftrightarrow F_2$. Тогда по тавтологии теоремы 3.3, *п* заключаем: формула $F_2 \leftrightarrow F_1$ принимает всегда те же самые значения, что и формула $F_1 \leftrightarrow F_2$, т.е. только истинные значения. Следовательно, $\models F_2 \leftrightarrow F_1$, или (по признаку равносильности) $F_2 \equiv F_1$. Симметричность доказана.

Наконец, если $F_1 \equiv F_2$ и $F_2 \equiv F_3$, т.е. $\models F_1 \leftrightarrow F_2$ и $\models F_2 \leftrightarrow F_3$, то на основании определения конъюнкции заключаем, что: $\models (F_1 \leftrightarrow F_2) \wedge (F_2 \leftrightarrow F_3)$. Привлекая теперь тавтологию из теоремы 3.3, *р* и правило заключения для получения тавтологий (теорема 3.5), получаем $\models F_1 \leftrightarrow F_3$, или (по теореме 4.2) $F_1 \equiv F_3$. Следовательно, отношение $\equiv$ транзитивно.

Таким образом, отношение $\equiv$ есть отношение эквивалентности, что и требовалось доказать. $\square$

Как и всякое отношение эквивалентности, отношение $\equiv$ разбивает множество, на котором оно задано, на непересекающиеся классы эквивалентных элементов. В данном случае множество всех формул алгебры высказываний распадается на попарно непересекающиеся классы, в каждом из которых находятся равносильные между собой формулы. Один класс, например, образуют все тавтологии, другой — все тождественно ложные формулы; имеется и много других классов.

Примеры равносильных формул. В теореме 4.4 перечисляются некоторые основные равносильности. Они получаются из тавтологий, приведенных в теоремах 3.1 — 3.4, на основании признака равносильности формул.

Теорема 4.4. *Справедливы следующие равносильности :*

- а) $\neg\neg P \equiv P$;
- б) $P \rightarrow Q \equiv \neg Q \rightarrow \neg P$;
- в) $P \leftrightarrow Q \equiv \neg P \leftrightarrow \neg Q$;
- г) $P \rightarrow (Q \rightarrow R) \equiv (P \wedge Q) \rightarrow R$;
- д) $(P \rightarrow R) \wedge (Q \rightarrow R) \equiv (P \vee Q) \rightarrow R$;
- е) $P \wedge P \equiv P$;
- ж) $P \vee P \equiv P$;
- з) $P \wedge Q \equiv Q \wedge P$;
- и) $P \vee Q \equiv Q \vee P$;
- к) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$;
- л) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$;
- м) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$;
- н) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$;
- о) $P \wedge (P \vee Q) \equiv P$;
- п) $P \vee (P \wedge Q) \equiv P$;
- р) $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ (1-й закон де Моргана);
- с) $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ (2-й закон де Моргана);
- т) $P \leftrightarrow Q \equiv Q \leftrightarrow P$;
- у) $P \rightarrow Q \equiv \neg P \vee Q$;
- ф) $P \rightarrow Q \equiv \neg(P \wedge \neg Q)$;
- х) $P \wedge Q \equiv \neg(P \rightarrow \neg Q)$;
- ц) $P \vee Q \equiv \neg P \rightarrow Q$;
- ч) $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$;
- ш) $P \vee \neg P \equiv 1, P \wedge \neg P \equiv 0$;
- щ) $P \vee 1 \equiv 1, P \wedge 1 \equiv P$;
- ы) $P \vee 0 \equiv P, P \wedge 0 \equiv 0$.

Сформулируем и докажем лемму о замене, которая служит основанием для равносильных преобразований и упрощения формул.

Лемма 4.5 (о замене). *Если $G(Y_1, \dots, Y_s) \equiv H(Y_1, \dots, Y_s)$, то для любой формулы алгебры высказываний $F(X_1, \dots, X_{i-1}, Y, X_{i+1}, \dots, X_n)$ имеет место равносильность $F(X_1, \dots, X_{i-1}, G(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n) \equiv F(X_1, \dots, X_{i-1}, H(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n)$.*

Другими словами, если в формуле некоторую ее подформулу заменить на равносильную ей формулу, то полученная формула будет равносильна исходной.

Доказательство. Поскольку формулы $G(Y_1, \dots, Y_s)$ и $H(Y_1, \dots, Y_s)$ принимают всегда одинаковые значения при одинаковых значениях пропозициональных переменных $Y_1, \dots, Y_s$, то формулы

$$\begin{aligned} & F(X_1, \dots, X_{i-1}, G(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n) \\ \text{и} & F(X_1, \dots, X_{i-1}, H(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n) \end{aligned}$$

принимают одинаковые значения при любых одинаковых наборах значений переменных $X_1, \dots, X_n, Y_1, \dots, Y_s$. Следовательно,

$$\begin{aligned} & \models F(X_1, \dots, X_{i-1}, G(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n) \leftrightarrow \\ & \leftrightarrow F(X_1, \dots, X_{i-1}, H(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n), \end{aligned}$$

т.е. $F(X_1, \dots, X_{i-1}, G(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n) \equiv F(X_1, \dots, X_{i-1}, H(Y_1, \dots, Y_s), X_{i+1}, \dots, X_n)$, что и требовалось доказать. $\square$

Например, на основании этой леммы и равносильности из теоремы 4.4, n , формула $(\neg X_1 \rightarrow (Y_1 \vee (Y_1 \wedge Y_2))) \vee X_2$ равносильна формуле $(\neg X_1 \rightarrow Y_1) \vee X_2$.

Общая формулировка леммы о замене может быть конкретизирована в соответствии с индуктивным определением формулы следующим образом. Пусть имеется формула $\neg F$. Если $F \equiv G$, то $\neg F \equiv \neg G$. Далее, пусть исходная формула имеет следующее строение: $F_1 \wedge F_2$. Если $F_1 \equiv G_1$, то $F_1 \wedge F_2 \equiv G_1 \wedge F_2$. Если, кроме того, $F_2 \equiv G_2$, то $F_1 \wedge F_2 \equiv G_1 \wedge F_2 \equiv G_1 \wedge G_2$, т.е. $F_1 \wedge F_2 \equiv G_1 \wedge G_2$. Об этом свойстве говорят, что отношение равносильности формул *стабильно* относительно операции конъюнкции. (Предыдущее свойство означает стабильность относительно отрицания.) Аналогично, отношение равносильности стабильно и относительно остальных логических операций — дизъюнкции, импликации и эквивалентности. Это означает, что если $F_1 \equiv G_1$ и $F_2 \equiv G_2$, то $F_1 \vee F_2 \equiv G_1 \vee G_2$, $F_1 \rightarrow F_2 \equiv G_1 \rightarrow G_2$, $F_1 \leftrightarrow F_2 \equiv G_1 \leftrightarrow G_2$.

Равносильные преобразования формул. Используя лемму о замене и приведенные в теореме 4.4 равносильности, можем от одной формулы переходить к равносильной ей формуле. Такой переход называется *равносильным преобразованием* исходной формулы. Равносильные преобразования формул применяются прежде всего для упрощения формул.

Пример 4.6. Упростим формулу $\neg(X_1 \rightarrow \neg X_2) \wedge \neg(X_2 \rightarrow \neg X_1)$, используя равносильности из теоремы 4.4: $\neg(X_1 \rightarrow \neg X_2) \wedge \neg(X_2 \rightarrow \neg X_1) \equiv \neg(\neg X_1 \vee \neg X_2) \wedge \neg(\neg X_2 \vee \neg X_1) \equiv \neg(\neg X_1 \vee \neg X_2) \wedge \neg(\neg X_1 \vee \neg X_2) \equiv \neg(\neg X_1 \vee \neg X_2) \equiv \neg\neg X_1 \wedge \neg\neg X_2 \equiv X_1 \wedge X_2$.

Равносильные преобразования формул применяются также для приведения формул к специальному виду или к специальной форме (к так называемой совершенной нормальной форме), имеющей исключительно важное значение как в самой алгебре высказываний, так и в ее приложениях. Об этом речь пойдет в следующем параграфе.

Замечание 4.7. Отметим, что если некоторая формула является тавтологией, то и всякая равносильная ей формула также является тавтологией:

$$\models F \text{ и } F \equiv H \Rightarrow \models H.$$

Сделанное замечание позволяет обнаружить еще одну сферу применения равносильных преобразований: доказательство тожде-

ственной истинности тех или иных формул. Для этого данную формулу нужно равносильными преобразованиями свести к формуле, очевидно, являющейся тавтологией (см. Задачник, № 1.60, 1.61).

Равносильности в логике и тождества в алгебре. Можно провести параллель между понятием логической равносильности формул в алгебре высказываний и известным понятием тождества школьной алгебры. Равносильность формул $F(X_1, \dots, X_n)$ и $H(X_1, \dots, X_n)$ — это не что иное, как их тождественное равенство с точки зрения школьной алгебры, с той лишь разницей, что тождественность рассматривается относительно различных базисных множеств: в школьной алгебре — относительно множества R всех вещественных чисел, а в алгебре логики — относительно двухэлементного множества $\{0, 1\}$.

В школьной алгебре	В алгебре логики
Тождественное равенство (тождество) $(a + b)^2 \equiv a^2 + 2ab + b^2$ означает, что выражения в левой и правой его частях принимают одинаковые значения при <i>всех</i> значениях вещественных переменных $a, b \in R$	Равносильность $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ означает, что левая и правая его части принимают одинаковые логические значения при <i>всех</i> значениях пропозициональных переменных $P, Q \in \{0, 1\}$

Ввиду конечности базисного множества алгебры логики проверить справедливость той или иной равносильности можно механическим перебором всех возможных наборов значений (пропозициональных) переменных, входящих в равносильность, и вычислением на них значений левой и правой частей равносильности. В школьной алгебре бесконечность базисного множества R не позволяет доказать ни одно тождество методом перебора всех значений входящих в него переменных. Для этого разработан метод тождественных преобразований алгебраических выражений, опирающийся на основные свойства арифметических операций над вещественными числами. Этими свойствами являются перестановочность (коммутативность) и сочетательность (ассоциативность) сложения и умножения, распределительность (дистрибутивность) умножения относительно сложения и т. п. Правда, ввиду нестрогости введения понятия вещественного числа в школьном курсе математики сами эти свойства принимаются без доказательства.

Подобно тому как в школьной алгебре понятие тождества (тождественного равенства) приводит к понятию тождественного преобразования алгебраических выражений, так в алгебре логики понятие равносильности формул естественным образом приводит к понятию равносильного преобразования формул логики высказываний. Здесь важно уяснить, что равносильные преобразования формул основываются на лемме 4.5 о замене. Равносиль-

ные преобразования используют основные равносильности, приведенные в теореме 4.4.

Полезно сравнить свойства логических операций, выраженные в основных равносильностях, со свойствами арифметических операций, помня, что некоторые логические операции имеют претензии на аналогию с некоторыми арифметическими операциями. Так, конъюнкция нередко называется логическим умножением, а дизъюнкция — логическим сложением. Наиболее разительны отличия в следующих свойствах: идемпотентность конъюнкции и дизъюнкции (это означает, что невозможны степени и «умножения» на натуральные числа), дистрибутивность дизъюнкции относительно конъюнкции, законы поглощения. Таким образом, мы приходим к некоей новой алгебре, необычной по сравнению со школьной алгеброй, основанной на вещественных числах. Это и есть алгебра логики или алгебра высказываний. Равносильные преобразования в ней, как и в школьной алгебре, предназначены для приведения логических выражений (формул) к определенному виду.

§ 5. Нормальные формы для формул алгебры высказываний

Для каждой формулы алгебры высказываний можно указать равносильную ей формулу, содержащую из логических связок лишь отрицание, конъюнкцию и дизъюнкцию. Для этого нужно, используя равносильности теоремы 4.4, $\neg$, $\wedge$, выразить все имеющиеся в формуле импликации и эквивалентности через отрицание, конъюнкцию и дизъюнкцию. Так, для формулы $(\neg X \wedge (X \rightarrow Y)) \rightarrow Y$ равносильной ей формулой, не содержащей логических связок $\rightarrow$ и $\leftrightarrow$, будет, например, формула $\neg(\neg X \wedge (\neg X \vee Y)) \vee Y$. Выразить данную формулу через отрицание, конъюнкцию и дизъюнкцию возможно не одним способом, а многими. К примеру, рассматриваемая формула равносильна также следующим формулам, содержащим из логических связок лишь $\neg$, $\wedge$ и $\vee$: $\neg\neg X \vee Y$, $X \vee Y$, $(X \vee Y) \wedge (\neg Y \vee Y)$, $(X \wedge \neg Y) \vee Y$, $(X \wedge \neg Y) \vee ((X \vee \neg X) \wedge Y)$, $(X \wedge \neg Y) \vee (X \wedge Y) \vee (\neg X \wedge Y)$. Среди всевозможных выражений данной формулы через конъюнкцию, дизъюнкцию и отрицание некоторые играют важную роль как в алгебре высказываний, так и в ее приложениях. Рассмотрение таких выражений, называемых *совершенными нормальными формами*, и составляет цель настоящего параграфа.

Понятие нормальных форм. Конъюнктивным одночленом от переменных $X_1, X_2, \dots, X_n$ называется конъюнкция этих переменных или их отрицаний. Здесь «или» употребляется в неисключающем смысле, т.е. в конъюнктивный одночлен может входить одновременно и переменная, и ее отрицание. Приведем несколько при-

меров конъюнктивных одночленов: $X_1 \wedge X_1$, $X_1 \wedge \neg X_2 \wedge X_3$, $X_2 \wedge \neg X_1 \wedge X_3 \wedge \neg X_2 \wedge X_5$, $X_1 \wedge X_2 \wedge \neg X_1 \wedge X_3 \wedge X_1$ ¹.

Дизъюнктивным одночленом от переменных $X_1, X_2, \dots, X_n$ называется дизъюнкция этих переменных или их отрицаний (и здесь союз «или» употребляется в неисключающем смысле). Приведем примеры дизъюнктивных одночленов: $\neg X_1 \vee X_2 \vee X_3$, $X_2 \vee X_2$, $X_1 \vee \vee X_2 \vee \neg X_3 \vee \neg X_1 \vee X_4 \vee X_2$, $\neg X_2 \vee X_1 \vee \neg X_4 \vee X_1 \vee X_4$ ².

Дизъюнктивной нормальной формой называется дизъюнкция конъюнктивных одночленов, т. е. выражение вида $K_1 \vee K_2 \vee \dots \vee K_p$, где все K_i , $i = 1, 2, \dots, p$, являются конъюнктивными одночленами (не обязательно различными). Аналогично *конъюнктивной нормальной формой* называется конъюнкция дизъюнктивных одночленов $D_1 \wedge D_2 \wedge \dots \wedge D_q$, где все D_j , $j = 1, 2, \dots, q$, являются дизъюнктивными одночленами (не обязательно различными). Будем также называть дизъюнктивной (конъюнктивной) нормальной формой указанные выражения при $p = 1$ ($q = 1$).

Нормальную форму, представляющую формулу F (т. е. равносильную F), будем называть просто *нормальной формой этой формулы*.

Нетрудно понять, что всякая формула обладает как дизъюнктивной, так и конъюнктивной нормальными формами. В самом деле, всякую формулу можно выразить через конъюнкцию, дизъюнкцию и отрицание. Используя законы де Моргана (теорема 4.4, p, c) и свойство дистрибутивности конъюнкции относительно дизъюнкции (теорема 4.4, m), можем преобразовать равносильным образом полученное выражение к дизъюнкции конъюнктивных одночленов (к дизъюнктивной нормальной форме). Если же к исходному выражению применить свойство дистрибутивности дизъюнкции относительно конъюнкции (теорема 4.4, n), то его можно свести к конъюнкции дизъюнктивных одночленов (к конъюнктивной нормальной форме).

Очевидно, что у данной формулы F существует неограниченно много как дизъюнктивных, так и конъюнктивных нормальных форм. Одни из них более громоздкие и сложные, другие — более простые (см. Задачник, № 2.1, 2.2).

Здесь мы можем продолжить до некоторого момента аналогию со школьной алгеброй. В школьной алгебре выражения типа ax , $ху$, $(a + b)uv$ (последнее действие в них — умножение) называются одночленами, а выражения типа $a + b$, $ax + b$, $xy + uv + p$ (последнее действие — сложение) называются многочленами. В алгебре логики логическое умножение (конъюнкция) и логическое сложение (дизъюнкция) равноправны по своим свойствам. Поэтому выражения типа $X \wedge Y$, $X \wedge Y \wedge Z$ называются конъюнктивными одночленами, а выражения типа $X \vee Y$, $X \vee Y \vee Z$ —

¹ Ввиду ассоциативности конъюнкции и дизъюнкции (теорема 4.4, k, l) скобки внутри каждого из данных одночленов не пишутся.

² См. предыдущую сноску.

дизъюнктивными одночленами. Образования из одночленов выражений типа $(X \wedge Y) \vee (P \wedge Q \wedge R)$, $(P \vee Q) \wedge (X \vee Y \vee Z)$ называются не многочленами, а нормальными формами. На этом аналогия заканчивается. Далее вводятся понятия совершенных нормальных форм — дизъюнктивной и конъюнктивной.

Совершенные нормальные формы. Среди множества дизъюнктивных (равно как и конъюнктивных) нормальных форм, которыми обладает данная формула алгебры высказываний, существует уникальная форма: она единственна для данной формулы. Это так называемая совершенная дизъюнктивная нормальная форма (среди конъюнктивных форм — совершенная конъюнктивная нормальная форма).

Определение 5.1. Одночлен (конъюнктивный или дизъюнктивный) от переменных $X_1, X_2, \dots, X_n$ называется *совершенным*, если в него от каждой пары $X_i, \neg X_i$ ($i = 1, 2, \dots, n$) входит только один представитель (X_i или $\neg X_i$). Нормальная форма (дизъюнктивная или конъюнктивная) от переменных $X_1, X_2, \dots, X_n$ называется *совершенной* от этих переменных, если в нее входят лишь совершенные одночлены (конъюнктивные или дизъюнктивные соответственно) от $X_1, X_2, \dots, X_n$.

Приведем пример совершенной конъюнктивной нормальной формы от четырех переменных X_1, X_2, X_3, X_4 : $(X_1 \vee X_2 \vee X_3 \vee X_4) \wedge \wedge (\neg X_1 \vee X_2 \vee \neg X_3 \vee X_4) \wedge (X_1 \vee \neg X_2 \vee \neg X_3 \vee X_4)$. Вот несколько примеров совершенных дизъюнктивных нормальных форм: $(X \wedge Y) \vee \vee (\neg X \wedge Y) \vee (X \wedge \neg Y)$, $(X \wedge Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y \wedge Z) \vee (X \wedge \neg Y \wedge \neg Z) \vee (X \wedge Y \wedge Z)$, $(X_1 \wedge X_2 \wedge X_3 \wedge X_4) \vee (\neg X_1 \wedge \neg X_2 \wedge X_3 \wedge X_4) \vee (X_1 \wedge X_2 \wedge \neg X_3 \wedge X_4)$.

Представление формул алгебры высказываний совершенными дизъюнктивными нормальными (СДН) формами. Введем обозначение, которое будет удобно в дальнейшем:

$$X^\alpha = \begin{cases} X, & \text{если } \alpha = 1, \\ \neg X, & \text{если } \alpha = 0. \end{cases}$$

Легко проверить, что $0^0 = 1$, $0^1 = 0$, $1^0 = 0$, $1^1 = 1$, т.е. $X^\alpha = 1$ тогда и только тогда, когда $X = \alpha$, и $X^\alpha = 0$ тогда и только тогда, когда $X \neq \alpha$ (см. пояснения о значении формулы перед теоремой 2.2).

Введем еще одно обозначение. Вместо дизъюнкции $X_1 \vee X_2 \vee \dots \vee X_n$ будем писать $\bigvee_{i=1}^n X_i$. В частности, запись $\bigvee_{(\alpha_1, \alpha_2, \dots, \alpha_n)} H(X_1, \dots, X_n, \alpha_1, \dots, \alpha_n)$ обозначает дизъюнкцию всевозможных выражений (формул) $H(X_1, \dots, X_n, \alpha_1, \dots, \alpha_n)$, зависящих от переменных $X_1, \dots, X_n$, когда индексы суммирования (дизъюнктивирования) $\alpha_1, \dots, \alpha_n$ пробегают всевозможные упорядоченные наборы длины n , составленные из нулей и единиц. Например, $\bigvee_{(\alpha, \beta)} (X^\alpha \wedge X^\beta) = (X^0 \wedge Y^0) \vee (X^0 \wedge Y^1) \vee (X^1 \wedge Y^0) \vee (X^1 \wedge Y^1) = (\neg X \wedge \neg Y) \vee (\neg X \wedge Y) \vee (X \wedge \neg Y) \vee (X \wedge Y)$.

Лемма 5.2. Для всякой формулы алгебры высказываний $F(X_1, X_2, \dots, X_n)$ справедливо разложение

$$F(X_1, X_2, \dots, X_n) \equiv \bigvee_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (F(\alpha_1, \alpha_2, \dots, \alpha_n) \wedge X_1^{\alpha_1} \wedge X_2^{\alpha_2} \wedge \dots \wedge X_n^{\alpha_n}).$$

Доказательство. Возьмем произвольный набор из нулей и единиц $\xi_1, \xi_2, \dots, \xi_n$ (каждое ξ_i , где $1 \leq i \leq n$, есть либо 0, либо 1) и вычислим значения формул, стоящих в правой и левой частях доказываемой равносильности, при $X_1 = \xi_1, X_2 = \xi_2, \dots, X_n = \xi_n$.

С одной стороны, в правой части доказываемого равенства получим

$$\bigvee_{(\alpha_1, \alpha_2, \dots, \alpha_n)} (F(\alpha_1, \alpha_2, \dots, \alpha_n) \wedge \xi_1^{\alpha_1} \wedge \xi_2^{\alpha_2} \wedge \dots \wedge \xi_n^{\alpha_n}),$$

что представляет собой дизъюнкцию нескольких конъюнктивных одночленов. Каждый конъюнктивный одночлен характеризуется индексным набором нулей и единиц $\alpha_1, \alpha_2, \dots, \alpha_n$. Если для данного конъюнктивного одночлена набор $\alpha_1, \alpha_2, \dots, \alpha_n$ нулей и единиц таков, что $\alpha_1 \neq \xi_1$, или $\alpha_2 \neq \xi_2, \dots$, или $\alpha_n \neq \xi_n$, то согласно определению формулы X^α , введенному в начале пункта, будем иметь или $\xi_1^{\alpha_1} = 0$, или $\xi_2^{\alpha_2} = 0, \dots$, или $\xi_n^{\alpha_n} = 0$. Но тогда и весь данный конъюнктивный одночлен будет равен нулю и потому на результат дизъюнкции влияния не окажет, а значит, из числа дизъюнктивных «слагаемых» может быть безболезненно исключен. Только один конъюнктивный одночлен окажется не равным нулю — тот, что характеризуется таким набором $(\alpha_1, \alpha_2, \dots, \alpha_n)$, который равен взятому в начале набору $(\xi_1, \xi_2, \dots, \xi_n)$, т.е. для которого $\alpha_1 = \xi_1, \alpha_2 = \xi_2, \dots, \alpha_n = \xi_n$. Только для этого конъюнктивного одночлена будем иметь $F(\alpha_1, \alpha_2, \dots, \alpha_n) \wedge \xi_1^{\alpha_1} \wedge \xi_2^{\alpha_2} \wedge \dots \wedge \xi_n^{\alpha_n} = F(\xi_1, \xi_2, \dots, \xi_n) \wedge \xi_1^{\xi_1} \wedge \xi_2^{\xi_2} \wedge \dots \wedge \xi_n^{\xi_n} = F(\xi_1, \xi_2, \dots, \xi_n) \wedge 1 \wedge 1 \wedge \dots \wedge 1 = F(\xi_1, \xi_2, \dots, \xi_n)$. Таким образом, конъюнктивный одночлен, соответствующий индексному набору $(\xi_1, \xi_2, \dots, \xi_n)$, равен $F(\xi_1, \xi_2, \dots, \xi_n)$. Этому же значению равна и вся дизъюнкция, потому что, как показано выше, все остальные конъюнктивные одночлены равны нулю.

С другой стороны, формула, стоящая в левой части доказываемого равенства, обратится при $X_1 = \xi_1, X_2 = \xi_2, \dots, X_n = \xi_n$ в то же самое значение $F(\xi_1, \xi_2, \dots, \xi_n)$. Набор нулей и единиц $\xi_1, \xi_2, \dots, \xi_n$ был выбран произвольно. Следовательно, формулы в левой и правой частях равносильности действительно равносильны. Лемма доказана. $\square$

Теорема 5.3 (о представлении формул алгебры высказываний совершенными дизъюнктивными нормальными формулами). Каждая не тождественно ложная формула алгебры высказываний от n аргументов имеет единственную (с точностью до перестановки дизъюнктивных членов) совершенную дизъюнктивную нормальную форму.

Доказательство. Существование. Всякая формула $F(X_1, X_2, \dots, X_n)$ обладает указанным в предыдущей лемме разложением.

Поскольку формула $F(X_1, X_2, \dots, X_n)$ не тождественно ложна, то существуют такие наборы $(\alpha_1, \alpha_2, \dots, \alpha_n)$ нулей и единиц, что $F(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$. Наборы $(\alpha_1, \alpha_2, \dots, \alpha_n)$, обращающие формулу F в нуль, будут обращать в нуль также и конъюнктивные одночлены, входящие в дизъюнкцию и соответствующие данным индексным наборам. Поэтому все такие одночлены исключим из дизъюнкции. Итак, в дизъюнкции остаются конъюнктивные одночлены, соответствующие лишь индексным наборам $(\alpha_1, \alpha_2, \dots, \alpha_n)$ нулей и единиц, для которых $F(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$. Тогда разложение для формулы F принимает следующий вид:

$$\begin{aligned} F(X_1, X_2, \dots, X_n) &\equiv \bigvee ((F(\alpha_1, \alpha_2, \dots, \alpha_n) \wedge X_1^{\alpha_1} \wedge X_2^{\alpha_2} \wedge \dots \wedge X_n^{\alpha_n})) \equiv \\ &\quad (\alpha_1, \alpha_2, \dots, \alpha_n) \\ F(\alpha_1, \alpha_2, \dots, \alpha_n) &= 1 \\ &\equiv \bigvee (X_1^{\alpha_1} \wedge X_2^{\alpha_2} \wedge \dots \wedge X_n^{\alpha_n}), \\ F(\alpha_1, \alpha_2, \dots, \alpha_n) &= 1 \end{aligned}$$

где дизъюнкция («суммирование») ведется по всем индексным наборам $(\alpha_1, \alpha_2, \dots, \alpha_n)$ нулей и единиц, для которых $F(\alpha_1, \alpha_2, \dots, \alpha_n) = 1$. Выражение, стоящее в правой части полученной равносильности, есть не что иное, как совершенная дизъюнктивная нормальная форма от переменных $X_1, X_2, \dots, X_n$, потому что каждый конъюнктивный одночлен $X_1^{\alpha_1} \wedge X_2^{\alpha_2} \wedge \dots \wedge X_n^{\alpha_n}$, входящий в дизъюнкцию, совершенен (каждая переменная $X_1, X_2, \dots, X_n$ входит в него точно один раз: либо сама, либо со знаком отрицания в зависимости от значения ее показателя степени).

Единственность. Предположим, что некоторая формула $F(X_1, X_2, \dots, X_n)$ имеет два представления совершенными дизъюнктивными нормальными формами:

$$\begin{aligned} F(X_1, X_2, \dots, X_n) &\equiv K_1 \vee K_2 \vee \dots \vee K_q; \\ F(X_1, X_2, \dots, X_n) &\equiv K_1^* \vee K_2^* \vee \dots \vee K_r^*, \end{aligned}$$

где $K_i, 1 \leq i \leq q$, и $K_j^*, 1 \leq j \leq r$, есть совершенные конъюнктивные одночлены от переменных $X_1, X_2, \dots, X_n$. Причем, не нарушая общности, считаем, что ни один из одночленов $K_1, K_2, \dots, K_q$ не повторяется в этом наборе, потому что повторяющиеся одночлены можно исключить ввиду идемпотентности дизъюнкции (теорема 4.4, ж). Аналогична ситуация в форме $K_1^* \vee K_2^* \vee \dots \vee K_r^*$. Тогда имеет место равносильность $K_1 \vee K_2 \vee \dots \vee K_q \equiv K_1^* \vee K_2^* \vee \dots \vee K_r^*$. Пусть, например, совершенный конъюнктивный одночлен K_1 имеет вид $K_1 \equiv (X_1^{\alpha_1} \wedge X_2^{\alpha_2} \wedge \dots \wedge X_n^{\alpha_n})$. Придадим переменным $X_1, X_2, \dots, X_n$ значения $\alpha_1, \alpha_2, \dots, \alpha_n$ соответственно. Тогда совершенный конъюнктивный одночлен K_1 примет значение 1, и, следовательно, вся совершенная дизъюнктивная нормальная форма, стоящая в левой части равносильности, станет равна единице. Тогда

и правая часть данной равносильности обратится в единицу, и для набора $\alpha_1, \alpha_2, \dots, \alpha_n$ значений переменных одна из совершенных элементарных конъюнкций K^* , например K_j^* , также станет равной единице. Если K_j^* имеет вид $K_j^* \equiv (X_1^{\beta_1} \wedge X_2^{\beta_2} \wedge \dots \wedge X_n^{\beta_n})$, то доказанное означает, что $\alpha_1^{\beta_1} \wedge \alpha_2^{\beta_2} \wedge \dots \wedge \alpha_n^{\beta_n} = 1$. Последнее равенство возможно в том и только в том случае, когда $\alpha_1^{\beta_1} = 1$, $\alpha_2^{\beta_2} = 1$, ..., $\alpha_n^{\beta_n} = 1$, что может быть лишь тогда и только тогда, когда $\beta_1 = \alpha_1$, $\beta_2 = \alpha_2$, ..., $\beta_n = \alpha_n$. Следовательно, $K_j^* \equiv (X_1^{\alpha_1} \wedge X_2^{\alpha_2} \wedge \dots \wedge X_n^{\alpha_n})$, т.е. $K_j^* = K_1$. Таким образом, совершенная элементарная конъюнкция K_1 встречается среди совершенных элементарных конъюнкций $K_1^*, K_2^*, \dots, K_r^*$. Тем же самым способом устанавливается, что любая из совершенных элементарных конъюнкций $K_1, K_2, \dots, K_q$ встречается среди $K_1^*, K_2^*, \dots, K_r^*$, и обратно, любая из совершенных элементарных конъюнкций $K_1^*, K_2^*, \dots, K_r^*$ встречается среди $K_1, K_2, \dots, K_q$. Ввиду того что одночлены в данных наборах не повторяются, то $q = r$ и обе части равносильности $K_1 \vee K_2 \vee \dots \vee K_q \equiv K_1^* \vee K_2^* \vee \dots \vee K_r^*$ отличаются самое большее порядком членов дизъюнкции. $\square$

Доказанная теорема — одна из важнейших в алгебре высказываний. Если вы до конца разобрали обе части доказательства (существование и единственность), то значит вы *начали* понимать категории и методы математической логики как математической науки. Доказательство существования состоит из двух частей: леммы и собственно теоремы. Доказательство единственности полностью содержится в теореме и не опирается на лемму.

Представление формул алгебры высказываний совершенными конъюнктивными нормальными (СКН) формами. Понятия и теоремы этого пункта носят двойственный характер по отношению к соответствующим понятиям и теоремам предыдущего пункта. Вводится следующее обозначение:

$${}^{\beta}X = \begin{cases} \neg X, & \text{если } \beta = 1, \\ X, & \text{если } \beta = 0. \end{cases}$$

Легко проверяется, что ${}^0 0 = 0$, ${}^1 0 = 1$, ${}^0 1 = 1$, ${}^1 1 = 0$, т.е. ${}^{\beta}X = 1$ тогда и только тогда, когда $X \neq \beta$; и ${}^{\beta}X = 0$ тогда и только тогда, когда $X = \beta$.

Вместо конъюнкции $X_1 \wedge X_2 \wedge \dots \wedge X_n$ будем писать $\bigwedge_{i=1}^n X_i$. В частности, запись $\bigwedge_{(\beta_1, \dots, \beta_n)} H(X_1, \dots, X_n, \beta_1, \dots, \beta_n)$ обозначает дизъюнкцию всевозможных выражений (формул) $H(X_1, \dots, X_n, \beta_1, \dots, \beta_n)$, зависящих от переменных $X_1, \dots, X_n$, когда индексы произведения (конъюнктирования) $\beta_1, \dots, \beta_n$ пробегают всевозможные упорядоченные наборы длины n , составленные из нулей и единиц. Например, $\bigwedge_{(\alpha, \beta)} ({}^{\alpha}X \vee {}^{\beta}X) = ({}^0 X \vee {}^0 Y) \wedge ({}^0 X \vee {}^1 Y) \wedge ({}^1 X \vee {}^0 Y) \wedge ({}^1 X \vee {}^1 Y) = (X \vee Y) \wedge (X \vee \neg Y) \wedge (\neg X \vee Y) \wedge (\neg X \vee \neg Y)$.

Аналогично доказательству леммы 5.2 доказывается лемма 5.4.

Лемма 5.4. Для всякой формулы $F(X_1, X_2, \dots, X_n)$ алгебры высказываний справедливо разложение

$$F(X_1, X_2, \dots, X_n) \equiv \bigwedge_{(\beta_1, \beta_2, \dots, \beta_n)} (F(\beta_1, \beta_2, \dots, \beta_n) \vee \beta_1 X_1 \vee \beta_2 X_2 \vee \dots \vee \beta_n X_n).$$

Подобно теореме 5.3 выводится теорема 5.5.

Теорема 5.5 (о представлении формул алгебры высказываний совершенными конъюнктивными нормальными формами). *Каждая формула алгебры высказываний от n переменных, не являющаяся тавтологией, имеет единственную (с точностью до перестановки конъюнктивных членов) совершенную конъюнктивную нормальную форму.*

Доказательство этой теоремы можно восстановить, руководствуясь доказательством теоремы 5.3.

Два способа приведения формулы алгебры высказываний к совершенной нормальной форме. Эти два способа проистекают из двух способов задания формулы алгебры высказываний: с помощью таблицы ее значений или с помощью аналитической формы записи.

Если формула задана таблицей своих значений, то из доказательств теорем 5.3 и 5.5 о представлении формул совершенными нормальными формами необходимо вынести формулу (в некоем обычном понимании смысла этого термина) разложения формулы алгебры высказываний в совершенную нормальную форму. Для случая СДН-формы эта формула имеет следующий вид:

$$F(X_1, \dots, X_n) \equiv \bigvee (X_1^{\alpha_1} \wedge \dots \wedge X_n^{\alpha_n}), \text{ где } X^\alpha = \begin{cases} X, & \text{если } \alpha = 1, \\ \neg X, & \text{если } \alpha = 0. \end{cases}$$

$$F(\alpha_1, \dots, \alpha_n) = 1$$

По сути, эта формула описывает **правило (алгоритм) отыскания совершенной дизъюнктивной нормальной формы для данной формулы**: нужно выбрать все те наборы значений ее переменных, на которых формула принимает значение 1; для каждого такого набора выписать совершенный конъюнктивный одночлен, принимающий значение 1 на этом наборе и только на нем; полученные совершенные конъюнктивные одночлены соединить знаками дизъюнкции (см. Задачник, № 2.6, л). Для случая СКН-формы эта формула имеет вид

$$F(X_1, \dots, X_n) \equiv \bigwedge_{(\beta_1, \dots, \beta_n)} (F(\beta_1, \dots, \beta_n) \vee \beta_1 X_1 \vee \dots \vee \beta_n X_n), \text{ где } \beta X = \begin{cases} X, & \text{если } \beta = 0 \\ \neg X, & \text{если } \beta = 1. \end{cases}$$

$$F(\beta_1, \dots, \beta_n) = 0$$

и, в свою очередь, описывает следующее **правило (алгоритм) отыскания совершенной конъюнктивной нормальной формы для данной формулы**: нужно выбрать все те наборы значений ее переменных, на которых формула принимает значение 0. Для каждого такого набора

выписать совершенный дизъюнктивный одночлен, принимающий значение 0 на этом наборе и только на нем. Полученные совершенные дизъюнктивные одночлены соединить знаками конъюнкции (см. Задачник, № 2.9, л).

Пример 5.6. Пусть, например, формула $F(X, Y, Z)$ задана следующей таблицей своих значений:

X	Y	Z	$F(X, Y, Z)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Таким образом, она принимает значения 1 на следующих наборах значений своих переменных (или при следующих конкретизациях): (0, 0, 0), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 1, 1). Запишем предыдущую формулу разложения в СДН-форму для случая $n = 3$ и применим ее в нашей ситуации:

$$\begin{aligned}
 F(X, Y, Z) &\equiv \bigvee (X^\alpha \wedge Y^\beta \wedge Z^\gamma) \equiv \\
 &F(\alpha, \beta, \gamma) = 1 \\
 &\equiv (X^0 \wedge Y^0 \wedge Z^0) \vee (X^0 \wedge Y^1 \wedge Z^0) \vee (X^0 \wedge Y^1 \wedge Z^1) \vee (X^1 \wedge Y^0 \wedge Z^0) \vee (X^1 \wedge Y^1 \wedge Z^1) \equiv \\
 &(\neg X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge \neg Z) \vee \\
 &\vee (\neg X \wedge Y \wedge Z) \vee (X \wedge \neg Y \wedge \neg Z) \vee (X \wedge Y \wedge Z). \quad (5.1)
 \end{aligned}$$

Пример 5.7. Для формулы $F(X, Y, Z)$ из предыдущего примера найдем ее СКН-форму. Для этого сначала отметим все те наборы значений переменных, на которых она принимает значение 0: (0, 0, 1), (1, 0, 1), (1, 1, 0). Теперь запишем формулу разложения в СКН-форму для случая $n = 3$ и применим ее в нашей ситуации:

$$\begin{aligned}
 F(X, Y, Z) &\equiv \bigwedge (\alpha X \vee \beta Y \vee \gamma Z) \equiv \\
 &F(\alpha, \beta, \gamma) = 0 \\
 &\equiv ({}^0X \vee {}^0Y \vee {}^1Z) \wedge ({}^1X \vee {}^0Y \vee {}^1Z) \wedge ({}^1X \vee {}^1Y \vee {}^0Z) \equiv \\
 &\equiv (X \vee Y \vee \neg Z) \wedge (\neg X \vee Y \vee \neg Z) \wedge (\neg X \vee \neg Y \vee Z). \quad (5.2)
 \end{aligned}$$

Еще раз обращаем внимание на то, что для каждой формулы алгебры высказываний СДН-форма единственна и СКН-форма единственна (если они существуют). СДН-форма (5.1) отмечает все те наборы значений пропозициональных переменных, на которых данная формула принимает значение 1, а СКН-форма (5.2) отме-

чает все те наборы значений пропозициональных переменных, на которых данная формула принимает значение 0. Тем не менее необходимо отчетливо осознавать, что две полученные формулы (5.1) и (5.2) равносильны. Так, формула (5.1) принимает значение 0 на тех и только тех наборах значений переменных, на которых принимает значение 0 и формула (5.2). Аналогично формула (5.2) принимает значение 1 на тех и только тех наборах значений переменных, на которых принимает значение 1 формула (5.1).

Второй способ приведения формул алгебры высказываний к совершенной нормальной форме основан на равносильных преобразованиях данной формулы. В этом случае формула должна быть задана в аналитической форме. Для приведения формулы к совершенной нормальной форме нужно сначала привести ее к дизъюнктивной (или конъюнктивной) нормальной форме. Алгоритм такого приведения подробно рассмотрен в Задачнике, № 2.1, л. 2.2, л. Затем нужно продолжить равносильные преобразования полученных нормальных форм, с тем чтобы довести их до совершенства. Примеры приведения рассмотрены в Задачнике, № 2.3, л. 2.4, л.

В заключение отметим, что одной из сфер применения нормальных форм является та, где требуется получить аналитическое выражение для формулы алгебры высказываний, которая задана своей таблицей значений (таблицей истинности), т.е. про которую известно, на каких наборах она принимает значение 0, а на каких — 1. Примеры задач приведены в Задачнике, № 2.20, 2.27 — 2.31.

§ 6. Логическое следование формул

Раздел алгебры высказываний, изучающий закономерности логического следования, логического умозаключения, является ее сердцевиной. Именно в этом разделе на данном уровне развития математической логики решается основная задача логики, состоящая в нахождении общих способов установления связей логических значений одних высказываний с логическими значениями других высказываний на основании исследования *формальной структуры* высказываний. Одно из важнейших предназначений логики состоит в том, чтобы устанавливать, что из чего следует, т.е. устанавливать структуры высказываний, связанных отношением логического следования (часть общего назначения математики, по выражению Н.Винера, «находить порядок в хаосе, который нас окружает»). Знание этих закономерностей необходимо прежде всего самой математической науке. С помощью таких знаний происходит доказательство математических теорем и, следовательно, развитие математики. Это знание важно и для других наук, для систематизации научного знания вообще; да и в повседневной жизни оно служит инструментом рассуждений, обоснований и доказательств.

Понятие логического следствия. Когда говорят, что из одного или нескольких предложений $A_1, A_2, \dots, A_m$ следует предложение B , то подразумевают следующее: всякий раз, когда окажутся истинными все предложения $A_1, A_2, \dots, A_m$, истинным будет и предложение B . Вот примеры таких следований: «Если летом я устроюсь на временную работу (утверждение A), то у меня будут заработанные деньги (утверждение B)», «Если у меня будут заработанные деньги (утверждение B), то я куплю видеоманитофон (утверждение C)», «Если днем я не приготовлю уроки на завтра (утверждение A_1), и если вечером я пойду в кино (утверждение A_2), то завтра я буду не готов к занятиям (утверждение D)». Установление справедливости приведенных суждений не относится к компетенции математической логики, а осуществляется на основе анализа их содержания и смысла.

Задача математической логики (в частности, алгебры высказываний) в вопросах логического следования состоит в том, чтобы указать такие формы высказываний $A_1, A_2, \dots, A_m, B$, когда последнее высказывание непременно было бы следствием m первых, независимо от конкретного содержания всех этих высказываний. Формы высказываний выражаются, как нам известно, формулами алгебры высказываний. Итак, теория логического следования (в рамках алгебры высказываний) должна изучать закономерности образования формул $F_1, F_2, \dots, F_m, H$, по которым первые m из них связаны с последней отношением логического следования.

Вернемся к двум первым суждениям, приведенным в начале пункта: $A \rightarrow B$ и $B \rightarrow C$. Вынесем относительно них следующее умозаключение: «Если $A \rightarrow B$ и $B \rightarrow C$, то $A \rightarrow C$ ». Формулировка данного суждения без использования математической символики будет, конечно, неуклюжа. Поэтому сформулируем его так: «Если высказывание $A \rightarrow B$ верно и высказывание $B \rightarrow C$ верно, то верно и высказывание $A \rightarrow C$ ». Нет никаких сомнений в том, что указанное суждение справедливо. Более того, мы осознаем его справедливость, даже не интересуясь содержанием простейших высказываний A, B и C . Значит, высказывание, имеющее форму $X \rightarrow Z$, следует из двух высказываний, имеющих формы $X \rightarrow Y$ и $Y \rightarrow Z$, независимо от того, каковы высказывания X, Y и Z .

Перейдем теперь к точному определению понятия логического следствия и к изучению свойств этого понятия.

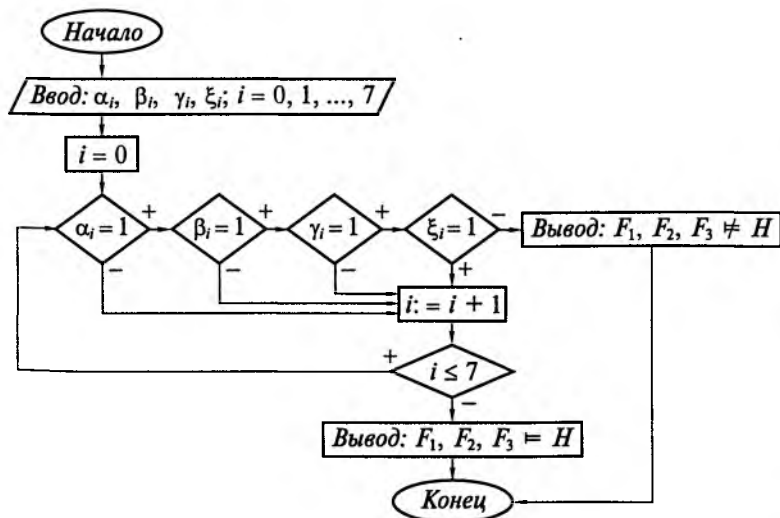
Определение 6.1. Формула $H(X_1, \dots, X_n)$ называется *логическим следствием формул* $F_1(X_1, \dots, X_n), \dots, F_m(X_1, \dots, X_n)$, если формула $H(X_1, \dots, X_n)$ превращается в истинное высказывание при всякой такой подстановке вместо всех ее пропозициональных переменных $X_1, \dots, X_n$ конкретных высказываний, при которой в истинное высказывание превращаются все формулы $F_1(X_1, \dots, X_n), \dots, F_m(X_1, \dots, X_n)$. То, что формула H является логическим следствием формул $F_1, \dots, F_m$, записывается так: $F_1, \dots, F_m = H$. Формулы $F_1, \dots, F_m$ называются *посылками* для логического следствия H .

Таким образом, $F_1, \dots, F_m = H$, если для любых высказываний $A_1, \dots, A_n$ из $\lambda(F_1(A_1, \dots, A_n)) = 1, \dots, \lambda(F_m(A_1, \dots, A_n)) = 1$ следует $\lambda(H(A_1, \dots, A_n)) = 1$. Наконец можно и так сказать о логическом следствии. Составим таблицы истинности для формул $F_1, \dots, F_m, H$. Предположим, что если в какой-то строке таблицы все формулы $F_1, \dots, F_m$ принимают значение 1, то в этой строке непременно и формула H принимает значение 1. Это и будет означать, что H является логическим следствием формул $F_1, \dots, F_m$.

Из сформулированного определения вытекает четкий алгоритм проверки формул на логическое следование (далее приводится в виде схемы). Рассмотрим его действие для случая, например, трех формул-посылок, зависящих от трех переменных: $F_1(X, Y, Z), F_2(X, Y, Z), F_3(X, Y, Z) = H(X, Y, Z)$. Все эти формулы должны быть заданы таблицей своих значений:

X	Y	Z	$F_1(X, Y, Z)$	$F_2(X, Y, Z)$	$F_3(X, Y, Z)$	$H(X, Y, Z)$
0	0	0	α_0	β_0	γ_0	ξ_0
0	0	1	α_1	β_1	γ_1	ξ_1
0	1	0	α_2	β_2	γ_2	ξ_2
0	1	1	α_3	β_3	γ_3	ξ_3
1	0	0	α_4	β_4	γ_4	ξ_4
1	0	1	α_5	β_5	γ_5	ξ_5
1	1	0	α_6	β_6	γ_6	ξ_6
1	1	1	α_7	β_7	γ_7	ξ_7

Алгоритм проверки формул на логическое следование



Алгоритм действует следующим образом. Он просматривает последовательно по строкам таблицы значений формул F_1, F_2, F_3, H . Если хотя бы один элемент нулевой строки $\alpha_0, \beta_0, \gamma_0$ равен 0, то без просмотра значения формулы H в этой строке (т.е. числа ξ_0) происходит переход к просмотру следующей строки $\alpha_1, \beta_1, \gamma_1$. Если все элементы $\alpha_0, \beta_0, \gamma_0$ нулевой строки равны 1, то просматривается значение ξ_0 формулы H в этой строке. При $\xi_0 = 0$ выдается результат: формула H не является логическим следствием формул F_1, F_2, F_3 . При $\xi_0 = 1$ происходит переход к просмотру следующей строки $\alpha_1, \beta_1, \gamma_1$. И так далее. Если после просмотра последней строки $\alpha_7, \beta_7, \gamma_7, \xi_7$ должен произойти переход к просмотру следующей строки, то это означает, что определение логического следования выполнено и формула H является логическим следствием формул F_1, F_2, F_3 .

Разберите действие этого алгоритма при решении конкретных задач на логическое следование (см. Задачник, № 1.36). Сопоставьте его с рассмотренным в § 4 алгоритмом проверки формул на равносильность.

Пример 6.2. По таблице истинности нескольких формул попытаемся определить, какие из них следуют из каких:

№ строки	$\lambda(X)$	$\lambda(Y)$	$\lambda(Z)$	$\lambda((X \wedge Y) \rightarrow \neg Z)$	$\lambda(\neg Y)$	$\lambda(X \rightarrow Z)$	$\lambda(\neg(X \wedge Y))$
1	0	0	0	1	1	1	1
2	0	0	1	1	1	1	1
3	0	1	0	1	0	1	1
4	0	1	1	1	0	1	1
5	1	0	0	1	1	0	1
6	1	0	1	1	1	1	1
7	1	1	0	1	0	0	0
8	1	1	1	0	0	1	0

Рассмотрим формулы $X, Z, (X \wedge Y) \rightarrow \neg Z, \neg Y$. Из таблицы видно, что имеется только одна строка (6-я), в которой первые три формулы принимают значение 1. В этой строке и формула $\neg Y$ также принимает значение 1. Следовательно, $X, Z, (X \wedge Y) \rightarrow \neg Z \models \neg Y$.

Теперь рассматриваем формулы $(X \wedge Y) \rightarrow \neg Z, X \rightarrow Z, \neg(X \wedge Y)$. Из таблицы видно, что имеется точно пять строк, в которых первые две формулы принимают значение 1, а именно 1-я, 2-я, 3-я, 4-я и 6-я. В этих строках третья формула также принимает значение 1. Следовательно, $(X \wedge Y) \rightarrow \neg Z, X \rightarrow Z \models \neg(X \wedge Y)$.

Предлагается, глядя на таблицу, обнаружить еще какие-нибудь логические следствия одних формул из других (см. также Задачник, № 1.34).

Признаки логического следствия. То, что некоторая формула является логическим следствием каких-то формул, можно выразить так же, сказав, что подходящая формула является тавтологией. В этом существо признаков, о которых пойдет речь в настоящем пункте, чем еще раз подчеркивается важное значение тавтологий.

Теорема 6.3 (признак логического следствия). *Формула H будет логическим следствием формулы F тогда и только тогда, когда формула $F \rightarrow H$ является тавтологией: $F \models H \Leftrightarrow \models F \rightarrow H$.*

Доказательство. Необходимость. Дано: $F(X_1, \dots, X_n) \models H(X_1, \dots, X_n)$, т.е. если для набора высказываний $A_1, \dots, A_n$ имеет место $\lambda(F(A_1, \dots, A_n)) = 1$, то $\lambda(H(A_1, \dots, A_n)) = 1$. Тогда для любого набора высказываний $A_1, \dots, A_n$ имеет место равенство $\lambda(F(A_1, \dots, A_n)) \rightarrow \lambda(H(A_1, \dots, A_n)) = 1$, поскольку равенство нулю возможно лишь в том случае, когда $\lambda(F(A_1, \dots, A_n)) = 1$ и $\lambda(H(A_1, \dots, A_n)) = 0$, но такая ситуация исключена условием. Следовательно, на основании равенства (1.4) $\lambda(F(A_1, \dots, A_n)) \rightarrow \lambda(H(A_1, \dots, A_n)) = 1$ для любых высказываний $A_1, \dots, A_n$. Это означает, что формула $F(X_1, \dots, X_n) \rightarrow H(X_1, \dots, X_n)$ — тавтология, т.е. $\models F \rightarrow H$.

Достаточность. Дано: $\models F \rightarrow H$. Тогда: $\lambda(F(A_1, \dots, A_n) \rightarrow H(A_1, \dots, A_n)) = 1$ для любых высказываний $A_1, \dots, A_n$, откуда в силу равенства (1.4) $\lambda(F(A_1, \dots, A_n)) \rightarrow \lambda(H(A_1, \dots, A_n)) = 1$. Предположим теперь, что $\lambda(F(A_1, \dots, A_n)) = 1$. Тогда: $1 \rightarrow \lambda(H(A_1, \dots, A_n)) = 1$, откуда (на основании определения 1.7) $\lambda(H(A_1, \dots, A_n)) = 1$, ибо в противном случае $1 \rightarrow 0 = 1$ — противоречие. Но это значит (по определению 6.1 логического следствия), что $F \models H$. $\square$

Следующая теорема дает признаки того, что формула является логическим следствием двух или большего количества формул.

Теорема 6.4. *Для любых формул $F_1, F_2, \dots, F_m, H$ ($m \geq 2$) следующие утверждения равносильны:*

- а) $F_1, F_2, \dots, F_m \models H$;
- б) $F_1 \wedge F_2 \wedge \dots \wedge F_m \models H$;
- в) $\models (F_1 \wedge F_2 \wedge \dots \wedge F_m) \rightarrow H$.

Доказательство. Утверждения б) и в) равносильны на основании предыдущей теоремы. Докажем равносильность утверждений а) и б).

а) $\Rightarrow$ б). Дано: $F_1, F_2, \dots, F_m \models H$. Покажем, что $F_1 \wedge F_2 \wedge \dots \wedge F_m \models H$. Пусть $A_1, \dots, A_n$ — такие конкретные высказывания, что

$$\lambda(F_1(A_1, \dots, A_n) \wedge \dots \wedge F_m(A_1, \dots, A_n)) = 1. \quad (6.1)$$

Тогда по равенству (1.2)

$$\lambda(F_1(A_1, \dots, A_n)) \wedge \dots \wedge \lambda(F_m(A_1, \dots, A_n)) = 1. \quad (6.2)$$

Отсюда по определению 1.3

$$\lambda(F_1(A_1, \dots, A_n)) = 1, \dots, \lambda(F_m(A_1, \dots, A_n)) = 1. \quad (6.3)$$

Но поскольку по условию $F_1, F_2, \dots, F_m \models H$, то отсюда следует, что $\lambda(H(A_1, \dots, A_n)) = 1$. Следовательно, $F_1 \wedge F_2 \wedge \dots \wedge F_m \models H$.

б) $\Rightarrow$ а). Дано: $F_1 \wedge F_2 \wedge \dots \wedge F_m \models H$. Покажем, что $F_1, F_2, \dots, F_m \models H$. Предположим, что справедливы все соотношения (6.3) для некоторых $A_1, \dots, A_n$. Тогда имеет место соотношение (6.2), из которого на основании равенства (1.2) приходим к соотношению (6.1). Из последнего на основании условия $F_1 \wedge F_2 \wedge \dots \wedge F_m \models H$ заключаем: $\lambda(H(A_1, \dots, A_n)) = 1$. Но это и означает, что $F_1, F_2, \dots, F_m \models H$. $\square$

Два свойства логического следования. Свойства, формулируемые в теореме 6.5, используются для доказательства того, что какая-то формула является логическим следствием некоторых формул (см. пример 6.2).

Теорема 6.5. *Отношение логического следования между формулами алгебры высказываний обладает следующими свойствами:*

а) $F_1, F_2, \dots, F_m \models F_i$, для $i = 1, 2, \dots, m$;

б) если $F_1, F_2, \dots, F_m \models G_j$ для $j = 1, 2, \dots, p$ и $G_1, G_2, \dots, G_p \models H$, то $F_1, F_2, \dots, F_m \models H$.

Доказательство. а) Фактически это свойство состоит в следующем: $F_i \models F_i$. Оно непосредственно вытекает из определения 6.1 логического следования и означает, что отношение логического следования рефлексивно.

б) В частном случае при $m = p = 1$ данное свойство утверждает: если $F \models G$ и $G \models H$, то $F \models H$. Другими словами, отношение логического следования транзитивно. Докажем исходное утверждение. Строим таблицу истинности для всех формул, указанных в утверждении б), перечислив все пропозициональные переменные $X_1, X_2, \dots, X_n$, входящие хотя бы в одну из этих формул. Рассмотрим какую-нибудь строку этой таблицы, в которой каждая формула $F_1, F_2, \dots, F_m$ получает истинностное значение, равное 1. Тогда на основании условий каждая из формул $G_1, G_2, \dots, G_p$ также принимает истинностное значение, равное 1. Следовательно, и H имеет значение 1. Таким образом, для всякого набора истинностных значений переменных $X_1, X_2, \dots, X_n$, для которого каждая формула $F_1, F_2, \dots, F_m$ принимает значение 1, формула H также принимает значение 1. Это означает, что $F_1, F_2, \dots, F_m \models H$. $\square$

Следование и равносильность формул. Если говорить о следовании из одной формулы другой, то получаем бинарное отношение на совокупности всех формул алгебры высказываний. Две формулы F и H (в указанном порядке) находятся в данном отношении, если $F \models H$.

В § 4 рассмотрены бинарные отношения равносильности на совокупности всех формул алгебры высказываний. Две формулы F и H (в указанном порядке) находятся в этом отношении, если $F \equiv H$. Там же (следствие 4.3) установлено, что отношение равносильности формул есть отношение эквивалентности. Установим взаимосвязь между отношением равносильности и отношением следования.

Теорема 6.6. Две формулы алгебры высказываний равносильны тогда и только тогда, когда каждая из них является логическим следствием другой: $F \equiv H \Leftrightarrow F = H$ и $H = F$.

Доказательство. Необходимость. Дано: $F \equiv H$. По определению равносильности обе формулы $F(X_1, \dots, X_n)$ и $H(X_1, \dots, X_n)$ для любых конкретных высказываний $A_1, \dots, A_n$ превращаются в высказывания $F(A_1, \dots, A_n)$ и $H(A_1, \dots, A_n)$, которые одновременно либо оба истинны, либо оба ложны. А раз так, то каждое из высказываний $F(A_1, \dots, A_n) \rightarrow H(A_1, \dots, A_n)$ и $H(A_1, \dots, A_n) \rightarrow F(A_1, \dots, A_n)$ истинно для любых конкретных высказываний $A_1, \dots, A_n$. Это означает, что $\models F \rightarrow H$ и $\models H \rightarrow F$, откуда, по теореме 6.3, $F = H$ и $H = F$.

Достаточность. Дано: $F = H$ и $H = F$. Тогда, по теореме 6.3, $\models F \rightarrow H$ и $\models H \rightarrow F$. Поскольку формула $F \rightarrow H$ всегда превращается в истинное высказывание и формула $H \rightarrow F$ всегда превращается в истинное высказывание, то и их конъюнкция $(F \rightarrow H) \wedge (H \rightarrow F)$ является формулой, которая превращается в истинное высказывание всегда, т.е. $\models (F \rightarrow H) \wedge (H \rightarrow F)$. Но на основании теоремы 4.4, ч, $(F \rightarrow H) \wedge (H \rightarrow F) \equiv F \leftrightarrow H$. Тогда по замечанию 4.7 $\models F \leftrightarrow H$, а по теореме 4.2 $F \equiv H$. $\square$

Замечание 6.7. Если некоторая формула является тавтологией, то и всякое ее логическое следствие также является тавтологией. Символически это можно записать так: $\models F$ и $F = H \Rightarrow \models H$.

Продумайте это утверждение самостоятельно.

Правила логических умозаключений. Теперь можем рассмотреть примеры структур правильного мышления, т.е. ответить на вопрос, что из чего следует.

Начнем с тавтологии из теоремы 3.1, к: $\models (F \wedge (F \rightarrow G)) \rightarrow G$. (На основании замечания 3.7 пропозициональные переменные P и Q заменены произвольными формулами F и G алгебры высказываний.) На основании теоремы 6.4 заключаем, что $F, F \rightarrow G \models G$. Полученную схему, или правило вывода (умозаключения), также называют правилом *modus ponens*.

Правило 6.8 (modus ponens):
$$\frac{F, F \rightarrow G}{G}$$

Это правило означает, что от утверждения об истинности посылки F с помощью другой посылки $F \rightarrow G$ переходят к утверждению об истинности следствия G . Данное правило называют также *правилом заключения* или *отделения* (от посылки $F \rightarrow G$ с помощью посылки F отделяется заключение G). По теореме 3.5 правилу 6.8 можно придать несколько иной смысл: если формулы, стоящие в числителе, являются тавтологиями, то и формула в знаменателе — также тавтология.

Не менее важное и широко применяемое в рассуждениях правило умозаключения получается на основе тавтологии теоремы 3.1, л.

Правило 6.9 (*modus tollens*): $\frac{F \rightarrow G, \neg G}{\neg F}$.

Оно называется правилом *modus tollens*: от отрицания истинности посылки G с помощью посылки $F \rightarrow G$ переходят к отрицанию истинности F .

Таким образом, рассмотренные правила вывода 6.8 и 6.9 позволяют в истинной импликации $F \rightarrow G$ из истинности посылки F делать вывод об истинности следствия G , а из ложности следствия G — о ложности посылки F .

Укажем еще некоторые правила вывода, применяемые в рассуждениях. Путь их получения состоит в том, что сначала заменяем в соответствующей тавтологии каждую пропозициональную переменную произвольной формулой алгебры высказываний, в результате чего на основании теоремы 3.6 снова получаем тавтологию, а затем от нее по теореме 6.3 переходим к соответствующему правилу вывода (умозаключения), которое и записываем в принятой форме. Так, тавтология теоремы 3.3, б дает следующее правило вывода:

Правило 6.10 (введения конъюнкции): $\frac{F, G}{F \wedge G}$.

Из тавтологий теоремы 3.2, б приходим к таким правилам вывода:

Правило 6.11 (удаления конъюнкции): $\frac{F \wedge G}{F}, \quad \frac{F \wedge G}{G}$.

Правило 6.12 (введения дизъюнкции): $\frac{F}{F \wedge G}, \quad \frac{G}{F \wedge G}$.

Смысл названий этих правил виден из характера их действия.

Из тавтологии теоремы 3.1, д получаем правило контрапозиции.

Правило 6.13 (контрапозиции): $\frac{F \rightarrow G}{\neg G \rightarrow \neg F}$.

Из тавтологии теоремы 3.1, е вытекает *правило цепного заключения* (или *правило силлогизма*).

Правило 6.14 (цепного заключения): $\frac{F \rightarrow G, G \rightarrow H}{F \rightarrow H}$.

Из тавтологии теоремы 3.1, м следует правило перестановки посылок.

Правило 6.15 (перестановки посылок): $\frac{F \rightarrow (G \rightarrow H)}{G \rightarrow (F \rightarrow H)}$.

Наконец, из тавтологии теоремы 3.1, n получаем следующие правила:

Правила 6.16 (объединения и разъединения посылок):

$$\frac{F \rightarrow (G \rightarrow H)}{(F \wedge G) \rightarrow H}, \quad \frac{(F \wedge G) \rightarrow H}{F \rightarrow (G \rightarrow H)}.$$

Правило 6.17 (расширенной контрапозиции):

$$\frac{(F \wedge G) \rightarrow H}{(F \wedge \neg H) \rightarrow \neg G}.$$

Аналогично формулируются другие правила вывода тавтологий, что рекомендуется проделать самостоятельно.

На правила 6.8—6.17 можно смотреть с двух точек зрения. Во-первых, каждое из них представляет собой утверждение следующего типа: формула, записанная в знаменателе, является логическим следствием всех формул, записанных в числителе данного правила. Во-вторых, каждое из этих правил можно рассматривать как правило получения новой тавтологии из уже имеющихся: если все формулы, записанные в числителе, являются тавтологиями, то тавтологией будет и формула, записанная в знаменателе правила (для доказательства этого утверждения примените замечание 6.7).

Еще один способ проверки логического следования. Требуется выяснить, является ли формула $H(X_1, \dots, X_n)$ логическим следствием формул $F_1(X_1, \dots, X_n), \dots, F_m(X_1, \dots, X_n)$, т.е. $F_1, F_2, \dots, F_m \models H$. Предположим, что H не есть логическое следствие формул $F_1, F_2, \dots, F_m$. Значит, существуют такие конкретные высказывания $A_1, \dots, A_n$, что высказывание $H(A_1, \dots, A_n)$ ложно, в то время как все высказывания $F_1(A_1, \dots, A_n), \dots, F_m(A_1, \dots, A_n)$ истинны. Если при этом удастся найти распределение нулей и единиц между значениями переменных $X_1, \dots, X_n$, соответствующее сделанному предположению, то предположение верно. Если же возникает противоречие, то предположение неверно. Посмотрим на примерах, как это делается.

Пример 6.18. Выясните, выполняется ли логическое следование

$$X \rightarrow (\neg Y \vee Z), \neg X, Y \rightarrow Z \models X \vee Z.$$

Допустим, что существуют такие конкретные высказывания A, B, C , что $\lambda(A \rightarrow (\neg B \vee C)) = 1$, $\lambda(\neg A) = 1$, $\lambda(B \rightarrow C) = 1$, но $\lambda(A \vee C) = 0$. Тогда из последнего соотношения получаем $\lambda(A) = 0$, $\lambda(C) = 0$, что не противоречит соотношению $\lambda(\neg A) = 1$. Далее, соотношение $\lambda(B \rightarrow C) = 1$ дает $\lambda(B) = 0$ (так как $\lambda(C) = 0$). Наконец, вычислив при данных значениях A, B и C значение $\lambda(A \rightarrow (\neg B \vee C))$, убеждаемся, что оно равно 1, а это находится в полном соответствии с допущением. Следовательно, приходим к выводу: если высказывания A, B, C таковы, что $\lambda(A) = \lambda(B) = \lambda(C) = 0$, то

при подстановке $X = A$, $Y = B$, $Z = C$ формулы-посылки примут значение 1, а формула $X \vee Z$ примет значение 0. Значит, формула $X \vee Z$ не выводима из формул $X \rightarrow (\neg Y \vee Z)$, $\neg X$, $Y \rightarrow Z$.

Разберите также пример № 1.40, л из Задачника.

Нахождение следствий из данных посылок. Мы научились определять, является ли данная формула логическим следствием некоторых других данных формул. Теперь возникает вопрос, как можно находить все формулы, являющиеся логическим следствием данной совокупности формул. Следующая теорема дает ключ к решению этой задачи.

Теорема 6.19. Формула $H(X_1, \dots, X_n)$, не являющаяся тавтологией, тогда и только тогда будет логическим следствием формул $F_1(X_1, \dots, X_n), \dots, F_m(X_1, \dots, X_n)$, не все из которых являются тавтологиями, когда все совершенные дизъюнктивные одночлены из разложения формулы H в совершенную конъюнктивную нормальную форму входят в совершенную конъюнктивную нормальную форму формулы $F_1(X_1, \dots, X_n) \wedge \dots \wedge F_m(X_1, \dots, X_n)$.

Доказательство. Необходимость. Дано: $F_1, \dots, F_m = H$. Тогда, по теореме 6.4, $F_1 \wedge \dots \wedge F_m = H$. Найдем для формул $F_1 \wedge \dots \wedge F_m$ и H их совершенные конъюнктивные нормальные формы. Такая форма для каждой не тождественно истинной формулы существует и единственна с точностью до порядка совершенных дизъюнктивных одночленов в конъюнкции (см. теорему 5.5). Пусть $D_1 \wedge \dots \wedge D_k$ — СКН-форма для формулы $F_1 \wedge \dots \wedge F_m$, а $H_1 \wedge \dots \wedge H_l$ — СКН-форма для формулы H . Тогда: $F_1 \wedge \dots \wedge F_m \equiv D_1 \wedge \dots \wedge D_k$, $H \equiv H_1 \wedge \dots \wedge H_l$.

Допустим, что заключение теоремы не выполняется, т.е. среди совершенных дизъюнктивных одночленов $H_1, \dots, H_l$ имеется такой, которого нет среди совершенных дизъюнктивных одночленов $D_1, \dots, D_k$. Не нарушая общности (ввиду несущественности порядка вхождения одночленов $H_1, \dots, H_l$ в СКН-форму $H_1 \wedge \dots \wedge H_l$), можем считать, что таким одночленом является, например, H_1 . Итак, $H_1(X_1, \dots, X_n) \not\equiv D_1(X_1, \dots, X_n), \dots, H_1(X_1, \dots, X_n) \not\equiv D_k(X_1, \dots, X_n)$. Тогда существует единственный (с точки зрения логических значений) набор $A_1, \dots, A_n$, на котором совершенный дизъюнктивный одночлен $H_1(X_1, \dots, X_n)$ принимает значение 0: $\lambda(H_1(A_1, \dots, A_n)) = 0$, откуда

$$\lambda(H(A_1, \dots, A_n)) = 0. \quad (1)$$

Этот набор выбирается следующим образом. Если переменная X_i входит в H_1 без знака отрицания, то A_i таково, что $\lambda(A_i) = 0$; если X_i входит в H_1 со знаком отрицания, то A_i таково, что $\lambda(A_i) = 1$ ($1 \leq i \leq n$). Каждый из совершенных дизъюнктивных одночленов $D_1, \dots, D_k$ в силу его отличия от совершенного дизъюнктивного одночлена H_1 обращается на данном наборе в 1 (почему?): $\lambda(D_1(A_1, \dots, A_n)) = 1, \dots, \lambda(D_k(A_1, \dots, A_n)) = 1$. Тогда $\lambda(D_1(A_1, \dots, A_n)) \wedge \dots \wedge \lambda(D_k(A_1, \dots, A_n)) = 1$, откуда, в силу равносильности $D_1 \wedge \dots \wedge D_k \equiv$

$\equiv F_1 \wedge \dots \wedge F_m$, получаем $\lambda(F_1(A_1, \dots, A_n) \wedge \dots \wedge F_m(A_1, \dots, A_n)) = 1$. Следовательно, $\lambda(F_1(A_1, \dots, A_n)) \wedge \dots \wedge \lambda(F_m(A_1, \dots, A_n)) = 1$, а значит,

$$\lambda(F_1(A_1, \dots, A_n)) = 1, \dots, \lambda(F_m(A_1, \dots, A_n)) = 1. \quad (2)$$

Соотношения (1) и (2) противоречат условию: $F_1, \dots, F_m = H$. Следовательно, в СКН-форме формулы H нет ни одного совершенного дизъюнктивного одночлена, который отсутствовал бы в СКН-форме формулы $F_1 \wedge \dots \wedge F_m$.

Достаточность. Пусть $D_1 \wedge \dots \wedge D_k$ — СКН-форма формулы $F_1 \wedge \dots \wedge F_m$. Тогда $F_1 \wedge \dots \wedge F_m \equiv D_1 \wedge \dots \wedge D_k$. Пусть далее $H \equiv D_{i_1} \wedge \dots \wedge D_{i_s}$, где $1 \leq i_1, \dots, i_s \leq k$ и $i_1, \dots, i_s$ попарно различны. Тогда ясно, что если при некоторой подстановке формула $F_1 \wedge \dots \wedge F_m$ принимает истинное значение, то и равносильная ей формула $D_1 \wedge \dots \wedge D_k$ также принимает значение 1. Следовательно, и все члены $D_1, \dots, D_k$ последней конъюнкции принимают значение 1, включая члены $D_{i_1}, \dots, D_{i_s}$. Но тогда и конъюнкция $D_{i_1} \wedge \dots \wedge D_{i_s} \equiv H$ также принимает значение 1. Значит, $F_1, \dots, F_m = H$. $\square$

Эта теорема определяет следующее **правило (алгоритм) для нахождения всех (неравносильных) формул, являющихся логическими следствиями из посылок $F_1, \dots, F_m$** : 1) составить конъюнкцию $F_1 \wedge \dots \wedge F_m$; 2) найти СКН-форму формулы $F_1 \wedge \dots \wedge F_m$; 3) выписать все совершенные дизъюнктивные одночлены найденной СКН-формы, а также всевозможные конъюнкции этих одночленов. Полученное множество формул и является искомым (см. Задачник, № 2.34, л).

Нахождение посылок для данного следствия. Задача нахождения всех формул, из которых данная формула логически следует, является обратной по отношению к той, которая была рассмотрена в предыдущем пункте. Ее решение основывается на следующей теореме.

Теорема 6.20. *Чтобы найти все формулы, логическим следствием каждой из которых будет данная формула $G(X_1, \dots, X_n)$, нужно действовать по следующему алгоритму. Найти СКН-форму для формулы $G(X_1, \dots, X_n)$; выявить все совершенные дизъюнктивные одночлены, которые в ней отсутствуют; составить всевозможные конъюнкции формулы $G(X_1, \dots, X_n)$ с недостающими дизъюнктивными одночленами. Получившаяся совокупность формул (вместе с формулой G) будет искомой (с точностью до равносильности формул).*

Доказательство. Ясно, что из каждой формулы этой совокупности будет логически следовать формула G , так как $G \wedge H \equiv G$ (конъюнкция сильнее каждого из сомножителей). Обратно, покажем, что каждая формула F , из которой логически следует данная формула G , имеет указанный вид, т.е. представляет собой конъюнкцию формулы G и некоторых совершенных дизъюнктивных одночленов, отсутствующих в СКН-форме для G . В самом деле, пусть $F \equiv G$ и $G \equiv D_1 \wedge D_2 \wedge \dots \wedge D_k$ — СКН-форма для формулы $G(X_1, \dots, X_n)$ и $F \equiv \Delta_1 \wedge \Delta_2 \wedge \dots \wedge \Delta_s$ — СКН-форма для формулы

$F(X_1, \dots, X_n)$. По определению логического следования, $F \models G$ означает, что если формула $F(X_1, \dots, X_n)$ на некотором наборе $A_1, \dots, A_n$ значений пропозициональных переменных приняла значение 1, то и формула $G(X_1, \dots, X_n)$ на этом наборе примет значение 1. Другими словами, если формула $G(X_1, \dots, X_n)$ на некотором наборе $A_1, \dots, A_n$ значений пропозициональных переменных принимает значение 0, то и формула $F(X_1, \dots, X_n)$ на этом наборе принимает значение 0. Но все наборы значений переменных, на которых G принимает значение 0, находятся во взаимно-однозначном соответствии с совершенными дизъюнктивными одночленами $D_1, D_2, \dots, D_k$, образующими СКН-форму для формулы G , т.е. если $G(A_1, \dots, A_n) = 0$, то $D_i(A_1, \dots, A_n) = 0$ для некоторого $1 \leq i \leq k$. Следовательно, $F(A_1, \dots, A_n) = 0$ и значит на этом же наборе принимает значение 0 некоторый совершенный дизъюнктивный одночлен Δ_i , входящий в ее СКН-форму. Но тогда этот одночлен совпадает с одночленом D_i . Таким образом, каждый совершенный дизъюнктивный одночлен D_i из СКН-формы для G входит в СКН-форму для формулы F , т.е. СКН-форма для F имеет вид: $F \equiv D_1 \wedge D_2 \wedge \dots \wedge D_k \wedge \Delta_{k+1} \wedge \dots \wedge \Delta_s$, где $\Delta_{k+1}, \dots, \Delta_s$ — совершенные дизъюнктивные одночлены от переменных $X_1, \dots, X_n$, не входящие в СКН-форму для формулы G . $\square$

Разберите решение задачи № 2.39, л из Задачника.

§ 7. Приложение алгебры высказываний к логико-математической практике

Прямая и обратная теоремы. Многие математические теоремы имеют структуру, выражаемую формулой $X \rightarrow Y$. Утверждение X называется *условием теоремы*, а утверждение Y — *ее заключением*. Например: «Если в четырехугольнике все стороны равны между собой (A_1), то его диагонали перпендикулярны (B_1)». Символическая запись этой теоремы: $A_1 \rightarrow B_1$. Второй пример: «Если в четырехугольнике все стороны равны (A_1), то его диагонали делятся точкой пересечения пополам (B'_1)». Символически: $A_1 \rightarrow B'_1$. Третий пример: «Если в четырехугольнике все стороны равны между собой (A_1), то его диагонали делят соответствующие углы пополам (B''_1)». Символически: $A_1 \rightarrow B''_1$. Рассмотрим еще такой пример: «Если один из углов треугольника прямой (A_2), то квадрат длины одной из сторон этого треугольника равен сумме квадратов длин двух других его сторон (B_2)». Символически: $A_2 \rightarrow B_2$. Тщательный анализ теоремы $A_2 \rightarrow B_2$ позволяет выявить в ней более сложную структуру: условие A_2 представляет собой дизъюнкцию трех утверждений ($A'_2 \vee A''_2 \vee A'''_2$), где высказывание A'_2 есть « $\alpha = 90^\circ$ », высказывание A''_2 есть « $\beta = 90^\circ$ » и высказывание A'''_2 — « $\gamma = 90^\circ$ » (символами α, β, γ обозначены величины углов треугольника). Аналогично, заключение B_2 также представляет собой дизъюнкцию трех утверждений:

$B'_2 \vee B''_2 \vee B'''_2$, где B'_2 — высказывание « $a^2 = b^2 + c^2$ », B''_2 — высказывание « $b^2 = a^2 + c^2$ », B'''_2 — высказывание « $c^2 = a^2 + b^2$ » (символами a, b, c обозначены длины сторон треугольника, лежащие против углов величины α, β, γ соответственно). Таким образом, теорема $A_2 \rightarrow B_2$ при более пристальном рассмотрении имеет вид $(A'_2 \vee A''_2 \vee A'''_2) \rightarrow (B'_2 \vee B''_2 \vee B'''_2)$.

Далее, если некоторая теорема имеет форму $X \rightarrow Y$, утверждение $Y \rightarrow X$ называется *обратным* для данной теоремы. Это утверждение может быть справедливым, и тогда оно называется *теоремой, обратной для теоремы $X \rightarrow Y$* , которая, в свою очередь, называется *прямой теоремой*. Если же утверждение $Y \rightarrow X$ не выполняется, то говорят, что обратная теорема для теоремы $X \rightarrow Y$ неверна. Так, для теоремы $A_1 \rightarrow B_1$ обратная теорема неверна, а для теоремы $A_2 \rightarrow B_2$ справедлива обратная теорема $B_2 \rightarrow A_2$ (проверьте!). Таким образом, при доказательстве теоремы нужно четко выделять, каково ее условие и что доказывается. Доказательство прямой теоремы не дает оснований для вывода о том, что и обратная теорема также верна. Обратная теорема требует специальной проверки. Это обусловлено тем, что формулы $X \rightarrow Y$ и $Y \rightarrow X$, выражающие структуры прямой и обратной теорем, не равносильны, в чем мы убедились на приведенных примерах. Их неравносильность можно усмотреть также из таблиц истинности данных формул.

Структура теоремы $A_1 \rightarrow B_1$ достаточно проста. Рассмотрим теорему более сложной структуры: «В равных треугольниках против равных углов лежат равные стороны». Чтобы четко выделить условие данной теоремы и заключение, сформулируем ее следующим образом: «Если два треугольника равны (A), то из попарного равенства двух углов этих треугольников (B) следует равенство их противолежащих сторон (C)». Символически теорема записывается так: $A \rightarrow (B \rightarrow C)$, т. е. она имеет строение, описываемое формулой $P \rightarrow (Q \rightarrow R)$. На основании равносильности, получающейся из тавтологии теоремы 3.1, m (правило перестановки посылок), данная формула равносильна формуле $Q \rightarrow (P \rightarrow R)$, а на основании равносильности теоремы 4.4, z (см. также тавтологию теоремы 3.1, n — правило объединения и разъединения посылок) она равносильна формуле $(P \wedge Q) \rightarrow R$. Следовательно, теорема $A \rightarrow (B \rightarrow C)$ может быть сформулирована в виде $B \rightarrow (A \rightarrow C)$: «Если два угла двух треугольников попарно равны (B), то из равенства этих треугольников (A) следует равенство сторон, противолежащих этим углам (C)». Наконец, третий вид данной теоремы $(A \wedge B) \rightarrow C$: «Если треугольники равны (A) и в них два угла попарно равны (B), то и противолежащие стороны равны (C)». Таким образом, условие этой теоремы состоит из двух утверждений A и B или представляет собой их конъюнкцию $A \wedge B$, а заключением является утверждение C .

Если теперь зададимся целью сформулировать теорему, обратную рассмотренной теореме $A \rightarrow (B \rightarrow C)$, то столкнемся с

некоторыми трудностями, преодолеть которые помогает алгебра высказываний. Обратная теорема — такая, в которой условие и заключение прямой теоремы поменялись местами. В рассматриваемой прямой теореме два условия и одно заключение. Это приводит к тому, что получается не одна обратная теорема, а несколько. Так, обращение первых трех форм данной теоремы приводит к следующим обратным утверждениям:

1) $(B \rightarrow C) \rightarrow A$: «Если из попарного равенства двух углов треугольников следует равенство их противолежащих сторон, то такие треугольники равны»;

2) $(A \rightarrow C) \rightarrow B$: «Если отрезки обладают тем свойством, что, будучи сторонами в равных треугольниках, они лежат против равных углов, то эти отрезки равны»;

3) $C \rightarrow (A \wedge B)$: «Если сторона одного треугольника равна стороне другого треугольника, то треугольники равны и углы, противолежащие этим сторонам, также равны».

Наконец, можем сформулировать еще два обратных утверждения, получающихся из суждений $A \rightarrow (B \rightarrow C)$ и $B \rightarrow (A \rightarrow C)$ перестановкой двух последних высказываний. Иначе говоря, эти обратные утверждения получаются перестановкой местами одного из двух условий прямой теоремы и ее заключения:

4) $A \rightarrow (C \rightarrow B)$: «Если треугольники равны, то из попарного равенства двух их сторон следует равенство противолежащих углов»;

5) $B \rightarrow (C \rightarrow A)$: «Если угол одного треугольника равен углу другого треугольника, то из равенства противолежащих этим углам сторон вытекает равенство самих треугольников».

Предлагается самостоятельно убедиться в том, что лишь второе и четвертое из обратных утверждений справедливы, т.е. действительно являются теоремами, а остальные утверждения неверны.

Необходимые и достаточные условия. С понятиями прямой и обратной теорем тесно связан вопрос о необходимых и достаточных условиях. Если некоторая математическая теорема имеет структуру, выражаемую формулой $X \rightarrow Y$, то высказывание Y называется *необходимым условием* для высказывания X (другими словами, если X истинно, то Y с необходимостью должно быть также истинным), а высказывание X называется *достаточным условием* для высказывания Y (другими словами, для того чтобы Y было истинным, достаточно, чтобы истинным было высказывание X). Посмотрим с этой точки зрения на первую теорему $A_1 \rightarrow B_1$. Необходимым условием равенства в четырехугольнике всех сторон является перпендикулярность его диагоналей. Иначе говоря, достаточным условием для перпендикулярности диагоналей четырехугольника является равенство всех его четырех сторон.

Одно и то же утверждение может иметь несколько необходимых условий. Так, необходимыми условиями равенства всех сторон четырехугольника являются, кроме указанного, деление диа-

гоналей точкой их пересечения пополам (B'_1), деление диагоналями соответствующих углов пополам (B''_1) и т.д. Аналогично, одно и то же утверждение может иметь несколько достаточных условий. Так, для перпендикулярности диагоналей четырехугольника достаточно также, чтобы в нем было две пары равных смежных сторон.

После того как доказана теорема $X \rightarrow Y$, возникает вопрос, будет ли найденное необходимое условие достаточным или достаточное — необходимым. Иначе говоря, будет ли верно утверждение $Y \rightarrow X$, называемое обратным по отношению к теореме $X \rightarrow Y$. Известно, что условие перпендикулярности диагоналей четырехугольника (B_1), необходимое для равенства всех его сторон (A_1), не будет достаточным для такого равенства. Для проверки нужно привести пример четырехугольника с перпендикулярными диагоналями, у которого не все стороны равны (сделайте это!).

Если справедливы утверждения $X \rightarrow Y$ и $Y \rightarrow X$, т.е. справедливо $X \leftrightarrow Y$, то считают, что X — необходимое и достаточное условие для Y , и, наоборот, что Y — необходимое и достаточное условие для X , или же что Y является *критерием* (для) X . Математическая наука изобилует утверждениями вида $X \leftrightarrow Y$, представляющими собой необходимые и достаточные условия, и их приходится отыскивать в самых разных ее областях. Происходит это приблизительно следующим образом. Предположим, требуется найти необходимое и достаточное условие для некоторого утверждения X . Начинают с отыскания ряда необходимых условий для X , т.е. утверждений $Y_1, Y_2, Y_3, \dots$, следующих из X : $X \rightarrow Y_1, X \rightarrow Y_2, X \rightarrow Y_3, \dots$ При этом каждый раз пытаются анализировать, не окажется ли то или иное найденное условие или какая-либо их совокупность (конъюнкция) достаточным условием для X , т.е. окажется ли истинной какая-либо из импликаций: $Y_1 \rightarrow X, Y_2 \rightarrow X, Y_3 \rightarrow X, (Y_1 \wedge Y_2) \rightarrow X, (Y_1 \wedge Y_3) \rightarrow X, (Y_2 \wedge Y_3) \rightarrow X, (Y_1 \wedge Y_2 \wedge Y_3) \rightarrow X, \dots$

Так, в примере с четырехугольником имеем два необходимых условия B_1 и B'_1 для свойства A , т.е. верны две теоремы: $A_1 \rightarrow B_1, A_1 \rightarrow B'_1$. Затем, если ни одно из необходимых условий в отдельности не является достаточным (именно такая ситуация в данном примере), то пытаются проверять на достаточность всевозможные конъюнкции этих условий. Так, в указанном примере справедливо следующее утверждение: $(B_1 \wedge B'_1) \rightarrow A$. (Убедитесь в этом самостоятельно.) Поэтому конъюнкция $B_1 \wedge B'_1$ является достаточным условием для свойства A .

Рассмотрим еще один пример.

Пример 7.1. Пусть требуется найти необходимое и достаточное условие того, что выпуклый четырехугольник является квадратом (A). Находим ряд необходимых условий для этого утверждения:

B_1 : «Диагонали четырехугольника перпендикулярны»;

B_2 : «Диагонали четырехугольника равны»;

B_3 : «Диагонали четырехугольника точкой пересечения делятся пополам».

Ясно, что каждое из утверждений $A \rightarrow B_1$, $A \rightarrow B_2$, $A \rightarrow B_3$ верно. Анализируем обратные утверждения. Очевидно, неверны следующие из них:

Утверждение	Контрпример
$B_1 \rightarrow A$	Ромб, не являющийся квадратом
$B_2 \rightarrow A$	Прямоугольник, не являющийся квадратом
$B_3 \rightarrow A$	Параллелограмм

Неверны также и следующие утверждения:

Утверждение	Контрпример
$(B_1 \wedge B_2) \rightarrow A$	Укажите самостоятельно
$(B_1 \wedge B_3) \rightarrow A$	Ромб, не являющийся квадратом
$(B_2 \wedge B_3) \rightarrow A$	Прямоугольник, не являющийся квадратом

И только соединение (конъюнкция) всех трех необходимых для A условий B_1 , B_2 , B_3 дает условие, достаточное для A . Это $B_1 \wedge B_2 \wedge B_3$: «Диагонали четырехугольника перпендикулярны, равны и делятся пополам точкой их пересечения». Таким образом, истинно утверждение $(B_1 \wedge B_2 \wedge B_3) \rightarrow A$. Кроме того, из истинности утверждений $A \rightarrow B_1$, $A \rightarrow B_2$, $A \rightarrow B_3$ вытекает истинность утверждения $A \rightarrow (B_1 \wedge B_2 \wedge B_3)$. Итак, необходимым и достаточным условием для A является условие $B_1 \wedge B_2 \wedge B_3$.

Противоположная и обратная противоположной теоремы. Закон контрапозиции. Для теоремы, сформулированной в виде импликации $X \rightarrow Y$, кроме обратного утверждения $Y \rightarrow X$ можно сформулировать *противоположное утверждение*. Им называется утверждение вида $\neg X \rightarrow \neg Y$. Утверждение, противоположное данной теореме, может быть также теоремой, т. е. быть истинным высказыванием, но может таковым и не быть. Это следует из того, что формулы $X \rightarrow Y$ и $\neg X \rightarrow \neg Y$ не являются равносильными, в чем нетрудно убедиться, составив таблицы истинности данных формул (составьте их). В этом можно убедиться и на примерах. Возьмем теорему $A_1 \rightarrow B_1$ из предыдущего пункта: «Если в четырехугольнике все стороны равны, то его диагонали перпендикулярны». Составляем противоположное утверждение $\neg A_1 \rightarrow \neg B_1$: «Если в четырехугольнике все стороны не равны, то его диагонали не перпендикулярны». Последнее утверждение неверно, т. е. теоремой не является. Рассмотрим

рим еще одну теорему: «Если сумма цифр натурального числа делится на три, то и само число делится на три». Противоположное утверждение для этой теоремы также справедливо, т.е. является теоремой, противоположной данной: «Если сумма цифр натурального числа не делится на три, то и само число не делится на три». Итак, в том случае, когда утверждение $X \rightarrow Y$ истинно, утверждение $\neg X \rightarrow \neg Y$ может быть как истинным, так и ложным. Это означает, что утверждение, противоположное доказанной теореме, в свою очередь нуждается в доказательстве или опровержении.

При составлении противоположных утверждений к теоремам, условия и заключения которых представляют собой конъюнкции или дизъюнкции нескольких высказываний, нужно пользоваться законами де Моргана (см. теорему 4.4, *p*, *c*). Вспомним, например, теорему $A_2 \rightarrow B_2$ (см. § 7, первый пункт), более подробная запись которой имела вид $(A'_2 \vee A''_2 \vee A'''_2) \rightarrow (B'_2 \vee B''_2 \vee B'''_2) : (\alpha = 90^\circ \vee \beta = 90^\circ \vee \gamma = 90^\circ) \rightarrow ((a^2 = b^2 + c^2) \vee (b^2 = a^2 + c^2) \vee (c^2 = a^2 + b^2))$.

Противоположное утверждение для данной теоремы формулируется следующим образом: $(\alpha \neq 90^\circ \wedge \beta \neq 90^\circ \wedge \gamma \neq 90^\circ) \rightarrow ((a^2 \neq b^2 + c^2) \wedge (b^2 \neq a^2 + c^2) \wedge (c^2 \neq a^2 + b^2))$. Предлагается выяснить, справедливо ли это утверждение, т.е. является ли оно теоремой.

Остается рассмотреть еще один вид теорем, связываемых с прямыми теоремами вида $X \rightarrow Y$, и установить взаимоотношения между этими видами. Имеется в виду теорема, обратная противоположной: $\neg Y \rightarrow \neg X$. Мы не случайно назвали теоремой утверждение, обратное противоположному. Оно действительно будет истинным тогда и только тогда, когда истинно исходное утверждение, что вытекает из равносильности $X \rightarrow Y \equiv \neg Y \rightarrow \neg X$ (см. теорему 4.4, *b*), называемой законом контрапозиции. Таким образом, на основании закона контрапозиции предложение, обратное какой-либо противоположной теореме, само является теоремой, и вместо доказательства данной теоремы можно доказывать теорему, обратную противоположной ей.

Модификация структуры математической теоремы. Приведем ряд равносильностей, которые помогают модифицировать структуру математической теоремы, не нарушая при этом ее логики. Прозерьте равносильными преобразованиями их справедливость:

1) $X \rightarrow (Y \wedge Z) \equiv (X \rightarrow Y) \wedge (X \rightarrow Z)$. Эта равносильность позволяет теорему, имеющую два следствия (заключения Y и Z), расчленить на две теоремы $X \rightarrow Y$ и $X \rightarrow Z$. Число следствий может быть любым конечным. В частности, $X \rightarrow (Y \wedge Z \wedge V) \equiv (X \rightarrow Y) \wedge (X \rightarrow Z) \wedge (X \rightarrow V)$;

2) $(X \vee Y) \rightarrow Z \equiv (X \rightarrow Z) \wedge (Y \rightarrow Z)$. Эта равносильность так же, как и предыдущая, позволяет теорему, в которой условие представляет собой дизъюнкцию двух условий, расчленить на две теоремы: $X \rightarrow Z$ и $Y \rightarrow Z$. Она также допускает обобщения типа:

$(X \vee Y \vee Z) \rightarrow V \equiv (X \rightarrow V) \wedge (Y \rightarrow V) \wedge (Z \rightarrow V)$. На практике данная равносильность скорее применяется в обратном направлении — для объединения ряда теорем с общим заключением в одну. Например, рассмотрим следующие три теоремы. $A \rightarrow D$ ($B \rightarrow D$, $C \rightarrow D$): «Если две биссектрисы (высоты, медианы) треугольника равны, то треугольник — равнобедренный». На основании рассматриваемой равносильности их можно объединить в одну $(A \vee B \vee C) \rightarrow D$: «Если в треугольнике две биссектрисы, или две высоты, или две медианы равны, то треугольник — равнобедренный»;

3) $(X \wedge Y) \rightarrow Z \equiv (X \wedge \neg Z) \rightarrow \neg Y$. Эта равносильность представляет собой обобщение понятия теоремы, обратной противоположной (в последнем случае равносильность имеет вид $Y \rightarrow Z \equiv \neg Z \rightarrow \neg Y$).

Рассмотрим, например, следующую геометрическую теорему: «Если прямая l перпендикулярна двум прямым a и b , лежащим в плоскости π (утверждение A), и прямые a и b не параллельны т.е. $a \nparallel b$ (утверждение B), то прямая l перпендикулярна всякой прямой c , лежащей в плоскости π (утверждение C). На основании рассматриваемой равносильности будет справедлива следующая теорема: «Если прямая l перпендикулярна двум прямым a и b , лежащим в плоскости π (утверждение A), и не перпендикулярна некоторой прямой c , лежащей в этой плоскости (утверждение $\neg C$), то прямые a и b параллельны т.е. $a \parallel b$ (утверждение $\neg B$)».

Ясно, что на основании той же равносильности будет справедлива и такая теорема $(B \wedge \neg C) \rightarrow \neg A$: «Если две прямые a и b , лежащие в плоскости π , не параллельны, т.е. $a \nparallel b$ (утверждение B) и прямая l не перпендикулярна хотя бы одной прямой c , лежащей в плоскости π (утверждение $\neg C$), то l не перпендикулярна одной из прямых a или b (утверждение $\neg A$)».

4) $(X \wedge Y) \rightarrow Z \equiv (X \rightarrow Z) \vee (Y \rightarrow Z)$. Данная равносильность служит ярким примером того, что к трактовке логических равносильностей в рассмотренном выше духе следует все же относиться с осторожностью. Рассмотрим в связи с данной равносильностью, например, следующие утверждения:

A : «Четырехугольник — прямоугольник»;

B : «Четырехугольник — ромб»;

C : «Четырехугольник — квадрат».

Тогда утверждение в левой части равносильности примет вид $(A \wedge B) \rightarrow C$: «Если четырехугольник является прямоугольником и ромбом, то он является квадратом». Оно, несомненно, истинно. В то же время утверждение в правой части принимает вид $(A \rightarrow C) \vee (B \rightarrow C)$: «Если четырехугольник является прямоугольником, то он является квадратом, или же он является квадратом, если он является ромбом». Это утверждение конечно же ложно. При этом исходная равносильность справедлива, что можно проверить простыми равносильными преобразованиями.

Последняя равносильность является еще одним свидетельством того, что математическая логика отражает процесс человеческого мышления с определенной степенью приближенности.

Методы доказательства математических теорем. *Метод доказательства от противного*, несомненно, один из самых распространенных в математике методов доказательства теорем. Суть его состоит в следующем. Для того чтобы доказать утверждение (теорему) $X \rightarrow Y$, т.е. «Если X , то Y », предполагается, что верно утверждение X . Отсюда нужно логическими рассуждениями прийти к утверждению Y . Вместо этого делается предположение, противное (т.е. противоположное) тому, которое требуется доказать, т.е. предполагается $\neg Y$. Далее, рассуждая на основании этого предположения, мы приходим к нелепому выводу $\neg X$. «Нелепость» (абсурдность) вывода состоит в том, что он противоречит исходному данному утверждению X . Получение такого вывода заставляет нас отвергнуть сделанное предположение $\neg Y$ и принять то, которое требовалось доказать, — Y .

Что же происходит в этих рассуждениях с точки зрения (математической) логики? А происходит то, что доказательство данной теоремы $X \rightarrow Y$ фактически заменяется (подменяется) доказательством теоремы $\neg Y \rightarrow \neg X$, противоположной обратной (или обратной противоположной) для данной теоремы. Почему это возможно сделать? А потому, что в этом состоит логический закон контрапозиции $X \rightarrow Y \equiv \neg Y \rightarrow \neg X$, устанавливающий равносильность этих утверждений. Таким образом, описанный метод доказательства от противного основывается на логическом законе контрапозиции.

В задаче № 3.4 Задачника приведены примеры теорем, доказываемых методом от противного, основывающимся на законе контрапозиции.

Метод доказательства от противного применяется также и в других формах. Например, вместо импликации $X \rightarrow Y$ доказывают равносильную ей импликацию $(X \wedge \neg Y) \rightarrow \neg X$, т.е. предполагая, что истинны утверждения X и $\neg Y$, выводят истинность утверждения $\neg X$ в противоречие с предположением. На основании равносильности $X \rightarrow Y \equiv (X \wedge \neg Y) \rightarrow \neg X$ делается вывод об истинности импликации $X \rightarrow Y$. Вторая равносильность $X \rightarrow Y \equiv (X \wedge \neg Y) \rightarrow Y$ дает возможность заменить доказательство импликации $X \rightarrow Y$ доказательством импликации $(X \wedge \neg Y) \rightarrow Y$, т.е. предположив, что истинны утверждения X и $\neg Y$, вывести отсюда истинность утверждения Y в противоречие с предположением. Наконец еще одна форма этого метода, являющаяся также одной из форм метода приведения к абсурду (см. § 3, **О значении тавтологий**), основана на равносильности $X \rightarrow Y \equiv (X \wedge \neg Y) \rightarrow (Z \wedge \neg Z)$. Предпологая, что истинны утверждения X и $\neg Y$, выводим из них некоторое утверждение и его отрицание.

Метод приведения к абсурду (нелепости, противоречию) (по-латински *reductio ad absurdum*) имеет две модификации, которые

являются существенно различными как по форме, так и по существу, т.е. по своей логической (дедуктивной) силе. Это — метод приведения *противоположного* утверждения к абсурду и метод приведения *данного* утверждения к абсурду.

Метод приведения противоположного утверждения к абсурду состоит в следующем. Пусть требуется доказать утверждение X . Рассматривается (допускается) противоположное ему утверждение (т.е. утверждение, являющееся его отрицанием) $\neg X$ и из него выводятся два противоречащих друг другу утверждения (т.е. некоторое утверждение и его отрицание) Y и $\neg Y$: $\neg X \rightarrow Y$ и $\neg X \rightarrow \neg Y$. Из этого делается вывод о том, что справедливо исходное утверждение X . Оправданием этому методу может служить следующая тавтология: $(\neg X \rightarrow \neg Y) \rightarrow ((\neg X \rightarrow Y) \rightarrow X)$.

Метод приведения данного утверждения к абсурду состоит в следующем. Пусть требуется опровергнуть утверждение X , т.е. доказать отрицательное утверждение $\neg X$. В этом случае два противоречащих друг другу утверждения Y и $\neg Y$ выводятся не из утверждения $\neg X$, а из самого данного утверждения X : $X \rightarrow Y$ и $X \rightarrow \neg Y$. Из этого делается вывод о том, что справедливо утверждение $\neg X$, т.е. данное утверждение X опровергнуто. Оправданием этому методу служит следующая формула, также являющаяся тавтологией: $(X \rightarrow \neg Y) \rightarrow ((X \rightarrow Y) \rightarrow \neg X)$. Приведем пример рассуждения (доказательства) этим методом.

Пример 7.2. Доказать, что не существует биекции множества M на множество $P(M)$ всех его подмножеств.

Другими словами, требуется опровергнуть следующее утверждение A : «Существует биекция множества M на множество $P(M)$ всех его подмножеств». Обозначим эту биекцию φ . Теперь нам нужно указать некоторое высказывание B , для которого оно само и его отрицание $\neg B$ можно вывести из утверждения A . Предварительно нам потребуется рассмотреть следующее множество: $M_0 = \{x \in M : x \notin \varphi(x)\}$ — множество всех таких элементов из M , которые не принадлежат своему образу (а это есть некоторое подмножество множества M) при биекции φ . Так как $M_0 \subseteq M$, а φ — биекция M на $P(M)$, то существует такой элемент $x_0 \in M$, что $M_0 = \varphi(x_0)$.

Рассмотрим теперь такое высказывание B : « $x_0 \in M_0$ ». Докажем, что B истинно. Допустим противное, т.е. истинно $\neg B$. Тогда $x_0 \notin M_0$. Но $M_0 = \varphi(x_0)$. Тогда $x_0 \notin \varphi(x_0)$. Следовательно, в силу определения M_0 заключаем, что $x_0 \in M_0$. Получаем противоречие, из которого делаем вывод, что предположение о том, что $\neg B$ истинно, неверно. Следовательно, истинно B . (Но тогда истинно и высказывание $\neg A \rightarrow B$.)

Теперь докажем, что $\neg B$ истинно. Допустим противное, т.е. истинно B . Тогда $x_0 \in M_0$. Но по определению M_0 это означает, что $x_0 \notin \varphi(x_0)$. Но $\varphi(x_0) = M_0$. Следовательно, $x_0 \in M_0$. Получаем проти-

воречие, из которого заключаем, что предположение об истинности высказывания B неверно. Следовательно, истинно $\neg B$, но, тогда истинно и высказывание $\neg A \rightarrow \neg B$.

Таким образом, мы пришли к абсурду, противоречию: из данного утверждения A вывели истинность двух взаимно отрицающих друг друга утверждений B и $\neg B$. Значит, данное утверждение A неверно, а верно его отрицание $\neg A$. $\square$

Доказательство *методом приведения к абсурду* может основываться также на следующей тавтологии (см. теорему 3.1, n): $\equiv (\neg X \rightarrow \rightarrow (Y \wedge \neg Y)) \rightarrow X$. Метод доказательства, основанный на данной тавтологии, состоит в следующем. Допустим, нужно доказать некоторое утверждение X . Предполагаем, что справедливо его отрицание $\neg X$, и выводим отсюда некоторое утверждение Y и его отрицание $\neg Y$. В результате заключаем, что справедливо утверждение X .

Нередко в математических доказательствах используется *правило цепного заключения*, или *правило силлогизма* (см. теорему 3.1, n). Пусть нужно доказать утверждение $P \rightarrow R$. Находим такое утверждение Q , для которого можем доказать истинность утверждений $P \rightarrow Q$ и $Q \rightarrow R$. Тогда на основании правила силлогизма заключаем, что справедливо и утверждение $P \rightarrow R$. Например, из двух теорем «Если треугольник равносторонний, то все его углы равны» и «Если в треугольнике все углы равны, то величина каждого его угла равна 60° » — по правилу силлогизма получаем теорему «Если треугольник равносторонний, то величина каждого его угла равна 60° ».

Существуют и другие методы математических доказательств, состоятельность которых подтверждается математической логикой. Далее будет приведена теорема 7.18, представляющая еще один метод получения математических теорем.

Дедуктивные и индуктивные умозаключения. На этом этапе весьма целесообразно рассмотреть вопрос о том, что представляют собой рассуждения, умозаключения, каковы их структура, виды и критерии правильности, какие умозаключения изучает логика и, в частности, математическая логика.

Умозаключение есть логическая (мыслительная) операция (процедура), состоящая в получении нового суждения (высказывания, утверждения) из одного или нескольких ранее известных суждений. Ранее известные суждения, входящие в состав умозаключения, называются его *посылками*, а новое суждение называется его *следствием* (или *заключением*). С содержательной точки зрения умозаключение есть переход от уже имеющегося (наличного) знания к новому знанию. С формальной точки зрения умозаключение есть переход от посылок к следствию. В логике умозаключение принято представлять в виде фигуры, в которой посылки записаны одна под другой и отделены горизонтальной чертой, под которой записано следствие. *Рассуждение* есть последовательность умозаключе-

чений, причем посылками последующих умозаключений служат следствия предыдущих умозаключений данной последовательности.

Умозаключения делятся на дедуктивные и индуктивные. Расхожим является мнение о том, что дедуктивные умозаключения — это «умозаключения от общего к частному», а индуктивные — «от частного к общему». Эти «определения» лишь в самых общих чертах характеризуют, в частности, дедуктивные умозаключения. Это одно приведенное свойство еще не является для них определяющим. *Дедуктивное умозаключение*, прежде всего, основано на анализе формальной (логической) структуры посылок и следствия, *индуктивное умозаключение* основано на анализе их содержания.

Рассмотрим и проанализируем следующие примеры.

Пример 7.3

«Если четырехугольник является квадратом, то его диагонали равны»;
«Четырехугольник $ABCD$ — квадрат».

«Диагонали четырехугольника $ABCD$ равны».

Пример 7.4

«Если число делится на 6, то оно четное»;
«Число 18 делится на 6».

«Число 18 четное».

Пример 7.5

«Дуб — лиственное дерево»;
«Береза — лиственное дерево»;
«Липа — лиственное дерево».

«Все деревья — лиственные».

Пример 7.6

«Обь замерзает зимой»;
«Енисей замерзает зимой»;
«Лена замерзает зимой».

«Все сибирские реки замерзают зимой».

В примерах 7.3 и 7.4 сделаем соответствующие выводы исходя из анализа формальной структуры посылок и следствия, фактически не обращая внимания на их содержание. Более того, с точки зрения логики эти умозаключения представляются одинаковыми, несмотря на то что не имеют между собой ничего общего по содержанию. Это типичные примеры дедуктивных умозаключений. В то же время, переходя от посылок к следствиям в умозаключениях примеров 7.5 и 7.6, мы не можем отвлечься от их содержания. И хотя эти умозаключения также имеют одинаковую структуру, анализ их содержания приводит нас к построению неверного умозаключения. Дело в том, что все посылки каждого из этих умозаключений истинны, но вывод истинен только

в примере 7.6, а в примере 7.5 он ложен. Таким образом, умозаключения примеров 7.5 и 7.6 не носят дедуктивный характер, они не основаны на анализе формальной структуры умозаключения, на строгих законах формальной логики. Это — индуктивные умозаключения. Их изучение не входит в задачу формальной логики.

Еще более ярким примером индуктивного умозаключения, в котором связь между посылками и следствием является связью не по логической форме, а по содержанию, является следующее умозаключение.

Пример 7.7

«Спичка зажжена»;

«Зажженная спичка поднесена к бумаге».

«Бумага воспламеняется».

В нем связь между посылками и следствием носит и вовсе некий физический причинно-следственный характер.

Важнейшим методологическим вопросом, связанным с дедуктивными умозаключениями, является вопрос об определении правильности (верности) умозаключения. Распространенная ошибка здесь состоит в том, что правильность умозаключения отождествляется с истинностью получаемого на основании этого умозаключения вывода: умозаключение считается правильным, если «в результате мы приходим к истине». Это не так. *Правильность* дедуктивного умозаключения означает, что оно приводит к истинному выводу не всегда, но *всякий* раз, когда оно исходит из *всех* истинных посылок. Другими словами, умозаключение считается правильным, если мы, имея посылки и следствия данной структуры (как определено в умозаключении), при условии истинности всех посылок непременно будем получать истинность следствия. Таким образом, чтобы доказать неправильность умозаключения, нужно указать такую его конкретизацию (пример), в которой все посылки были бы истинными, а следствие было бы ложным. Такой пример называется *опровергающим* (или *контр-примером*).

Итак, в правильном дедуктивном умозаключении следствие должно быть истинным при условии истинности всех посылок. Отсюда не следует делать вывод, что если среди посылок имеются ложные, то следствие должно быть ложным, хотя и такая ситуация возможна. Следующий пример показывает, что даже при всех ложных посылках правильное умозаключение может дать истинное следствие.

Пример 7.8

«Если треугольник равносторонний, то он прямоугольный»;

«Если треугольник прямоугольный, то его внутренние углы равны».

«Если треугольник равносторонний, то его внутренние углы равны».

Данное умозаключение правильное, так как основано на схеме: $X \rightarrow Y, Y \rightarrow Z \models X \rightarrow Z$ (правило 6.14 цепного заключения).

В случае когда среди посылок умозаключения имеются ложные, говорят о наличии в умозаключении *фактической ошибки*; если же неправильным является само дедуктивное умозаключение, то говорят о *логической ошибке*.

В заключение обратим внимание на то, что в отличие от высказываний (суждений), которые делятся на истинные и ложные, умозаключения делятся на правильные и неправильные. Это терминологическое различие не является случайным. Дело в том, что каждое высказывание утверждает наличие или отсутствие у предметов или явлений тех или иных свойств или отношений между ними. Поэтому каждое высказывание имеет в качестве своего «прообраза» некоторые связи и отношения между предметами и явлениями реального мира и допускает, хотя бы в принципе, проверку на истинность (мы рассматривали такие задачи в начале курса — см. Задачник, № 1.1, № 1.2). Именно это обстоятельство подчеркивают, говоря, что данное высказывание является истинным или ложным. В то же время в реальном мире не происходит никаких реальных процессов и явлений, которые можно было бы считать «прообразами» логической операции перехода от одних высказываний к другим. Эта логическая операция является чисто умственной, она происходит лишь в нашем сознании и даже в принципе не допускает «проверки на истинность». Выделение правильных умозаключений является одним из видов познавательной деятельности, который связан с другими видами познания и основан в конечном итоге на громадном практическом опыте человечества.

Правильные и неправильные дедуктивные умозаключения. В § 6 разработана теория, позволяющая давать ответ на вопрос, является ли та или иная формула логическим следствием данной совокупности формул или нет, а также находить все логические следствия из данных формул. Применим ее к рассуждениям, представляющим собой последовательности высказываний (суждений), для того чтобы определить, правильно рассуждение или нет, т. е. правильное или неправильное умозаключение сделано с помощью данного рассуждения из данных посылок.

Пример 7.9. Рассмотрим следующее рассуждение: «Если четырехугольник $ABCD$ — параллелограмм, то его противоположные углы равны. Четырехугольник $ABCD$ — параллелограмм. Следовательно, его противоположные углы равны». Чтобы ответить на вопрос, верно ли это рассуждение, нужно выяснить, будет ли формула алгебры высказываний, отражающая структуру заключения данного рассуждения, логическим следствием формул алгебры высказываний, отражающих структуры его посылок. Структура посылок выражается формулами $X, X \rightarrow Y$, а структура заключе-

ния — формулой Y . (Легко убедиться в этом, если вместо пропозициональной переменной X подставить в формулы высказывание «Четырехугольник $ABCD$ — параллелограмм», а вместо Y — высказывание: «Противоположные углы четырехугольника $ABCD$ равны».) Известно (см. правило 6.8), что формула Y является логическим следствием формул X , $X \rightarrow Y$. Поэтому приведенное рассуждение является правильным, и сделанное заключение действительно следует из посылок.

Рассуждения такой формы нередки в математике. Приведем еще одно подобное рассуждение: «Если 10 делится на 3, то 100 делится на 3. 10 делится на 3. Следовательно, 100 делится на 3». Проведенное рассуждение правильно, но его заключение ложно. Это обстоятельство не должно нас смущать: ведь правильное рассуждение приводит к истинному утверждению при условии, что все посылки рассуждения были истинными. В данном случае из двух посылок одна не является истинной.

Пример 7.10. Рассмотрим следующее рассуждение: «Если курс математической логики неинтересен, то он полезен. Курс математической логики бесполезен или нетруден. Курс математической логики труден. Следовательно, этот курс интересен». Введем обозначения:

X : «Курс математической логики интересен»;

Y : «Курс математической логики полезен»;

Z : «Курс математической логики труден».

Тогда для ответа на вопрос, правильно ли приведенное рассуждение, нужно выяснить, справедливо ли следующее логическое следование: $\neg X \rightarrow Y, \neg Y \vee \neg Z, Z \equiv X$. Покажем, что оно справедливо. На основании равносильности из теоремы 4.4, у вторую посылку можно заменить на $Y \rightarrow \neg Z$. Далее по правилу 6.14 имеем $\neg X \rightarrow Y, Y \rightarrow \neg Z \equiv \neg X \rightarrow \neg Z$. Затем по правилу 6.13 $\neg X \rightarrow \neg Z \equiv \neg \neg Z \rightarrow \neg \neg X$. Последняя формула, на основании равносильности из теоремы 4.4, а, равносильна формуле $Z \rightarrow X$. Наконец, привлекая еще не использованную третью посылку Z , получаем на основании правила 6.8 $Z, Z \rightarrow X \equiv X$. Учитывая свойство выводимости, установленное в теореме 6.5, б, заключаем, что рассматриваемое логическое следование справедливо, и, таким образом, данное рассуждение правильно.

Разберите приведенные в Задачнике решения задач № 3.32, 3.35, 3.36, 3.44, 3.48.

Обратим особое внимание на два типа наиболее часто встречающихся неправильных рассуждений. Первое рассуждение выглядит так. Мы исходим из некоторого предположения и, правильно рассуждая, приходим к правильному выводу. Отсюда делаем вывод, что сделанное предположение верно. С точки зрения математической логики схема этого рассуждения такова: из истинности

утверждений $X \rightarrow Y$ и Y делается вывод об истинности утверждения X . Чтобы ответить на вопрос о правильности такой схемы рассуждений, рассмотрим два примера рассуждений, основанных на этой схеме.

Пример 7.11. «Если число натуральное, то оно рациональное ($A \rightarrow B$). Число 17 рациональное (B). Следовательно, число 17 натуральное (A)».

Пример 7.12. «Если число натуральное, то оно рациональное ($A \rightarrow B$). Число $3/4$ рациональное (B). Следовательно, число $3/4$ натуральное (A)».

В каждом из этих рассуждений обе посылки являются истинными утверждениями. Но в первом случае мы приходим к истинному заключению (число 17 — натуральное), а во втором — к ложному (число $3/4$ не натуральное). Это означает, что неверной является сама схема построения умозаключения, примененная в этих примерах. Неверность, неправомочность схемы означает, что между посылками и заключением нет отношения логического следования. Здесь еще раз уместно подчеркнуть, что правильность умозаключения определяется формой умозаключения, а не истинностью входящих в него утверждений. Иначе говоря, анализируя правильность рассуждения, нужно помнить о том, что его правильность не совпадает с истинностью полученного заключения. Схема умозаключения — это и есть то, что изучает логика, а истинность утверждений, входящих в рассуждение, — это прерогатива той науки (или практики), откуда взяты эти утверждения. Развивая эту мысль, можно заметить, что и термин «следует» употребляется в разных смыслах. Важно понимать существенное различие между следованиями: «из $F \rightarrow G$ следует $\neg G \rightarrow \neg F$ » и «из $a < 3$ следует $a < 5$ ». Первое — утверждение логики, т. е. логическое следование, второе — как свойство отношения порядка $<$ в каком-то числовом множестве, есть некое математическое следование (т. е. следование в рамках некоторой математической теории). Мы придем к подробному рассмотрению этой связи в гл. 6 при уточнении понятия доказательства.

Итак, неправильность рассмотренной схемы рассуждений приводит к тому, что относительно исходного предположения X нельзя сделать вывод о его истинности: оно может быть как истинным, так и неистинным, причем его истинность или ложность никак не связаны с проведенным рассуждением. Этот же вывод подтверждает математическая логика: логическое следование $X \rightarrow Y$, $Y = X$ несправедливо, потому что формула $((X \rightarrow Y) \wedge Y) \rightarrow X$ не является тавтологией (проверьте!).

Тем не менее рассуждения по указанной схеме нередко встречаются в школьной практике, особенно в алгебре и тригонометрии. Так, при доказательстве тождества рассуждения начинаются

именно с этого тождества: обе его части преобразуют так, что оно превращается в некоторое очевидное тождество. После этого делается заключение о том, что исходное тождество верно. Узнаете рассмотренную схему? Например, при доказательстве тригонометрического тождества

$$\frac{\sin x + \cos x}{\cos^3 x} = \operatorname{tg}^3 x + \operatorname{tg}^2 x + \operatorname{tg} x + 1$$

можно встретить такие рассуждения. «Умножим обе его части на $\cos^3 x$. Получим: $\sin x + \cos x = \sin^3 x + \sin^2 x \cos x + \sin x \cos^2 x + \cos^3 x$. Сгруппируем слагаемые в правой части:

$$\sin x + \cos x = \sin^2 x (\sin x + \cos x) + \cos^2 x (\sin x + \cos x).$$

Продолжим группировку в правой части:

$$\sin x + \cos x = (\sin^2 x + \cos^2 x) (\sin x + \cos x).$$

Поделим обе части на $\sin x + \cos x$. Получим: $1 = \sin^2 x + \cos^2 x$ — известное тождество. Отсюда делается вывод, что исходное тождество доказано».

В данном случае правильным доказательством будет проведение рассуждений в обратном направлении, от известного (очевидного) тождества к исходному, данному тождеству. Эти рассуждения-преобразования здесь проделать можно и тем самым действительно доказать данное тождество. Но нередко умозаключение по такой неверной схеме приводит к ошибкам, т.е. к ложным утверждениям. Такие рассуждения иногда относят к разряду занимательной математики, где они получили название «парадоксов» или «софизмов».

Пример 7.13. Рассмотрим пример софизма. Докажем, что $3 = 7$. Из чисел 3 и 7 вычтем одно и то же число 5. Получим: $3 - 5 = -2$, $7 - 5 = 2$. Возведем числа -2 и 2 в квадрат. В результате получим равные числа: $(-2)^2 = 4$ и $2^2 = 4$. Следовательно, должны быть равны и исходные числа: $3 = 7$.

Ясно, что полученное заключение ложно. Проанализируем проведенное рассуждение, чтобы обнаружить допущенную ошибку. Рассуждение состоит из трех шагов. Выделим эти шаги более отчетливо.

Первый шаг (вычитание из целых чисел 3 и 7 целого числа 5). *Первая посылка* $A \rightarrow B$: «Если a и b — целые числа, то их разность $a - b$ существует и есть число целое». *Вторая посылка* A : «Числа 3 и 5 (а также 7 и 5) — целые». *Заключение* B : «Разности $3 - 5$ и $7 - 5$ существуют, и $3 - 5 = -2$, $7 - 5 = 2$ ».

Данное умозаклучение сделано по правилу МР: $X \rightarrow Y$, $X \equiv Y$ и потому является правильным.

Второй шаг (возведение чисел -2 и 2 в квадрат). *Первая посылка* $A \rightarrow B$: «Если число a целое, то его квадрат a^2 существует и является неотрицательным целым числом». *Вторая посылка* A : «Число -2 (а также число 2) — целое». *Заключение* B : «Квадраты чисел -2 и 2 существуют, причем $(-2)^2 = 4$ и $2^2 = 4$ ».

Умозаклучение и здесь сделано по правилу МР: $X \rightarrow Y$, $X \equiv Y$, и потому и на этом шаге рассуждения ошибка не допущена.

Третий шаг (заключение о равенстве чисел 3 и 7). *Первая посылка* $A \rightarrow B$: «Если целые числа равны, то равны и их квадраты». *Вторая посылка* B : «Квадраты целых чисел -2 и 2 равны: $4 = 4$ ». *Заключение* A : «Равны сами числа -2 и 2 , т.е. $3 - 5 = 7 - 5$, т.е. $3 = 7$ ».

На данном этапе рассуждения умозаклучение сделано по схеме: $X \rightarrow Y$, $Y \equiv X$, которая не является правильной. Следовательно, в этом умозаклучении сделана логическая ошибка, которая и привела к ложному выводу, несмотря на то что исходили мы из всех истинных посылок.

Второй распространенный тип неправильных рассуждений выглядит так. Мы исходим из некоторого неверного предположения и, правильно рассуждая, приходим к некоторому выводу. Отсюда делаем заключение, что полученный вывод неверен. С точки зрения математической логики схема этого рассуждения такова: из истинности утверждений $\neg X$ и $X \rightarrow Y$ делается вывод об истинности утверждения $\neg Y$. Следующие два примера рассуждений, основанных на этой схеме, позволяют ответить на вопрос о ее правомочности.

Пример 7.14. «Если число натуральное, то оно рациональное ($A \rightarrow B$). Число $3/4$ не натуральное ($\neg A$). Следовательно, число $3/4$ не рациональное ($\neg B$)».

Пример 7.15. «Если число натуральное, то оно рациональное ($A \rightarrow B$). Число $\sqrt{2}$ не натуральное ($\neg A$). Следовательно, число $\sqrt{2}$ не рациональное ($\neg B$)».

В каждом из этих рассуждений обе посылки являются истинными утверждениями. Но в первом случае мы приходим к ложному заключению (число $3/4$ — рациональное), а во втором — к истинному (число $\sqrt{2}$ иррациональное). Это снова означает, что неверной является сама схема построения умозаклучения, примененная в этих примерах, т.е. эта схема при всех истинных посылках не обязательно дает истинное следствие. Вывод, основанный на примерах, подтверждается математической логикой: из формул $X \rightarrow Y$ и $\neg X$ не следует формула $\neg Y$, в чем нетрудно убедиться, проверив, что формула $((X \rightarrow Y) \wedge \neg X) \rightarrow \neg Y$ не является тавтологией.

Решение «логических» задач. Алгебра высказываний может быть с успехом применена к решению одного типа задач, которые называют «логическими». Эти задачи можно решать и непосредственным рассуждением, но не всегда очевиден путь таких рассуждений. Применение алгебры высказываний дает единый и достаточно общий метод решения указанных задач. Рассмотрите задачи № 3.54 и 3.57 в Задачнике.

Отметим некоторые особенности решения «логических» задач методами алгебры высказываний. В таких задачах, как правило, имеется ряд высказываний, относительно которых известно, что столько-то из них истинны, а столько-то ложны, но не известно, какие именно истинны, а какие ложны. Например, имеется три высказывания U , V , W , из которых два истинны, а одно ложно. Учитывая эти условия, нужно составить из этих высказываний некое сложное высказывание, которое будет заведомо истинно (или ложно). Затем, используя законы логики, преобразовать его к виду, из которого определится ответ на вопрос задачи. В процессе равносильных преобразований использовать другие условия задачи. В рассматриваемом примере такое сложное высказывание строится исходя из следующих соображений. Так как из высказываний U , V , W два истинны, то все дизъюнкции пар этих высказываний также будут истинны: $U \vee V$, $U \vee W$, $V \vee W$. Следовательно, будет истинной и конъюнкция этих высказываний: $(U \vee V) \wedge (U \vee W) \wedge (V \vee W)$. Равносильное преобразование этого выражения будет зависеть от структуры высказываний U , V , W . Разберем пример решения такой задачи.

Пример 7.16. Перед финалом школьного шахматного турнира, в который вышли Александров, Васин и Сергеев, один болельщик сказал, что первое место займет Александров, второй болельщик сказал, что Сергеев не будет последним, а третий — что Васину не занять первого места. После игр оказалось, что один болельщик ошибся, а два других угадали. Как распределились места, если никакие два участника не заняли одно и то же место?

Для решения введем следующие высказывания ($i = 1, 2, 3$):

A_i : «Александров занял i -е место»;

B_i : «Васин занял i -е место»;

C_i : «Сергеев занял i -е место».

Тогда три высказывания болельщиков можно записать так:

1-й болельщик U : A_1 ;

2-й болельщик V : $\neg C_3$;

3-й болельщик W : $\neg B_1$.

Составим сложное высказывание, которое будет заведомо истинным. Так как из трех высказываний U , V , W два высказывания истинны, то каждая из дизъюнкций $(U \vee V)$, $(U \vee W)$, $(V \vee W)$ будет истинной, а значит, истинной будет и их конъюнкция $(U \vee V) \wedge$

$\wedge (U \vee W) \wedge (V \vee W)$. Преобразуем это высказывание равносильным образом:

$$\begin{aligned} (U \vee V) \wedge (U \vee W) \wedge (V \vee W) &\equiv (A_1 \vee \neg C_3) \wedge (A_1 \vee \neg B_1) \wedge \\ &\wedge (\neg C_3 \vee \neg B_1) \equiv (A_1 \vee (A_1 \wedge \neg B_1) \vee (\neg C_3 \wedge A_1) \vee (\neg C_3 \wedge \neg B_1)) \wedge \\ &\wedge (\neg C_3 \vee \neg B_1) \equiv (A_1 \wedge (\neg C_3 \vee \neg B_1)) \vee (A_1 \wedge \neg B_1 \wedge (\neg C_3 \vee \neg B_1)) \vee \\ &\vee (\neg C_3 \wedge A_1 \wedge (\neg C_3 \vee \neg B_1)) \vee (\neg C_3 \wedge \neg B_1 \wedge (\neg C_3 \vee \neg B_1)) \equiv (A_1 \wedge \\ &\wedge \neg C_3) \vee (A_1 \wedge \neg B_1) \vee (A_1 \wedge \neg B_1) \vee (A_1 \wedge \neg C_3) \vee (\neg B_1 \wedge \neg C_3) \equiv \\ &\equiv (A_1 \wedge \neg C_3) \vee (A_1 \wedge \neg B_1) \vee (\neg B_1 \wedge \neg C_3). \end{aligned}$$

Полученное высказывание, представляющее собой дизъюнкцию некоторых высказываний, истинно. Следовательно, истинно по меньшей мере одно слагаемое. Рассмотрим последовательно все эти случаи:

$A_1 \wedge \neg C_3 = 1$. Тогда $A_1 = 1$ и $\neg C_3 = 1$, т.е. $C_3 = 0$. Мы получаем следующее распределение мест: ACB ;

$A_1 \wedge \neg B_1 = 1$. Тогда $A_1 = 1$ и $\neg B_1 = 1$, т.е. $B_1 = 0$. Здесь мы получаем две возможности распределения мест: ABC или ACB ;

$\neg B_1 \wedge \neg C_3 = 1$. Тогда $\neg B_1 = 1$ и $\neg C_3 = 1$, т.е. $B_1 = 0$ и $C_3 = 0$. Здесь варианты распределения такие: ACB , CAB , CBA .

В итоге получаем варианты ответов: ACB , ABC , CAB , CBA . Проверяя первый вариант, видим, что при нем истинными оказываются все три высказывания U , V , W болельщиков, что не соответствует условию задачи. Окончательно получаем три решения: ABC , CAB , CBA .

Рассмотренный метод решения привел к получению своего рода «лишнего корня», что потребовало проверки полученных вариантов на соответствие условию задачи.

Рассмотрим более тонкий метод, который сразу даст только те ответы, которые удовлетворяют условию задачи. Он основан на составлении вместо высказывания $(U \vee V) \wedge (U \vee W) \wedge (V \vee W)$ такого высказывания, которое более точно передает (описывает) суть условий задачи. Эта передача (описание) достаточно точна для того, чтобы не могло возникнуть никаких двусмысленностей и кривотолков.

Для составления такого высказывания кроме U , V , W рассмотрим также высказывания:

X : «1-й болельщик угадал»;

Y : «2-й болельщик угадал»;

Z : «3-й болельщик угадал».

Тогда нетрудно понять, что из двух высказываний $X \wedge U$ и $\neg X \wedge \neg U$ точно одно высказывание истинно. Значит, истинна и их дизъюнкция: $(X \wedge U) \vee (\neg X \wedge \neg U)$. Аналогично, истинны следующие высказывания, связанные со 2-м и 3-м болельщиками: $(Y \wedge V) \vee (\neg Y \wedge \neg V)$ и $(Z \wedge W) \vee (\neg Z \wedge \neg W)$. Следовательно, истинна и конъюнкция всех этих трех высказываний:

$$\begin{aligned} ((X \wedge U) \vee (\neg X \wedge \neg U)) \wedge ((Y \wedge V) \vee (\neg Y \wedge \neg V)) \wedge \\ \wedge ((Z \wedge W) \vee (\neg Z \wedge \neg W)). \end{aligned} \quad (7.1)$$

Для преобразования этого высказывания нужно применить закон дистрибутивности конъюнкции относительно дизъюнкции. В итоге получится СДН-форма от переменных X, Y, Z, U, V, W . Но многие ее совершенные конъюнктивные одночлены в силу условий задачи окажутся равными 0. Так как из трех высказываний X, Y, Z точно два высказывания истинны, конъюнктивные одночлены, содержащие сомножители $\neg X \wedge \neg Y \wedge Z, X \wedge \neg Y \wedge \neg Z, \neg X \wedge Y \wedge \neg Z, \neg X \wedge \neg Y \wedge \neg Z$, обратятся в 0. Так как из трех высказываний X, Y, Z одно высказывание ложно, конъюнктивный одночлен, содержащий сомножитель $X \wedge Y \wedge Z$, также равен 0. В итоге в СДН-форме останутся лишь три совершенных конъюнктивных одночлена: это те, которые содержат сомножители $X \wedge Y \wedge \neg Z, \neg X \wedge Y \wedge Z, X \wedge \neg Y \wedge Z$. Данная СДН-форма имеет вид

$$(X \wedge Y \wedge \neg Z \wedge U \wedge V \wedge \neg W) \vee (\neg X \wedge Y \wedge Z \wedge \neg U \wedge V \wedge W) \vee (X \wedge \neg Y \wedge Z \wedge U \wedge \neg V \wedge W).$$

Для рассматриваемой задачи эта СДН-форма имеет вид

$$(X \wedge Y \wedge \neg Z \wedge A_1 \wedge \neg C_3 \wedge B_1) \vee (\neg X \wedge Y \wedge Z \wedge \neg A_1 \wedge \neg C_3 \wedge \neg B_1) \vee (X \wedge \neg Y \wedge Z \wedge A_1 \wedge C_3 \wedge \neg B_1).$$

Истинность этого высказывания означает, что истинна хотя бы одна элементарная конъюнкция. Рассмотрим последовательно все эти случаи:

1) $X \wedge Y \wedge \neg Z \wedge A_1 \wedge \neg C_3 \wedge B_1 = 1$. Тогда $A_1 = 1, \neg C_3 = 1$, а следовательно, $C_3 = 0$ и $B_1 = 1$. Этот случай не может иметь места, так как A и B оказываются на первом месте;

2) $\neg X \wedge Y \wedge Z \wedge \neg A_1 \wedge \neg C_3 \wedge \neg B_1 = 1$. Тогда $\neg A_1 = 1, \neg C_3 = 1, \neg B_1 = 1$ и, следовательно, $A_1 = 0, C_3 = 0, B_1 = 0$, т.е. получаются две возможности распределения мест: CAB, CBA ;

3) $X \wedge \neg Y \wedge Z \wedge A_1 \wedge C_3 \wedge \neg B_1 = 1$. Тогда $A_1 = 1, C_3 = 1, \neg B_1 = 1$, т.е. $B_1 = 0$ и получается следующее распределение мест: ABC .

Окончательно получаем три решения: ABC, CAB, CBA .

Рассмотрим теперь задачу, получающуюся из предыдущей при изменении одного условия. Тонкий метод и в этом случае дает прекрасный результат. Чтобы применить более грубый метод, нужно проявить некоторую изобретательность, и при этом также получится «лишний корень», который нужно будет устранить проверкой.

Пример 7.17. Решить задачу из предыдущего примера при условии, что результат финала угадал только один болельщик, а два других ошиблись.

Решим сначала эту задачу более тонким методом. Для этого, как и в предыдущей задаче, составим высказывание (7.1). Отличие от предыдущей задачи начнется в процессе преобразования этого высказывания, когда мы начнем учитывать новое условие задачи. В данном случае обратятся в 0 следующие конъюнктивные

одночлены, входящие в полученную СДН-форму от переменных X, Y, Z, U, V, W . Так как из трех высказываний X, Y, Z точно два высказывания ложны, конъюнктивные одночлены, содержащие сомножители $\neg X \wedge Y \wedge Z, X \wedge \neg Y \wedge Z, X \wedge Y \wedge \neg Z, X \wedge Y \wedge Z$, обратятся в 0. Так как из трех высказываний X, Y, Z точно одно истинно, конъюнктивный одночлен, содержащий сомножитель $\neg X \wedge \neg Y \wedge \neg Z$, также равен 0. В итоге в СДН-форме останутся только три совершенных конъюнктивных одночлена: это те, которые содержат сомножители $X \wedge \neg Y \wedge \neg Z, \neg X \wedge Y \wedge \neg Z, \neg X \wedge \neg Y \wedge Z$. В данном случае СДН-форма имеет вид

$$(X \wedge \neg Y \wedge \neg Z \wedge A_1 \wedge C_3 \wedge B_1) \vee (\neg X \wedge Y \wedge \neg Z \wedge \neg A_1 \wedge \neg C_3 \wedge B_1) \vee (\neg X \wedge \neg Y \wedge Z \wedge \neg A_1 \wedge C_3 \wedge \neg B_1).$$

Полученное высказывание истинно. Значит, истинна по меньшей мере одна элементарная конъюнкция. Рассмотрим все эти случаи:

1) $X \wedge \neg Y \wedge \neg Z \wedge A_1 \wedge C_3 \wedge B_1 = 1$. Тогда $A_1 = 1, C_3 = 1, B_1 = 1$. Этот случай невозможен, так как A и B оказываются на первом месте;

2) $\neg X \wedge Y \wedge \neg Z \wedge \neg A_1 \wedge \neg C_3 \wedge B_1 = 1$. Тогда $\neg A_1 = 1, \neg C_3 = 1, B_1 = 1$, т.е. $A_1 = 0, C_3 = 0$, и распределение мест следующее: BCA ;

3) $\neg X \wedge \neg Y \wedge Z \wedge \neg A_1 \wedge C_3 \wedge \neg B_1 = 1$. Тогда $\neg A_1 = 1, C_3 = 1, \neg B_1 = 1$, т.е. $A_1 = 0, B_1 = 0$.

Эти условия не могут быть выполнены: если C на третьем месте, то из A и B один окажется на первом, что не так. Значит, этот случай также не может иметь места.

В итоге получаем следующее единственно возможное распределение мест: BCA .

При решении этой задачи более грубым методом (без введения высказываний X, Y, Z) рассуждаем следующим образом. Так как из трех высказываний U, V, W два высказывания ложны, каждая из конъюнкций $U \wedge V, U \wedge W, V \wedge W$ будет ложной, следовательно, ложной будет и их дизъюнкция:

$$(U \wedge V) \vee (U \wedge W) \vee (V \wedge W) \equiv (A_1 \wedge \neg C_3) \vee (A_1 \wedge \neg B_1) \vee (\neg B_1 \wedge \neg C_3) \equiv$$

(это равносильное преобразование проделано в обратном направлении в начале решения предыдущего примера)

$$\equiv (A_1 \vee \neg C_3) \wedge (A_1 \vee \neg B_1) \wedge (\neg B_1 \vee \neg C_3).$$

Полученное высказывание, представляющее собой конъюнкцию некоторых высказываний, ложно. Следовательно, ложен по меньшей мере один из сомножителей. Рассмотрим последовательно все эти случаи:

1) $A_1 \vee \neg C_3 = 0$. Тогда $A_1 = 0$ и $\neg C_3 = 0$, т.е. $C_3 = 1$ и получается следующее распределение мест: BAC ;

2) $A_1 \vee \neg B_1 = 0$. Тогда $A_1 = 0$ и $\neg B_1 = 0$, т. е. $B_1 = 1$. В данном случае получаем две возможности распределения мест: BAC (уже была), BCA ;

3) $\neg B_1 \vee \neg C_3 = 0$. Тогда $\neg B_1 = 0$, $\neg C_3 = 0$, т. е. $B_1 = 1$ и $C_3 = 1$. Получается один уже имеющийся вариант: BAC .

В итоге получим два варианта ответа: BAC и BCA . Проверка первого варианта на его соответствие условиям задачи показывает, что при нем ложными оказываются все три высказывания U , V , W болельщиков, что не соответствует условию задачи. Окончательно получаем единственное решение: BCA .

Принцип полной дизъюнкции. Этот принцип носит также название «теоремы об обратимости системы импликаций», или «закона замкнутой системы утверждений», или «закона Гаубера». Обратим внимание на то, что этот принцип представляет собой обобщение ситуации, связанной с отношениями между истинностными значениями прямой, обратной, противоположной и обратной противоположной теорем. В самом деле, для утверждений $A \rightarrow B$ (прямая теорема), $\neg A \rightarrow \neg B$ (противоположная теорема), $B \rightarrow A$ (обратная теорема), $\neg B \rightarrow \neg A$ (теорема, обратная противоположной) справедливо следующее: если первые два из них ($A \rightarrow B$ и $\neg A \rightarrow \neg B$) верны, то верны оба вторых утверждения ($B \rightarrow A$ и $\neg B \rightarrow \neg A$). Если исходных утверждений будет не два, а больше, то этот случай и рассматривается в теореме об обратимости системы импликаций. Она позволяет делать вывод о справедливости обратных теорем, если посылки и следствия прямых теорем удовлетворяют некоторым условиям.

Теорема 7.18 (об обратимости системы импликаций, или принцип полной дизъюнкции). Пусть справедливы все следующие прямые теоремы ($m \geq 2$): $A_1 \rightarrow B_1$, $A_2 \rightarrow B_2$, ..., $A_m \rightarrow B_m$. Причем из посылок A_1 , A_2 , ..., A_m по меньшей мере одна выполняется (т. е. истинна), а следствия B_1 , B_2 , ..., B_m попарно исключают друг друга (т. е. никакие два различных следствия не могут быть истинны одновременно, а значит истинны все следующие утверждения $\neg(B_i \wedge B_j)$, для $1 \leq i, j \leq m$, $i \neq j$). Тогда справедливы и все обратные импликации: $B_1 \rightarrow A_1$, $B_2 \rightarrow A_2$, ..., $B_m \rightarrow A_m$.

Доказательство. Покажем сначала истинность первой обратной импликации: $B_1 \rightarrow A_1$. Если высказывание B_1 ложно, то импликация $B_1 \rightarrow A_1$ истинна в силу определения 1.7 импликации. Предположим теперь, что высказывание B_1 истинно. Покажем, что тогда все высказывания A_2 , A_3 , ..., A_m ложны. Допустим противное: например, пусть A_2 истинно. Тогда из истинности высказываний A_2 и $A_2 \rightarrow B_2$ заключаем, что исходя из определения импликации высказывание B_2 истинно. Таким образом, два различных следствия B_1 и B_2 прямых теорем истинны, но это противоречит условию. Следовательно, высказывание A_2 не может быть истинным. Аналогично, не могут быть истинными высказывания A_3 , ..., A_m .

Итак, все высказывания $A_2, A_3, \dots, A_m$ ложны. Но по условию по меньшей мере одна из посылок $A_1, A_2, \dots, A_m$ истинна. Следовательно, истинной должна быть посылка A_1 . Таким образом, высказывания B_1 и A_1 истинны. Тогда (по определению 1.7 импликации) истинна импликация $B_1 \rightarrow A_1$.

Совершенно аналогично устанавливается истинность и остальных обратных импликаций $B_2 \rightarrow A_2, \dots, B_m \rightarrow A_m$. Рекомендуется провести эти рассуждения, например, для следующей импликации: $B_2 \rightarrow A_2$. $\square$

Увидим теперь, что ситуация с прямой, обратной, противоположной и обратной противоположной теоремами есть частный случай принципа дизъюнкции. В самом деле, эта ситуация полностью укладывается в условия данной теоремы: у двух данных утверждений $A \rightarrow B$ и $\neg A \rightarrow \neg B$ из посылок A и $\neg A$ по меньшей мере одна (в данном случае точно одна) истинна, а следствия B и $\neg B$ исключают друг друга (т. е. не могут быть истинными одновременно). Тогда справедливы и обратные импликации $B \rightarrow A$ и $\neg B \rightarrow \neg A$.

Суть принципа полной дизъюнкции состоит в том, что он на основе законов логики гарантирует истинность обратных утверждений для специального набора прямых утверждений той или иной теории и позволяет тем самым эти обратные утверждения в этой теории не доказывать, после того как доказаны прямые утверждения. Но сам принцип полной дизъюнкции, конечно, требует доказательства. Это — теорема логики, и после того как она доказана в логике, она может быть применена в самых разных областях математики, она принимает как бы универсальный, всеобщий характер.

Принцип полной дизъюнкции представляет собой фактически утверждение о логическом следовании одного утверждения из каких-то других, т. е. это есть еще одно правило логического умозаключения в дополнение к тем, которые рассмотрены в § 6 (правила 6.8 — 6.17). Сформулируем, например, в виде такого правила данный принцип в случае, когда $n = 2$:

$$\frac{P_1 \rightarrow Q_1, P_2 \rightarrow Q_2, P_1 \vee P_2, \neg(Q_1 \wedge Q_2)}{(Q_1 \rightarrow P_1) \wedge (Q_2 \rightarrow P_2)}.$$

Принцип полной дизъюнкции имеет весьма широкое применение во всех дисциплинах школьного курса математики. Рассмотрим один такой пример (см. также Задачник, № 3.11— 3.15).

Пример 7.19. В школьном курсе геометрии доказываются следующие три теоремы: «Квадрат длины стороны, лежащей против острого угла треугольника, меньше суммы квадратов длин двух других сторон этого треугольника»; «Квадрат длины стороны, ле-

жащей против прямого угла треугольника, равен сумме квадратов длин двух других сторон этого треугольника» (теорема Пифагора); «Квадрат длины стороны, лежащей против тупого угла треугольника, больше суммы квадратов длин двух других сторон этого треугольника». Проанализируем данные утверждения в аспекте применимости к ним теоремы 7.18. Введем следующие обозначения для высказываний:

A_1 : «В треугольнике угол α острый»;

A_2 : «В треугольнике угол α прямой»;

A_3 : «В треугольнике угол α тупой»;

B_1 : « $a^2 < b^2 + c^2$ »;

B_2 : « $a^2 = b^2 + c^2$ »;

B_3 : « $a^2 > b^2 + c^2$ »,

где a, b, c — длины сторон треугольника; α — его угол, лежащий против стороны длины a . Тогда сформулированные три теоремы можно записать символически: $A_1 \rightarrow B_1$, $A_2 \rightarrow B_2$, $A_3 \rightarrow B_3$.

Ясно, что из трех посылок A_1, A_2, A_3 этих утверждений по меньшей мере одна истинна (угол α в треугольнике непременно должен быть либо острым, либо прямым, либо тупым), а следствия B_1, B_2, B_3 попарно исключают друг друга (в силу закона трихотомии для действительных чисел). Поэтому на основе теоремы 7.4 заключаем, что истинны и все три обратные импликации: $B_1 \rightarrow A_1$, $B_2 \rightarrow A_2$, $B_3 \rightarrow A_3$.

Например, теорема $B_2 \rightarrow A_2$, обратная теореме Пифагора, читается так: «Если в треугольнике квадрат длины некоторой стороны равен сумме квадратов длин двух других его сторон, то этот треугольник прямоугольный, причем прямым углом является угол, лежащий против первой стороны».

Одно обобщение принципа полной дизъюнкции. Теорема 7.20. Пусть справедливы все следующие прямые теоремы ($m \geq 2$): $(A_1 \wedge C) \rightarrow B_1$, $(A_2 \wedge C) \rightarrow B_2$, ..., $(A_m \wedge C) \rightarrow B_m$, причем из посылок $A_1, A_2, \dots, A_m$ по меньшей мере одна выполняется (истинна), а следствия $B_1, B_2, \dots, B_m$ попарно исключают друг друга (т.е. никакие два различных следствия не могут быть истинны одновременно). Тогда справедливы и все следующие обратные импликации: $(B_1 \wedge C) \rightarrow A_1$, $(B_2 \wedge C) \rightarrow A_2$, ..., $(B_m \wedge C) \rightarrow A_m$.

Доказательство. Покажем сначала истинность первой обратной импликации: $(B_1 \wedge C) \rightarrow A_1$.

Если высказывание B_1 ложно, то посылка $B_1 \wedge C$ ложна и, значит, импликация $(B_1 \wedge C) \rightarrow A_1$ истинна. Предположим теперь, что высказывание B_1 истинно. Тогда, если при этом высказывание C ложно, то снова посылка $B_1 \wedge C$ ложна, следовательно, импликация $(B_1 \wedge C) \rightarrow A_1$ истинна. Предположим теперь, что и высказывание C истинно. Покажем, что тогда все высказывания $A_2, A_3, \dots, A_m$ ложны. Допустим противное: например, пусть A_2 истинно. Тогда из истинности высказываний A_2, C (а значит, и

истинности их конъюнкции $A_2 \wedge C$ и $(A_2 \wedge C) \rightarrow B_2$, очевидно, вытекает истинность высказывания B_2 . Таким образом, два различных следствия B_1 и B_2 прямых теорем истинны. Это противоречит условию. Следовательно, высказывание A_2 не может быть истинным. Аналогично не могут быть истинными высказывания $A_3, \dots, A_m$. Итак, все высказывания $A_2, A_3, \dots, A_m$ ложны. Но по условию, по меньшей мере одна из посылок $A_1, A_2, \dots, A_m$ истинна. Следовательно, истинной должна быть посылка A_1 . Итак, высказывания B_2, C и A_1 истинны. Тогда истинна конъюнкция $B_1 \wedge C$ и истинна импликация $(B_1 \wedge C) \rightarrow A_1$, являющаяся обратной по отношению к первой данной импликации $(A_1 \wedge C) \rightarrow B_1$.

Совершенно аналогично устанавливается истинность и остальных обратных импликаций $(B_2 \wedge C) \rightarrow A_2, \dots, (B_m \wedge C) \rightarrow A_m$. $\square$

Пример 7.21. Примером применения данной общелогической теоремы могут служить следующие три утверждения а), б), в), выражающие свойство монотонности операции умножения в кольце целых чисел или в поле рациональных чисел (в правом столбце помещены обратные для них теоремы а'), б'), в'), справедливые на основании доказанной теоремы 7.20):

$$a) \ x < y, z > 0 \Rightarrow xz < yz;$$

$$a') \ xz < yz, z > 0 \Rightarrow x < y;$$

$$б) \ x > y, z > 0 \Rightarrow xz > yz;$$

$$б') \ xz > yz, z > 0 \Rightarrow x > y;$$

$$в) \ x = y, z > 0 \Rightarrow xz = yz;$$

$$в') \ xz = yz, z > 0 \Rightarrow x = y.$$

Аналогично для следующих трех утверждений з), д), е) относительно целых чисел:

$$з) \ x < y, z < 0 \Rightarrow xz > yz;$$

$$з') \ xz > yz, z < 0 \Rightarrow x < y;$$

$$д) \ x > y, z < 0 \Rightarrow xz < yz;$$

$$д') \ xz < yz, z < 0 \Rightarrow x > y;$$

$$е) \ x = y, z < 0 \Rightarrow xz = yz;$$

$$е') \ xz = yz, z < 0 \Rightarrow x = y.$$

Глава II

БУЛЕВЫ ФУНКЦИИ

Различные области математики имеют дело с разнообразными функциями. Это и действительные функции действительного аргумента, изучающиеся в курсе математического анализа, и комплексные функции комплексного аргумента, известные из теории функций комплексного переменного, и вектор-функции скалярного аргумента, играющие важную роль в дифференциальной геометрии, и скалярные функции векторных аргументов (например, скалярное и смешанное произведения векторов), и вектор-функции векторных аргументов (векторное произведение двух векторов), и функции, заданные и принимающие значения в множестве натуральных чисел (например, функция Эйлера, известная из теории чисел), и многие другие. В настоящей главе познакомимся с еще одним видом функций — булевыми функциями. Они возникли при математической постановке задач логики. Их называют также функциями алгебры логики.

§ 8. Множества, отношения, функции

Напомним некоторые необходимые в дальнейшем понятия так называемой наивной или интуитивной теории множеств.

Понятие множества. Понятие множества — одно из основных математических понятий. Оно первично, исходно, неопределяемо, т.е. не может быть сведено к другим понятиям. Под *множеством* понимается совокупность объектов (предметов), которая рассматривается, мыслится как одно целое, как нечто единое. Объекты, составляющие множество, называются его *элементами*. Множества обозначают заглавными буквами латинского алфавита: $A, B, C, \dots$, а элементы множеств — малыми латинскими буквами: $a, b, c, \dots, a_1, a_2, a_3, \dots$. Если некоторый объект a является элементом множества A , т.е. объект a принадлежит множеству A , то пишут $a \in A$. Если же элемент a не принадлежит множеству A , то пишут $a \notin A$. Символ $\in$ называется *знаком принадлежности*.

Множество, состоящее из элементов $a_1, a_2, \dots, a_n$, обозначается $\{a_1, a_2, \dots, a_n\}$. Символ $\{x : S(x)\}$ применяется для обозначения множества всех таких объектов x , которые удовлетворяют некоторому

свойству $S(x)$. Если объекты берутся из некоторого множества A , то множество всех таких объектов, удовлетворяющих свойству $S(x)$, обозначается $\{x \in A : S(x)\}$. Например, $\{x \in R: x^2 - x - 6 \leq 0\}$ — множество всех действительных чисел x , удовлетворяющих соотношению $x^2 - x - 6 \leq 0$ (нетрудно проверить, что это множество есть замкнутый интервал $[-2, 3]$ числовой прямой).

Включение и равенство множеств. Множество A называется *подмножеством* множества B , или говорят, что A *включается* в B , если каждый элемент множества A принадлежит множеству B . Запись: $A \subseteq B$. Множества A и B называются *равными*, если A состоит из тех и только тех элементов, которые принадлежат B , т. е. если $x \in A$ тогда и только тогда, когда $x \in B$. Запись: $A = B$. Ясно, что $A = B$ тогда и только тогда, когда $A \subseteq B$ и $B \subseteq A$. Множество A называется *собственным подмножеством* множества B , если $A \subseteq B$ и $A \neq B$. Обозначение: $A \subset B$. Символ $\subset$ называется *знаком включения*.

Множество называется *пустым*, если оно не содержит ни одного элемента. Существует единственное пустое множество, оно обозначается символом $\emptyset$. Значит, $\emptyset \subseteq A$ для любого множества A .

Операции над множествами. *Объединением* множеств A и B называется множество, обозначаемое $A \cup B$, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств A и B . Таким образом, по определению $A \cup B = \{x : x \in A \text{ или } x \in B\}$.

Пересечением множеств A и B называется множество, обозначаемое $A \cap B$, состоящее из тех и только тех элементов, которые принадлежат как множеству A , так и множеству B . Следовательно, по определению $A \cap B = \{x : x \in A \text{ и } x \in B\}$.

Разностью множеств A и B называется множество, обозначаемое $A \setminus B$, элементами которого являются все те элементы множества A , которые не принадлежат множеству B , и только они. Таким образом, по определению $A \setminus B = \{x : x \in A \text{ и } x \notin B\}$.

Если $A \subseteq U$ (где U — некоторое универсальное множество, которое содержит в качестве подмножеств все рассматриваемые нами множества), то *дополнением* множества A в множестве U называется множество, обозначаемое $\bar{A}$, состоящее из всех тех элементов множества U , которые не принадлежат множеству A . Итак, $\bar{A} = U \setminus A = \{x : x \in U \text{ и } x \notin A\} = \{x \in U : x \notin A\}$.

Перечислим некоторые наиболее важные *свойства* операций над множествами и отношения включения множеств:

- 1) $A \cup A = A$ (идемпотентность объединения);
- 2) $A \cap A = A$ (идемпотентность пересечения);
- 3) $A \cup B = B \cup A$ (коммутативность объединения);
- 4) $A \cap B = B \cap A$ (коммутативность пересечения);
- 5) $(A \cup B) \cup C = A \cup (B \cup C)$ (ассоциативность объединения);
- 6) $(A \cap B) \cap C = A \cap (B \cap C)$ (ассоциативность пересечения);
- 7) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность объединения относительно пересечения);

8) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (дистрибутивность пересечения относительно объединения);

9) $A \cup (B \cap A) = A$ (1-й закон поглощения);

10) $\overline{A \cap (B \cup A)} = \overline{A}$ (2-й закон поглощения);

11) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (1-й закон де Моргана);

12) $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (2-й закон де Моргана);

13) $A \cup U = U, A \cap U = A$;

14) $A \cup \emptyset = A, A \cap \emptyset = \emptyset$;

15) $A \cup \overline{A} = U, A \cap \overline{A} = \emptyset$;

16) $\overline{\emptyset} = U, \overline{U} = \emptyset$;

17) $\overline{\overline{A}} = A$ (закон инволюции);

18) $A \setminus B = A \cap \overline{B}$;

19) $A \subseteq A \cup B, B \subseteq A \cup B$;

20) $A \cap B \subseteq A, A \cap B \subseteq B$;

21) $A \subseteq B \Leftrightarrow A \cap B = A$;

22) $A \subseteq B \Leftrightarrow A \cup B = B$;

23) $A \subseteq B \Leftrightarrow \overline{A} \cup B = U$;

24) $A \subseteq B \Leftrightarrow A \cap \overline{B} = \emptyset$.

Покажем, как эти свойства доказываются с применением тавтологий алгебры высказываний, на которых они все базируются. Эти рассуждения будут служить продолжением темы предыдущего параграфа:

1) $x \in A \cup A \Leftrightarrow x \in A \vee x \in A \Leftrightarrow x \in A$. На последнем шаге применена тавтология из теоремы 3.2, а: $(P \vee P) \Leftrightarrow P$. Итак, множество $A \cup A$ состоит из тех и только тех элементов, из которых состоит множество A . Следовательно, по определению равенства множеств, $A \cup A = A$;

6) $x \in (A \cap B) \cap C \Leftrightarrow x \in A \cap B \wedge x \in C \Leftrightarrow (x \in A \wedge x \in B) \wedge x \in C \Leftrightarrow x \in A \wedge (x \in B \wedge x \in C) \Leftrightarrow x \in A \wedge x \in B \cap C \Leftrightarrow x \in A \cap (B \cap C)$. Использована тавтология из теоремы 3.2, г: $((P \wedge Q) \wedge R) \Leftrightarrow (P \wedge (Q \wedge R))$;

9) $x \in A \cup (B \cap A) \Leftrightarrow x \in A \vee x \in B \cap A \Leftrightarrow x \in A \vee (x \in B \wedge x \in A) \Leftrightarrow x \in A$. Использована тавтология из теоремы 3.2, е: $(P \vee (Q \wedge P)) \Leftrightarrow P$;

11) $x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow \neg(x \in A \cup B) \Leftrightarrow \neg(x \in A \vee x \in B) \Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \Leftrightarrow x \notin A \wedge x \notin B \Leftrightarrow x \in \overline{A} \wedge x \in \overline{B} \Leftrightarrow x \in \overline{A} \cap \overline{B}$. Использована тавтология из теоремы 3.2, ж: $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$;

20) $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B \Rightarrow x \in A$. Использована тавтология из теоремы 3.2, з: $(P \wedge Q) \rightarrow P$;

21) $A \cap B = A \Leftrightarrow A \cap B \subseteq A \wedge A \subseteq A \cap B \Leftrightarrow$
 $\Leftrightarrow (x \in A \cap B \rightarrow x \in A) \wedge (x \in A \rightarrow x \in A \cap B) \Leftrightarrow$
 $\Leftrightarrow ((x \in A \wedge x \in B) \rightarrow x \in A) \wedge (x \in A \rightarrow (x \in A \wedge x \in B)) \Leftrightarrow$
 $\Leftrightarrow 1 \wedge (x \in A \rightarrow (x \in A \wedge x \in B)) \Leftrightarrow$
 $\Leftrightarrow x \in A \rightarrow (x \in A \wedge x \in B) \Leftrightarrow \neg(x \in A) \vee (x \in A \wedge x \in B) \Leftrightarrow$

$$\Leftrightarrow (\neg(x \in A) \vee x \in A) \wedge (\neg(x \in A) \vee x \in B) \Leftrightarrow \\ \Leftrightarrow 1 \wedge (\neg(x \in A) \vee x \in B) \Leftrightarrow (x \in A \rightarrow x \in B) \Leftrightarrow A \subseteq B.$$

Проанализируйте приведенную цепочку рассуждений и выявите использованные тавтологии.

Бинарные отношения и функции. Пусть даны два (не обязательно различных) множества A и B . Выберем элементы $a \in A$ и $b \in B$. *Упорядоченной парой*, составленной из элементов a и b , называется пара (a, b) , в которой указано, какой элемент является первым, а какой — вторым. Таким образом, упорядоченная пара (b, a) отлична от упорядоченной пары (a, b) , если $a \neq b$. Упорядоченные пары (a, b) и (c, d) называются *равными*, если и только если $a = c$ и $b = d$.

Прямым (или *декартовым*) *произведением* двух множеств A и B называется множество $A \times B$ всевозможных упорядоченных пар (a, b) , таких, что $a \in A$ и $b \in B$: $A \times B = \{(a, b) : a \in A \text{ и } b \in B\}$.

Бинарным отношением между элементами множеств A и B называется любое множество упорядоченных пар (a, b) , таких, что $a \in A$ и $b \in B$, т.е. любое подмножество прямого произведения $A \times B$. Если ρ — бинарное отношение и записано $(x, y) \in \rho$, то говорят, что x и y связаны отношением ρ , или x находится с y в отношении ρ , или для x и y выполняется отношение ρ . Вместо записи $(x, y) \in \rho$ используют также запись $x \rho y$.

Бинарное отношение $f \subseteq A \times B$ называется *функцией*, *заданной на множестве A и принимающей значения в множестве B* (или *отображением множества A в B*), если: а) для любого $x \in A$ найдется $y \in B$, такой, что $(x, y) \in f$; б) для любых $x \in A$, $y_1, y_2 \in B$ из того, что $(x, y_1) \in f$ и $(x, y_2) \in f$, следует, что $y_1 = y_2$. Другими словами, f — функция, если для любого $x \in A$ существует единственный $y \in B$, такой, что $(x, y) \in f$. Этот единственный элемент y называется *значением функции f для аргумента x* и обозначается $f(x)$. Если $(x, y) \in f$, то используется запись $y = f(x)$. Множество A называется *областью определения функции f* , B — *областью ее изменения*. То, что f есть функция (отображение) из A в B , записывают в виде $f: A \rightarrow B$ или $A \xrightarrow{f} B$. Функция $f: A \rightarrow B$ называется *инъективной* (или *взаимно-однозначной*), если для любых $x_1, x_2 \in A$ из равенства $f(x_1) = f(x_2)$ непременно вытекает равенство аргументов $x_1 = x_2$. Функция $f: A \rightarrow B$ называется *сюръективной* (или *отображением A на B*), если для любого $y \in B$ найдется хотя бы один $x \in A$, такой, что $y = f(x)$. Функция $f: A \rightarrow B$ называется *биективной* (или *биекцией*), если она одновременно инъективна и сюръективна.

Понятие n -арного отношения. Обобщением понятия упорядоченной пары элементов является понятие *кортежа* (*упорядоченного набора*) объектов. Кортеж n объектов $a_1, a_2, \dots, a_n$ обозначается $(a_1, a_2, \dots, a_n)$. Два кортежа $(a_1, \dots, a_n)$ и $(b_1, \dots, b_n)$ называют *равными* и пишут $(a_1, \dots, a_n) = (b_1, \dots, b_n)$, если и только если $a_1 = b_1, \dots, a_n = b_n$. *Прямым произведением n множеств $A_1, \dots, A_n$* называется множество $A_1 \times \dots \times A_n = \{(x_1, \dots, x_n) : x_1 \in A_1, \dots, x_n \in A_n\}$.

Если $A_1 = \dots = A_n = A$, то прямое произведение $A \times \dots \times A$ называют n -й прямой степенью множества A и обозначают A^n . При этом будем считать, что $A^1 = A$.

Таким образом, n -арным отношением между элементами множеств $A_1, \dots, A_n$ называется любое подмножество прямого произведения $A_1 \times \dots \times A_n$. Функцией n аргументов, заданной на множестве A и принимающей значения в множестве B , называется такое $(n+1)$ -арное отношение $f \subseteq A^n \times B$, что: а) для любых $x_1, \dots, x_n \in A$ найдется $y \in B$, такой, что $(x_1, \dots, x_n, y) \in f$; б) для любых $x_1, \dots, x_n \in A$, $y, z \in B$ из того, что $(x_1, \dots, x_n, y) \in f$ и $(x_1, \dots, x_n, z) \in f$ следует, что $y = z$. Другими словами, f — функция, если для любых $x_1, \dots, x_n \in A$ существует единственный элемент $y \in B$, такой, что $(x_1, \dots, x_n, y) \in f$. Аналогично тому, как это делалось для функции одного аргумента, для функции n аргументов также вводятся понятия инъективности, сюръективности, биективности.

§ 9. Булевы функции от одного и двух аргументов

Булевы функции получили свое название по имени замечательного английского математика Джорджа Буля (1815—1864), который первым начал применять математические методы в логике.

Происхождение булевых функций. В конце § 1 отмечалось, что каждое из определений 1.1, 1.3, 1.5, 1.7, 1.9 операций над высказываниями (отрицания, конъюнкции, дизъюнкции, импликации, эквивалентности) можно рассматривать как определение некоторого действия над символами 0 и 1, т.е. как определение некоторой функции, заданной на двухэлементном множестве $\{0, 1\}$ и принимающей значения в том же множестве. Символом 0 обозначалось любое ложное высказывание, а символом 1 — любое истинное. Например, отрицание представляет собой в этом смысле функцию одного аргумента $f_2(x)$, которая принимает следующие значения: $f_2(0) = 1$, $f_2(1) = 0$; конъюнкция представляет собой функцию двух аргументов $g_1(x, y)$, принимающую следующие значения: $g_1(0, 0) = 0$, $g_1(0, 1) = 0$, $g_1(1, 0) = 0$, $g_1(1, 1) = 1$ и т.д. В § 2 эта мысль была развита дальше: отмечено, что каждая формула алгебры высказываний $F(X_1, X_2, \dots, X_n)$ от n пропозициональных переменных $X_1, X_2, \dots, X_n$ определяет по существу некоторую функцию от n аргументов, сопоставляющую любому набору длины n , составленному из элементов двухэлементного множества $\{0, 1\}$, единственный элемент того же множества. Этот элемент является логическим значением того составного высказывания, в которое превращается данная формула, если вместо всех ее пропозициональных переменных подставить конкретные высказывания, имеющие соответствующие значения истинности. Легко понять, что высказывания (точнее, их содержание) здесь ни при чем. Функция, о которой идет речь, определяется структурой

формулы F и определениями 1.1, 1.3, 1.5, 1.7, 1.9, которые понимаются как определения действий над символами 0, 1 — элементами двухэлементного множества $\{0, 1\}$.

В связи с этим естественно рассмотреть функции, заданные на двухэлементном множестве $\{0, 1\}$ и принимающие значения в нем же безотносительно к формулам алгебры высказываний, т.е. сами по себе. Тогда функции, определяемые таблицами в определениях 1.1, 1.3, 1.5, 1.7, 1.9, а также функции, определяемые формулами алгебры высказываний, будут служить примерами таких функций. Такие функции, заданные и принимающие значения в двухэлементном множестве, появляющиеся в алгебре высказываний, носят название функций алгебры логики или булевых функций.

Введя понятие булевой функции, мы окончательно отрываемся от того содержательного смысла, который имели в виду в алгебре высказываний: пропозициональные переменные служили там обозначениями для высказываний языка. Теперь же остались только два символа 0 и 1 и понятие булевой функции. Чтобы еще более оттенить это обстоятельство, обозначим переменные, пробегающие множество $\{0, 1\}$, малыми буквами латинского алфавита $x, y, z, u, v, \dots, x_1, x_2, \dots, x_n, \dots$ и будем называть их *булевыми*.

В этой главе изучим некоторые свойства булевых функций и посмотрим, как эти функции могут применяться в алгебре высказываний и в теории релейно-контактных схем.

Булевы функции от одного аргумента. *Определение 9.1.* Булевой функцией от одного аргумента называется функция f , заданная на множестве из двух элементов и принимающая значения в том же двухэлементном множестве.

Элементы двухэлементного множества будем обозначать 0 и 1. Таким образом, $f: \{0, 1\} \rightarrow \{0, 1\}$. Нетрудно перечислить все булевы функции от одного аргумента:

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
0	0	0	1	1
1	0	1	0	1

Составленная таблица означает, что, например, булева функция f_2 на аргументах 0 и 1 действует следующим образом: $f_2(0) = 1$ и $f_2(1) = 0$. Всего имеется четыре различных булевых функций от одного аргумента:

$f_0(x) = 0$ — функция, тождественно равная 0 (тождественный нуль);

$f_1(x) = x$ — тождественная функция;

$f_2(x) = x'$ — функция, называемая отрицанием;

$f_3(x) = 1$ — функция, тождественно равная 1 (тождественная единица).

Булевы функции от двух аргументов. Определение 9.2. Булевой функцией от двух аргументов называется функция g , заданная на множестве $\{0, 1\} \times \{0, 1\}$ и принимающая значения в двухэлементном множестве $\{0, 1\}$. Другими словами, булева функция от двух аргументов сопоставляет любой упорядоченной паре, составленной из элементов 0 и 1 (а таких упорядоченных пар будет четыре), либо 0, либо 1.

Перечислим все возможные булевы функции от двух аргументов в форме следующей таблицы:

		0	·	$\rightarrow'$	x	$\leftarrow'$	y	+	$\vee$	$\downarrow$	$\leftrightarrow$	y'	$\leftarrow$	x'	$\rightarrow$	$ $	1
x	y	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Заметим: функции пронумерованы так, что номер функции, записанный в двоичной системе счисления, дает последовательность значений соответствующей функции. Например, двоичная запись числа 13 имеет вид: 1101. Соответствующая функция $g_{13}(x, y)$ принимает следующие значения: $g_{13}(0, 0) = 1$, $g_{13}(0, 1) = 1$, $g_{13}(1, 0) = 0$, $g_{13}(1, 1) = 1$.

Многие из перечисленных функций имеют названия и специальные обозначения. Приведем их, сгруппировав функции в пары по тому принципу, что каждая функция из пары является отрицанием другой функции этой пары.

Первые две функции, которые рассматриваются, $g_0(x, y) = 0$ и $g_{15}(x, y) = 1$ — *тождественный ноль* и *тождественная единица*.

Далее, функция $g_1(x, y)$ называется *конъюнкцией* и обозначается $x \cdot y$ (или xy). Таким образом, $g_1(x, y) = x \cdot y$. Конъюнкция принимает значение 1 в том и только в том случае, когда оба ее аргумента принимают значение 1. Отрицание конъюнкции, функция $g_{14}(x, y)$, называется *штрихом Шеффера* и обозначается $x | y$. Таким образом, $g_{14}(x, y) = (x \cdot y)' = x | y$. Эта функция принимает значение 0 в том и только в том случае, когда функция $g_1(x, y)$ принимает значение 1, т.е. в случае, когда оба ее аргумента принимают значение 1.

Функция $g_7(x, y)$ называется *дизъюнкцией* и обозначается $x \vee y$. Таким образом, $g_7(x, y) = x \vee y$. Функция $g_8(x, y)$, являющаяся отрицанием функции $g_7(x, y)$, носит название *стрелка Пирса* (или *функция Вебба*) и обозначается $x \downarrow y$. Итак, $g_8(x, y) = (x \vee y)' = x \downarrow y$.

Функция $g_{13}(x, y)$ называется *импликацией* и обозначается $x \rightarrow y$, т.е. $g_{13}(x, y) = x \rightarrow y$. Аргумент x в этой функции называется *посыл-*

кой импликации, а аргумент y — ее следствием. Отрицанием импликации является функция $g_2(x, y) = (x \rightarrow y)'$. Специального названия она не имеет.

Функция $g_{11}(x, y)$ называется *антиимпликацией* или *обратной импликацией*, потому что представляет собой импликацию с посылкой y и следствием x . Таким образом, $g_{11}(x, y) = y \rightarrow x$. Ее отрицанием является функция $g_4(x, y) = (y \rightarrow x)'$, не имеющая названия.

Функция $g_9(x, y)$ называется *эквивалентностью* и обозначается $x \leftrightarrow y$, так что $g_9(x, y) = x \leftrightarrow y$. Она принимает значение 1 тогда и только тогда, когда оба ее аргумента принимают одинаковые значения. Функция $g_6(x, y)$, являющаяся отрицанием функции $g_9(x, y)$, называется *сложением по модулю два*, или *суммой Жегалкина*, и обозначается $x + y$.

Наконец остаются еще две пары функций. В первую пару входят функции $g_3(x, y)$ и $g_{12}(x, y)$. Первая из них принимает всегда те же самые значения, что и ее первый аргумент, т.е. $g_3(x, y) = x$, а вторая функция является отрицанием первой: $g_{12}(x, y) = x'$. Во вторую пару входят функции $g_5(x, y)$ и $g_{10}(x, y)$. Первая из них принимает всегда те же самые значения, что и ее второй аргумент, т.е. $g_5(x, y) = y$, а вторая функция является отрицанием первой: $g_{10}(x, y) = y'$.

Теперь установим некоторые важнейшие свойства введенных функций. Две булевы функции $f(x, y)$ и $g(x, y)$ называются *равными*, если каждому набору значений аргументов x, y обе функции сопоставляют один и тот же элемент из множества $\{0, 1\}$, т.е. $f(a, b) = g(a, b)$ для любых $a, b \in \{0, 1\}$. Например, $x \vee y = y \vee x$.

Из введенных простейших булевых функций можно строить с помощью суперпозиций более сложные булевы функции. Например, если в функцию $x \vee t$ вставить вместо аргумента t функцию $y \cdot z$, то получим следующую сложную функцию: $x \vee (y \cdot z)$. Если в нее в свою очередь вставить вместо аргумента z функцию $u \rightarrow v$, то получим сложную функцию $x \vee (y \cdot (u \rightarrow v))$. И так далее. В результате получаются булевы функции от трех, четырех и большего числа аргументов.

В следующих теоремах устанавливаются некоторые равенства одних булевых функций другим, выражающие свойства основных булевых функций.

Свойства дизъюнкции, конъюнкции и отрицания. Теорема 9.3. Для булевых функций выполняются следующие равенства:

- а) $x \vee x = x$, $x \cdot x = x$ (идемпотентность дизъюнкции и конъюнкции);
- б) $x \vee y = y \vee x$, $x \cdot y = y \cdot x$ (коммутативность дизъюнкции и конъюнкции);
- в) $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (ассоциативность дизъюнкции и конъюнкции);
- г) $x \vee 1 = 1$, $x \cdot 1 = x$;
- д) $x \vee 0 = x$, $x \cdot 0 = 0$;

е) $x \vee (y \cdot z) = (x \vee y) \cdot (x \vee z)$, $x \cdot (y \vee z) = (x \cdot y) \vee (x \cdot z)$ (дистрибутивность дизъюнкции относительно конъюнкции и дистрибутивность конъюнкции относительно дизъюнкции);

ж) $x \vee (y \cdot x) = x$, $x \cdot (y \vee x) = x$ (законы поглощения);

з) $(x \vee y)' = x' \cdot y'$, $(x \cdot y)' = x' \vee y'$ (законы де Моргана);

и) $x \vee x' = 1$, $x \cdot x' = 0$;

к) $x'' = x$.

Доказательство. а) Свойство идемпотентности дизъюнкции и конъюнкции означает, что применение как одной из них, так и другой к двум одинаковым элементам дает этот же самый элемент. Доказательства данных равенств вытекают непосредственно из таблиц, определяющих дизъюнкцию и конъюнкцию. В самом деле, для дизъюнкции $0 \vee 0 = 0$, $1 \vee 1 = 1$ и для конъюнкции $0 \cdot 0 = 0$, $1 \cdot 1 = 1$.

б) Коммутативность (перестановочность) дизъюнкции означает, что значение функции не зависит от порядка ее аргументов. Это действительно так, потому что, согласно определению дизъюнкции, она принимает значение 1 тогда и только тогда, когда хотя бы один из ее аргументов (не имеет значения, какой именно) принимает значение 1, и принимает значение 0 тогда и только тогда, когда оба аргумента равны 0. Аналогична ситуация и с конъюнкцией.

в) Вместо слова «ассоциативность» используется также термин «сочетательность». Докажем ассоциативность конъюнкции с помощью таблиц. Такой способ важен тем, что он может быть применен для доказательства (или опровержения) равенства между любыми двумя булевыми функциями. Итак, составляем последовательно таблицы значений булевых функций, суперпозиция которых дает левую часть тождества ассоциативности, а затем булевых функций, суперпозиция которых дает его правую часть, придавая всевозможные значения аргументам x , y , z :

x	y	z	$x \cdot y$	$(x \cdot y) \cdot z$	$y \cdot z$	$x \cdot (y \cdot z)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	0
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	1	0	0	0
1	1	1	1	1	1	1

Сравнивая пятый и седьмой столбцы таблицы, видим, что они одинаковы, т.е. функции, стоящие в левой и правой частях доказываемого равенства, принимают одинаковые значения при

одинаковых наборах значений аргументов. А это означает, что функции $(x \cdot y) \cdot z$ и $x \cdot (y \cdot z)$ действительно равны.

Составлением аналогичных таблиц может быть доказана и ассоциативность дизъюнкции. Ассоциативность означает, что при многократном применении дизъюнкции или конъюнкции результат не будет зависеть от последовательности их применения, и поэтому все скобки, обозначающие эту последовательность, могут быть опущены. Так, будем писать $x \cdot y \cdot z$ вместо $(x \cdot y) \cdot z$, а также вместо $x \cdot (y \cdot z)$, или $x \vee y \vee z$ вместо $(x \vee y) \vee z$ и вместо $x \vee (y \vee z)$. Точно так же будем писать $x \cdot y \cdot z \cdot t$ вместо каждой из следующих равных между собой булевых функций: $((x \cdot y) \cdot z) \cdot t = (x \cdot (y \cdot z)) \cdot t = x \cdot (y \cdot (z \cdot t)) = x \cdot ((y \cdot z) \cdot t) = (x \cdot y) \cdot (z \cdot t)$. Аналогичным образом будет использоваться запись $x \vee y \vee z \vee t$ и т. д.

з) Свойства сразу следуют из таблиц для дизъюнкции и конъюнкции. Первое свойство означает, что дизъюнкция любого элемента с элементом 1 дает снова элемент 1 (подобно тому как в арифметике умножение любого числа на ноль дает ноль). Второе свойство говорит о том, что относительно конъюнкции элемент 1 играет роль «нейтрального» элемента, т. е. такого элемента, конъюнкция которого с любым элементом не меняет его.

д) Аналогично двум предыдущим свойствам, эти свойства также легко вытекают из таблиц для дизъюнкции и конъюнкции. Здесь первое свойство говорит о «нейтральности» элемента 0 относительно дизъюнкции.

е) Для доказательства этих равенств можно воспользоваться рассмотренным выше методом таблиц, но можно использовать и ранее доказанные соотношения. Проверим, например, первое равенство. При $x = 1$ его левая часть в силу свойств з) и б) равна $1 \vee (y \cdot z) = 1$, а правая, в силу тех же свойств, равна $(1 \vee y) \cdot (1 \vee z) = 1 \cdot 1 = 1$. Если же $x = 0$, то левая часть доказываемого равенства становится, в силу свойств д) и б), равной $0 \vee (y \cdot z) = y \cdot z$; но тому же самому становится равной и правая часть: $(0 \vee y) \cdot (0 \vee z) = y \cdot z$. Следовательно, функции $x \vee (y \cdot z)$ и $(x \vee y) \cdot (x \vee z)$ при одинаковых значениях аргументов дают равные значения, т. е. они равны.

Совершенно аналогичным путем можно доказать и второе тождество дистрибутивности. Вместо слова «дистрибутивность» иногда употребляется термин «распределительность». Отметим, что в обычной арифметике умножение дистрибутивно (распределительно) относительно сложения: $x \cdot (y + z) = x \cdot y + x \cdot z$, но сложение, конечно, не дистрибутивно относительно умножения: $x + (y \cdot z) \neq (x + y) \cdot (x + z)$. Для булевых операций (функций) не только конъюнкция дистрибутивна относительно дизъюнкции, но и дизъюнкция дистрибутивна относительно конъюнкции.

ж) Снова при доказательстве можем пользоваться уже установленными свойствами. В самом деле, при $y = 0$ левая часть первого равенства превращается в $x \vee (0 \cdot x) = x \vee 0 = x$, т. е. равна правой.

Если же $y = 1$, то левая часть рассматриваемого соотношения равна $x \vee (1 \cdot x) = x \vee x = x$, т.е. снова равна его правой части. Следовательно, первое равенство доказано. Аналогично проверяется второе равенство.

з) Для доказательства второго равенства положим сначала, что $x = 0$. Тогда его левая часть будет равна $(0 \cdot y)' = 0' = 1$, а правая — $0' \vee y' = 1 \vee y' = 1$. Если же $x = 1$, то левая часть доказываемого тождества превратится в $(1 \cdot y)' = y'$, а его правая часть — в $1' \vee y' = 0 \vee y' = y'$. Следовательно, равенство выполняется. Аналогично проверяется первое равенство.

и) Если $x = 1$, то $1 \vee 1' = 1$. Если $x = 0$, то $0 \vee 0' = 0 \vee 1 = 1$. Таким образом, первое равенство справедливо. Аналогично проверяется второе равенство.

к) Если $x = 1$, то $1'' = (1')' = 0' = 1$. Если $x = 0$, то $0'' = (0')' = 1' = 0$. Следовательно, $x'' = x$.

Теорема полностью доказана. $\square$

Свойства эквивалентности, импликации и отрицания. Свойства эквивалентности и импликации только частично аналогичны свойствам дизъюнкции или конъюнкции.

Теорема 9.4. Для булевых функций справедливы следующие равенства:

- а) $x \leftrightarrow x = 1, x \leftrightarrow x' = 0$;
- б) $x \leftrightarrow y = y \leftrightarrow x$ (коммутативность эквивалентности);
- в) $(x \leftrightarrow y) \leftrightarrow z = x \leftrightarrow (y \leftrightarrow z)$ (ассоциативность эквивалентности);
- г) $1 \leftrightarrow x = x, 0 \leftrightarrow x = x'$;
- д) $x' \leftrightarrow y' = x \leftrightarrow y$;
- е) $x' \rightarrow y' = y \rightarrow x$;
- ж) $x \rightarrow x = 1$;
- з) $x \rightarrow x' = x'$;
- и) $x' \rightarrow x = x$;
- к) $1 \rightarrow x = x$;
- л) $0 \rightarrow x = 1$;
- м) $x \rightarrow 1 = 1$;
- н) $x \rightarrow 0 = x'$.

Доказательство этих соотношений не представляет труда. Предлагается проделать их самостоятельно с помощью таблиц. $\square$

Заметим, что импликация не обладает ни свойством коммутативности, ни свойством ассоциативности. Предлагается самостоятельно исследовать вопрос о том, будут ли эквивалентность и импликация дистрибутивны (распределительны) одна относительно другой справа и слева.

Некоторые дополнительные свойства булевых функций рассмотрены в Задачнике (см. № 4.10 — 4.24).

Выражение одних булевых функций через другие. О взаимозависимостях булевых функций возникает много вопросов. Как выражаются одни булевы функции в виде суперпозиций других бу-

левых функций? Можно ли все булевы функции выразить через какие-то одни и те же функции? Существует ли такая булева функция, через которую выражаются все остальные? И так далее. В следующей теореме приводятся основные выражения одних булевых функций через другие, которые можно использовать при получении новых зависимостей между булевыми функциями.

Теорема 9.5. *Справедливы следующие равенства, выражающие одни булевы функции через другие:*

$$\begin{array}{ll} а) x \cdot y = (x' \vee y')'; & ж) x' = x \mid x; \\ б) x \vee y = (x' \cdot y')'; & з) x \mid y = (x \cdot y)'; \\ в) x \vee y = (x \rightarrow y) \rightarrow y; & и) x \vee y = x' \mid y' = (x \mid x) \mid (y \mid y); \\ г) x \vee y = x' \rightarrow y; & к) x' = x \downarrow x; \\ д) x \rightarrow y = x' \vee y; & л) x \downarrow y = (x \vee y)'; \\ е) x \leftrightarrow y = (x \rightarrow y) \cdot (y \rightarrow x); & м) x \cdot y = x' \downarrow y' = (x \downarrow x) \downarrow (y \downarrow y). \end{array}$$

Доказательство. Для *а)* и *б)* доказательства равенств легко следуют из законов де Моргана (теорема 9.3, *з*), если на обе части каждого из них «навесить» знак отрицания, а затем к левым частям полученных равенств применить равенство из теоремы 9.3, *к*.

Для *в)* и *г)* равенства можно проверить с помощью общего метода таблиц, а можно воспользоваться равенством *д)*, преобразуя, например, правую часть первого равенства. Тогда $(x \rightarrow y) \rightarrow y = (x' \vee y) \rightarrow y = (x' \vee y)' \vee y = (x'' \cdot y') \vee y = (x \cdot y') \vee y = (x \vee y) \cdot (y' \vee y) = (x \vee y) \cdot 1 = x \vee y$. При доказательстве были использованы, кроме того, соотношения теоремы 9.3, *з*, *к*, *е*, *и*, *г*.

д) Равенство легко проверяется с помощью таблиц.

е) Докажите, построив таблицы.

ж) и *к)* Соотношения непосредственно видны из таблиц, определяющих функции штрих Шеффера и стрелку Пирса.

з) и *л)* Равенства уже отмечались при определении функций штрих Шеффера и стрелка Пирса.

и) Можно составить таблицы, а можно рассуждать следующим образом: $x' \mid y' = (x' \cdot y')' = x \vee y$. В первом равенстве использовано предыдущее соотношение *з*).

м) Докажите равенство подобно тому как было доказано равенство *и)*, используя при этом соотношение *л)*. $\square$

§ 10. Булевы функции от n аргументов

Понятие булевой функции. В предыдущем параграфе мы уже говорили о булевых функциях от одного и от двух аргументов. Введем понятие булевой функции от произвольного конечного числа аргументов.

Определение 10.1. *Булевой функцией от n аргументов* называется функция f , заданная на множестве $\{0, 1\}^n$ и принимающая значения в двухэлементном множестве $\{0, 1\}$. Другими словами, булева

функция от n аргументов сопоставляет каждому упорядоченному набору длины n , составленному из элементов 0 и 1, либо 0, либо 1.

Булева функция f от n аргументов $x_1, x_2, \dots, x_n$ обозначается так: $f(x_1, x_2, \dots, x_n)$.

Две булевы функции от n аргументов $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_n)$ называются *равными*, если любым одинаковым набором значений аргументов $x_1, x_2, \dots, x_n$ обе эти функции сопоставляют одинаковые элементы из множества $\{0, 1\}$, т.е. $f(a_1, a_2, \dots, a_n) = g(a_1, a_2, \dots, a_n)$ для любых элементов $a_1, a_2, \dots, a_n \in \{0, 1\}$.

В § 9 уже встречались булевы функции от трех аргументов, например

$$f_1(x_1, x_2, x_3) = (x_1 \vee x_2) \vee x_3, f_2(x_1, x_2, x_3) = x_1 \vee (x_2 \vee x_3),$$

$$g_1(x_1, x_2, x_3) = x_1 \vee (x_2 \cdot x_3), g_2(x_1, x_2, x_3) = (x_1 \vee x_2) \cdot (x_1 \vee x_3).$$

В частности, было показано, что $f_1(x_1, x_2, x_3) = f_2(x_1, x_2, x_3)$ и $g_1(x_1, x_2, x_3) = g_2(x_1, x_2, x_3)$. Перечисленные функции построены с помощью суперпозиций (или последовательного применения) более простых функций.

Определение 10.2. Суперпозицией булевых функций $g_1(y_1^1, y_1^2, \dots, y_1^{m_1}), \dots, g_n(y_n^1, y_n^2, \dots, y_n^{m_n})$ в булеву функцию $f(x_1, x_2, \dots, x_n)$ называется новая булева функция, получающаяся из функции $f(x_1, x_2, \dots, x_n)$ подстановкой вместо (всех или некоторых) аргументов $x_1, x_2, \dots, x_n$ функций $g_1, g_2, \dots, g_n$ соответственно $f(g_1(y_1^1, \dots, y_1^{m_1}), \dots, g_n(y_n^1, \dots, y_n^{m_n}))$. Полученная функция $F(y_1^1, \dots, y_1^{m_1}, \dots, y_n^1, \dots, y_n^{m_n})$ зависит от $m_1 + m_2 + \dots + m_n$ аргументов.

Например, если $f(u, x_3) = u \vee x_3$, $h_1(x_1, x_2) = x_1 \vee x_2$, то $F_1(x_1, x_2, x_3) = f(h_1(x_1, x_2), x_3) = (x_1 \vee x_2) \vee x_3$.

Или если $g(u, v) = u \cdot v$, $h_2(x_1, x_2) = x_1 \vee x_2$, $h_3(x_1, x_3) = x_1 \vee x_3$, то $F_2(x_1, x_2, x_3) = g(h_2(x_1, x_2), h_3(x_1, x_3)) = (x_1 \vee x_2) \cdot (x_1 \vee x_3)$.

Опишем еще одну процедуру, которую можно проделывать с булевыми функциями. Зафиксировав один из аргументов булевой функции $f(x_1, x_2, \dots, x_n)$ от n аргументов, т.е. придав этому аргументу какое-нибудь конкретное постоянное значение (из двухэлементного множества $\{0, 1\}$), получим функцию от $n-1$ аргументов. Так, фиксируя в функции $f(x_1, x_2, \dots, x_n)$ k -й аргумент ($1 \leq k \leq n$), можем получить две новые булевы функции от $n-1$ аргументов:

$$f(x_1, \dots, x_{k-1}, 0, x_{k+1}, \dots, x_n) \text{ и } f(x_1, \dots, x_{k-1}, 1, x_{k+1}, \dots, x_n).$$

Например, из функции от трех аргументов $F_2(x_1, x_2, x_3) = (x_1 \vee x_2) \cdot (x_1 \vee x_3)$ фиксированием первого аргумента получаем следующие функции от двух аргументов:

$$h'(x_2, x_3) = F_2(0, x_2, x_3) = (0 \vee x_2) \cdot (0 \vee x_3) = x_2 \cdot x_3;$$

$$h''(x_2, x_3) = F_2(1, x_2, x_3) = (1 \vee x_2) \cdot (1 \vee x_3) = 1 \cdot 1 = 1.$$

Предлагаем посмотреть самостоятельно, какие получатся функции из функции $F_2(x_1, x_2, x_3)$ при последовательном фиксировании остальных ее аргументов x_2, x_3 .

Число булевых функций. Перечислив в § 9 все булевы функции от одного аргумента и от двух аргументов, мы видели, что первых

имеется всего четыре, а вторых — шестнадцать. Возникает вопрос, сколько будет разных булевых функций от трех аргументов, от четырех аргументов и т.д. Нельзя ли указать формулу, по которой вычислялось бы число булевых функций от n аргументов? Ответ на поставленный вопрос дает следующая теорема.

Теорема 10.3 (о числе булевых функций от n аргументов). *Число различных булевых функций от n аргументов равно 2^{2^n} .*

Доказательство. Чтобы задать булеву функцию $f(x_1, \dots, x_n)$ от n аргументов, нужно перечислить все наборы $(a_1, \dots, a_n)$ из нулей и единиц значений, которые могут принимать ее аргументы $x_1, \dots, x_n$, и для каждого такого набора указать значение функции f , которое она принимает на этом наборе.

Выясним сначала, сколько существует различных наборов $(a_1, \dots, a_n)$, составленных из нулей и единиц, значений для n аргументов $x_1, \dots, x_n$. Покажем, что это число равно 2^n . Доказательство будем вести методом математической индукции по числу n . В самом деле, для $n = 1$ имеется всего два набора значений переменного x_1 . Это 0 и 1. Так что для $n = 1$ число наборов равно 2^1 . Предположим, что для k аргументов имеется точно 2^k различных наборов $(a_1, \dots, a_k)$, составленных из 0 и 1, значений для k аргументов. Тогда среди всевозможных различных наборов $(a_1, \dots, a_k, a_{k+1})$ значений для $k+1$ аргумента имеется, согласно предположению индукции, точно 2^k наборов вида $(a_1, \dots, a_k, 0)$ и точно 2^k наборов вида $(a_1, \dots, a_k, 1)$. Следовательно, всего будет $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ различных наборов. Тем самым доказано с помощью индукции утверждение о числе различных наборов.

Таким образом, для задания функции f от n аргументов нужно указать ее значение для каждого из 2^n различных наборов значений ее аргументов. Если каждое значение функции равно нулю, то такая функция постоянна. Она называется константа 0. Если каждое значение функции равно единице, то это вторая постоянная функция, называемая константа 1. Мы указали лишь две различные функции от n аргументов. Сколько же их существует всего? Ровно столько, сколько имеется разных наборов длины 2^n , составленных из нулей и единиц (см. таблицу).

Аргументы ($x_1, \dots, x_{n-1}, x_n$)	Булевы функции					
	f_0	f_1	f_2	...	f_{m-2}	f_{m-1}
(0, ..., 0, 0)	0	0	0	...	1	1
(0, ..., 0, 1)	0	0	0	...	1	1
(0, ..., 1, 0)	0	0	0	...	1	1
(0, ..., 1, 1)	0	0	0	...	1	1
...	...	...	...	...	...	...
(1, ..., 1, 0)	0	0	1	...	1	1
(1, ..., 1, 1)	0	1	0	...	0	1

Разных наборов длины 2^n , составленных из нулей и единиц, как показано в начале доказательства теоремы, имеется 2^l , где $l = 2^n$ — длина набора. Таким образом, число m разных булевых функций от n аргументов равно точно $2^l = 2^{2^n}$. Теорема доказана. $\square$

Выражение булевых функций через конъюнкцию, дизъюнкцию и отрицание. У нас уже возникали вопросы относительно выражения одних булевых функций через другие, и на некоторые из них мы уже дали ответ. Как будет показано ниже, существуют такие булевы функции (уже хорошо известные нам), через которые выражаются все (вообще все, от любого числа аргументов!) булевы функции. Этим замечательным свойством обладают взятые вместе конъюнкция, дизъюнкция и отрицание. Прежде чем сформулировать и доказать основную теорему этого пункта, обратимся к следующей важной лемме.

Лемма 10.4 (о разложении функции по переменной). *Для произвольной булевой функции $f(x_1, x_2, \dots, x_n)$ справедливы следующие формулы, называемые формулами разложения этой функции по переменной x_1 :*

$$f(x_1, x_2, \dots, x_n) = (x_1 \cdot f(1, x_2, \dots, x_n)) \vee (x_1' \cdot f(0, x_2, \dots, x_n));$$

$$f(x_1, x_2, \dots, x_n) = (x_1 \vee f(0, x_2, \dots, x_n)) \cdot (x_1' \vee f(1, x_2, \dots, x_n)).$$

Доказательство. Докажем справедливость первой формулы. Нужно проверить, что функции, стоящие в обеих частях равенства, при одинаковых значениях их аргументов принимают равные значения. Рассмотрим сначала всевозможные наборы значений аргументов следующего вида $(0, a_2, \dots, a_n)$, т.е. будем придавать аргументам $x_1, x_2, \dots, x_n$ значения: $x_1 = 0, x_2 = a_2, \dots, x_n = a_n$. При этом безразлично, каковы именно значения $a_2, \dots, a_n$. Вычислив, какое значение принимает на наборах такого вида функция, стоящая в правой части доказываемого равенства, убедимся, что оно совпадает со значением, принимаемым функцией, стоящей в левой части этого равенства, на том же наборе значений аргументов. В самом деле, $(0 \cdot f(1, a_2, \dots, a_n)) \vee (0' \cdot f(0, a_2, \dots, a_n)) = 0 \vee (1 \cdot f(0, a_2, \dots, a_n)) = 0 \vee f(0, a_2, \dots, a_n) = f(0, a_2, \dots, a_n)$.

Теперь рассмотрим всевозможные наборы значений аргументов вида $(1, a_2, \dots, a_n)$, т.е. будем придавать аргументам $x_1, x_2, \dots, x_n$ значения: $x_1 = 1, x_2 = a_2, \dots, x_n = a_n$. Аналогично вычисляем значение, принимаемое функцией, стоящей в правой части доказываемого равенства, на наборах такого вида: $(1 \cdot f(1, a_2, \dots, a_n)) \vee (1' \cdot f(0, a_2, \dots, a_n)) = f(1, a_2, \dots, a_n) \vee (0 \cdot f(0, a_2, \dots, a_n)) = f(1, a_2, \dots, a_n) \vee 0 = f(1, a_2, \dots, a_n)$.

Итак, функции из обеих частей равенства принимают одинаковые значения при одинаковых значениях их аргументов. Следовательно, эти функции равны и доказываемая формула справедлива.

Совершенно аналогично доказывается вторая формула. $\square$

Заметим, что подобным образом могут быть записаны формулы разложения булевой функции по любой ее переменной. Запишите, например, такие разложения по последней переменной.

Теорема 10.5 (о представлении булевых функций через конъюнкцию, дизъюнкцию и отрицание). *Всякая булева функция $f(x_1, x_2, \dots, x_n)$ может быть представлена в виде суперпозиции конъюнкции, дизъюнкции и отрицания; причем знак отрицания стоит только непосредственно около переменной и не стоит ни перед одной из внутренних скобок.*

Доказательство будем вести методом математической индукции по числу n аргументов функции f .

В предыдущем параграфе перечислены все булевы функции от одного аргумента. Их всего четыре. Напомним их (используя равенства теоремы 9.3, и): $f_0(x) = 0 = x \cdot x'$, $f_1(x) = x$, $f_2(x) = x'$, $f_3(x) = 1 = x \vee x'$. Отсюда видно, что все функции от одного аргумента выражаются через конъюнкцию, дизъюнкцию и отрицание; причем знак отрицания стоит только непосредственно около переменных. Это означает, что утверждение теоремы справедливо при $n = 1$.

Предположим, что теорема верна для всех функций от k аргументов. Докажем ее для функций от $k + 1$ аргумента. Пусть $f(x_1, \dots, x_k, x_{k+1})$ — произвольная булева функция от $k + 1$ аргумента. На основании предыдущей леммы запишем разложение данной функции по последней переменной: $f(x_1, \dots, x_k, x_{k+1}) = (x_{k+1} \cdot f(x_1, \dots, x_k, 1)) \vee (x'_{k+1} \cdot f(x_1, \dots, x_k, 0))$. Как отмечалось в начале настоящего параграфа, фиксирование в булевой функции одного аргумента приводит к булевой функции с числом аргументов на единицу меньше, нежели число аргументов исходной функции. Так что каждая из функций $f(x_1, \dots, x_k, 1)$ и $f(x_1, \dots, x_k, 0)$ есть булева функция от k аргументов. Но согласно предположению индукции, все такие функции выражаются через конъюнкцию, дизъюнкцию и отрицание, причем знак отрицания стоит только непосредственно около переменных и не стоит ни перед одной из внутренних скобок. Принимая это во внимание, видим, что правая часть последнего равенства представляет собой суперпозицию лишь трех функций — конъюнкции, дизъюнкции и отрицания. Причем отрицание стоит около переменной x_{k+1} . Это и доказывает окончательно теорему. $\square$

Булевы функции и формулы алгебры высказываний. Установим сначала соответствие между формулами алгебры высказываний и булевыми функциями. Это делается следующим образом. Во-первых, определяется взаимно-однозначное соответствие между пропозициональными переменными и булевыми переменными, при котором прописная буква, обозначающая пропозициональную переменную, соответствует той же самой строчной букве, обозначающей булеву переменную:

$$\begin{aligned} P, Q, R, X, Y, Z, X_1, X_2, \dots, Y_1, Y_2, \dots \\ p, q, r, x, y, z, x_1, x_2, \dots, y_1, y_2, \dots \end{aligned}$$

Во-вторых, устанавливается соответствие между знаками логических связей и одноименных булевых функций:

Логические связи	$\neg$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
Булевы функции	$'$	$\cdot$	$\vee$	$\rightarrow$	$\leftrightarrow$

Наконец скобкам ставятся в соответствие те же скобки. Тогда каждой формуле алгебры высказываний соответствует единственная булева функция, а каждой булевой функции соответствует формула алгебры высказываний. Чтобы найти для данной формулы алгебры высказываний соответствующую ей булеву функцию, достаточно каждую прописную букву формулы заменить на такую же строчную букву, а каждый символ логической операции — на символ одноименной булевой функции.

Например, формуле $(P \leftrightarrow \neg Q) \rightarrow ((\neg X_1 \vee X_2) \wedge \neg Z)$ соответствует булева функция $(p \leftrightarrow q') \rightarrow ((x_1' \vee x_2) \cdot z')$.

Если булева функция задана с помощью формулы, то для того чтобы найти соответствующую этой функции формулу алгебры высказываний, нужно в выражении для булевой функции заменить строчные буквы такими же прописными буквами, а каждый символ булевой функции $'$, $\cdot$, $\vee$, $\rightarrow$, $\leftrightarrow$ заменить соответственно символом одноименной логической операции $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$. Здесь возникает неоднозначность такого обратного соответствия, поскольку булева функция может иметь множество различных формульных выражений. Например, функция, рассмотренная в предыдущем абзаце, имеет также следующие формульные выражения:

$$\begin{aligned}(p \leftrightarrow q') &\rightarrow (x_1' \cdot z' \vee x_2 \cdot z'); \\ ((p \rightarrow q') \cdot (q' \rightarrow p)) &\rightarrow ((x_1' \vee x_2) \cdot z'); \\ ((p' \vee q') \cdot (p \vee q)) &\rightarrow (x_1' \cdot z' \vee x_2 \cdot z') \text{ и т. д.}\end{aligned}$$

Этим выражениям сопоставляются соответственно следующие формулы алгебры высказываний:

$$\begin{aligned}(P \leftrightarrow \neg Q) &\rightarrow ((\neg X_1 \wedge \neg Z) \vee (X_2 \wedge \neg Z)); \\ ((P \rightarrow \neg Q) \wedge (\neg Q \rightarrow P)) &\rightarrow ((\neg X_1 \vee X_2) \wedge \neg Z); \\ ((\neg P \vee \neg Q) \wedge (P \vee Q)) &\rightarrow ((\neg X_1 \wedge \neg Z) \vee (X_2 \wedge \neg Z)) \text{ и т. д.}\end{aligned}$$

Следовательно, все перечисленные формулы соответствуют одной и той же булевой функции.

Возникает вопрос, всякой ли булевой функции соответствует некоторая формула алгебры высказываний. Другими словами, всякая ли булева функция может быть выражена (представлена) некоторой формулой алгебры высказываний. Если булева функция задана с помощью формулы, то соответствующая этой функции формула алгебры высказываний отыскивается так, как описано в предыдущем абзаце. Если же булева функция задана не в виде формулы, то, в силу теоремы 10.5, формульное выражение для нее тем не менее существует, и, следовательно, представляющая

ее формула алгебры высказываний может быть найдена по правилу, описанному выше.

Итак, отметим еще раз, что каждой формуле алгебры высказываний соответствует единственная определяемая этой формулой булева функция, что будет для нас важным в дальнейшем.

Нормальные формы булевых функций. На основе теоремы 10.5 всякая булева функция может быть представлена некоторой формулой алгебры высказываний. Нетрудно понять, что всякая формула алгебры высказываний, *равносильная* формуле, представляющей некоторую булеву функцию f , будет представлять функцию, равную f . В частности, одной из таких представляющих формул будет совершенная дизъюнктивная нормальная форма (если данная булева функция не равна тождественно 0, т.е. представляющая формула не тождественно ложна) или совершенная конъюнктивная нормальная форма (если данная булева функция не равна тождественно 1, т.е. представляющая формула не является тавтологией). Отыскав совершенную нормальную форму для формулы алгебры высказываний, представляющей данную булеву функцию (применяя правила, полученные в теоремах 5.2 и 5.4), можно перейти от этой формы к формульному выражению для данной булевой функции. Его будем называть *совершенной (дизъюнктивной или конъюнктивной) нормальной формой* данной булевой функции, сокращенно *СДН-формой* или соответственно *СКН-формой*. Каждая из них для данной булевой функции, если она существует, единственна.

Приобретя опыт работы с булевыми функциями, можно отыскивать их нормальные формы, не переходя к символике алгебры высказываний. При этом, если функция задана каким-то формульным выражением, то для его тождественного преобразования следует пользоваться свойствами булевых функций, установленными в теоремах 9.3—9.5, а если функция задана своими значениями на всех наборах значений аргументов (т.е. если она задана таблично), то следует применять правила, полученные в теоремах 5.2 и 5.4, переведя их предварительно на язык булевых функций.

§ 11. Системы булевых функций

В теореме 10.5 доказано, что всякая булева функция может быть представлена в виде суперпозиции трех булевых функций: дизъюнкции, конъюнкции и отрицания. В настоящем параграфе тема представления булевых функций в виде суперпозиций функций из некоторой системы развивается и доводится до определенного конца: приводятся необходимые и достаточные условия (теорема 11.4 Поста), которым должна удовлетворять система булевых функций для того, чтобы всякая булева функция могла быть представлена в виде суперпозиции функций из этой системы.

Полные системы булевых функций. Напомним, что понятие суперпозиции булевых функций обсуждалось в § 10 (определение 10.2).

Определение 11.1. Система булевых функций называется *полной*, если всякая булева функция является суперпозицией функций из этой системы.

Теорема 11.2. Следующие системы булевых функций являются полными: 1) $\{\vee, \cdot, '\}$; 2) $\{+, \cdot, '\}$; 3) $\{\vee, '\}$; 4) $\{\cdot, '\}$; 5) $\{\rightarrow, '\}$; 6) $\{|\}$; 7) $\{\downarrow\}$.

Доказательство. Полнота первой системы доказана в теореме 10.5. Это можно использовать для доказательства полноты остальных систем, приведенных в теореме.

В силу полноты системы $\{\vee, \cdot, '\}$ каждая булева функция является суперпозицией дизъюнкции, конъюнкции и отрицания. Если мы сможем выразить дизъюнкцию через функции $+$, $\cdot$ и $'$, то тем самым докажем, что всякую функцию можно выразить через эти функции, т.е. докажем полноту системы функций $\{+, \cdot, '\}$. Это можно сделать так: $x \vee y = x + y + x \cdot y$. Предлагается самостоятельно проверить справедливость приведенного тождества.

Аналогично, для проверки полноты системы $\{\vee, '\}$ нужно выразить конъюнкцию через дизъюнкцию и отрицание. Соответствующее тождество известно (см. теорему 9.5, а).

Полнота системы $\{\cdot, '\}$ вытекает из полноты системы $\{\vee, \cdot, '\}$ и тождества теоремы 9.5, б, выражающего дизъюнкцию через конъюнкцию и отрицание, а полнота системы $\{\rightarrow, '\}$ — из полноты системы $\{\vee, '\}$ и тождества теоремы 9.5, в, выражающего дизъюнкцию через импликацию.

Наконец система $\{|\}$ полна, потому что каждая функция есть суперпозиция функций $\vee$ и $'$, а обе эти функции могут быть выражены через функцию штрих Шеффера (см. теорему 9.5, ж, и). Аналогично, система $\{\downarrow\}$ полна, так как полна система $\{\cdot, '\}$ и справедливы тождества теоремы 9.5, к, м, выражающие функции $\cdot$ и $'$ через стрелку Пирса $\downarrow$.

Теорема доказана. $\square$

Теперь от разрозненных и случайных примеров полных систем булевых функций перейдем к их исчерпывающему описанию. Прежде чем получить такое описание, в следующем пункте рассмотрим необходимые предварительные понятия.

Специальные классы булевых функций. Говорят, что булева функция $f(x_1, x_2, \dots, x_n)$ *сохраняет* 0, если $f(0, 0, \dots, 0) = 0$. Обозначим P_0 — класс всех булевых функций, сохраняющих 0.

Говорят, что булева функция $f(x_1, x_2, \dots, x_n)$ *сохраняет* 1, если $f(1, 1, \dots, 1) = 1$. Обозначим P_1 — класс всех булевых функций, сохраняющих 1.

Булева функция $f^*(x_1, x_2, \dots, x_n)$ называется *двойственной* функцией для булевой функции $f(x_1, x_2, \dots, x_n)$, если $f^*(x_1, x_2, \dots, x_n) = f'(x_1', x_2', \dots, x_n')$ для любых $x_1, x_2, \dots, x_n$. Булева функция f назы-

вается *самодвойственной*, если $f^* = f$. Класс всех самодвойственных булевых функций обозначим S .

Введем на множестве $\{0, 1\}$ отношение порядка, полагая, что $0 \leq 0, 0 \leq 1, 1 \leq 1$. Булева функция $f(x_1, x_2, \dots, x_n)$ называется *монотонной*, если для любых $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in \{0, 1\}$ из $\alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2, \dots, \alpha_n \leq \beta_n$ немедленно следует, что $f(\alpha_1, \alpha_2, \dots, \alpha_n) \leq f(\beta_1, \beta_2, \dots, \beta_n)$. Класс всех монотонных функций обозначим M .

Наконец, булева функция $f(x_1, x_2, \dots, x_n)$ называется *линейной*, если ее можно представить в виде следующего выражения (называемого полиномом Жегалкина степени не выше первой): $f(x_1, x_2, \dots, x_n) = a_0 + a_1x_1 + a_2x_2 + \dots + a_nx_n$, где $a_0, a_1, a_2, \dots, a_n$ — постоянные, равные либо 0, либо 1. Символом L обозначим класс всех линейных булевых функций.

Введенные классы булевых функций P_0, P_1, S, M, L играют главную роль при описании полных систем булевых функций. В следующей теореме устанавливаются два важных свойства этих классов и одновременно рассматриваются примеры функций, принадлежащих и не принадлежащих каждому из них.

Класс булевых функций называется *собственным*, если он не пуст и не совпадает с классом всех булевых функций. Класс булевых функций называется *замкнутым* или *классом Поста*, если он вместе со всякими своими функциями содержит любую их суперпозицию.

Теорема 11.3. *Классы P_0, P_1, S, M, L являются собственными замкнутыми классами булевых функций.*

Доказательство. Проверим сначала, что все эти классы являются собственными. Укажем функции, которые принадлежат и не принадлежат каждому из рассматриваемых классов, предоставляя читателю проверить самостоятельно данные утверждения. Как классу P_0 , так и классу P_1 принадлежит, например, конъюнкция и не принадлежит отрицание. Далее, конъюнкция не является самодвойственной функцией, а отрицание есть функция самодвойственная. (Проверим последнее утверждение. Пусть $f(x) = x'$. Тогда $f^*(x) = f'(x') = (f(x'))' = (x'')' = x' = f(x)$, т.е. $f^* = f$, а значит, $f(x) = x'$ — самодвойственная функция.) Наконец, к классу монотонных функций принадлежит конъюнкция и не принадлежит импликация, а к классу L линейных функций принадлежит сложение по модулю два (сумма Жегалкина) и не принадлежит конъюнкция.

Покажем теперь замкнутость этих классов. Пусть $f_1, f_2, f_3 \in P_0$, т.е. $f(0, 0) = f_2(0, 0) = f_3(0, 0) = 0$, и $g(x_1, x_2) = f_1(f_2(x_1, x_2), f_3(x_1, x_2))$. Тогда $g(0, 0) = f_1(f_2(0, 0), f_3(0, 0)) = f_1(0, 0) = 0$, т.е. $g \in P_0$.

Аналогично проверяется замкнутость класса P_1 .

Пусть теперь $f_1, f_2, f_3 \in S$, т.е. $f_1'(u, v) = f_1(u', v'), f_2'(x_1', x_2') = f_2(x_1, x_2), f_3'(x_1', x_2') = f_3(x_1, x_2)$ и $g(x_1, x_2) = f_1(f_2(x_1, x_2), f_3(x_1, x_2))$. Тогда $g^*(x_1, x_2) = g'(x_1', x_2') = f_1'(f_2(x_1', x_2'), f_3(x_1', x_2')) = f_1(f_2'(x_1', x_2'), f_3'(x_1', x_2'))$.

$f_3'(x_1', x_2')) = f_1(f_2(x_1, x_2), f_3(x_1, x_2)) = g(x_1, x_2)$, т.е. $g^* = g$ и значит $g \in S$.

Пусть далее $f_1, f_2, f_3 \in M$ и $\alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2$ и $g(x_1, x_2) = f_1(f_2(x_1, x_2), f_3(x_1, x_2))$. Тогда $f_2(\alpha_1, \alpha_2) \leq f_2(\beta_1, \beta_2), f_3(\alpha_1, \alpha_2) \leq f_3(\beta_1, \beta_2)$ и $g(\alpha_1, \alpha_2) = f_1(f_2(\alpha_1, \alpha_2), f_3(\alpha_1, \alpha_2)) \leq f_1(f_2(\beta_1, \beta_2), f_3(\beta_1, \beta_2)) = g(\beta_1, \beta_2)$. Следовательно, $g \in M$.

Наконец, пусть $f_1, f_2, f_3 \in L$, т.е., например, $f_1(x_1, x_2) = a_0 + a_1x_1 + a_2x_2, f_2(x_1, x_2) = b_0 + b_1x_1 + b_2x_2, f_3(x_1, x_2) = c_0 + c_1x_1 + c_2x_2$. Тогда $g(x_1, x_2) = f_1(f_2(x_1, x_2), f_3(x_1, x_2)) = a_0 + a_1 \cdot f_2(x_1, x_2) + a_2 \cdot f_3(x_1, x_2) = a_0 + a_1 \cdot (b_0 + b_1x_1 + b_2x_2) + a_2 \cdot (c_0 + c_1x_1 + c_2x_2) = (a_0 + a_1b_0 + a_2c_0) + (a_1b_1 + a_2c_1) \cdot x_1 + (a_1b_2 + a_2c_2) \cdot x_2 = d_0 + d_1x_1 + d_2x_2$, т.е. $g \in L$.

Теорема доказана. $\square$

Заметим, что, например, функция $f(x) = x$ принадлежит каждому из пяти классов P_0, P_1, S, M, L .

Теорема Поста о полноте системы булевых функций. Эта теорема доказана американским математиком Э. Постом в 1921 г.

Теорема 11.4 (о полноте системы булевых функций). Система булевых функций $\{f_0, f_1, \dots, f_s, \dots\}$ является полной тогда и только тогда, когда в этой системе имеется функция, не принадлежащая классу P_0 , имеется функция, не принадлежащая классу P_1 , имеется функция, не принадлежащая классу S , имеется функция, не принадлежащая классу M , имеется функция, не принадлежащая классу L .

Доказательство. Необходимость. Пусть система булевых функций $\{f_0, f_1, \dots, f_s, \dots\}$ полна. Допустим, что все функции этой системы входят в класс P_0 . Поскольку на основании предыдущей теоремы класс P_0 замкнут, то всякая суперпозиция любых функций из данной системы есть функция из класса P_0 . Но также по предыдущей теореме класс P_0 не исчерпывает всех булевых функций. Поэтому найдется булева функция (не принадлежащая классу P_0), которая не является суперпозицией функций из системы $\{f_0, f_1, \dots, f_s, \dots\}$, что противоречит полноте этой системы. Следовательно, в системе имеется функция, не принадлежащая классу P_0 .

Совершенно аналогично доказываются утверждения о наличии в системе $\{f_0, f_1, \dots, f_s, \dots\}$ функций, не принадлежащих классам P_1, S, M, L .

Достаточность. Предположим, что среди функций системы $\{f_0, f_1, \dots, f_s, \dots\}$ имеются такие функции f_0, f_1, f_2, f_3, f_4 , что $f_0 \notin P_0, f_1 \notin P_1, f_2 \notin S, f_3 \notin M, f_4 \notin L$. Покажем, что из этих пяти функций с помощью суперпозиций можно сконструировать такие функции, которые заведомо образуют полную систему.

Начнем с f_0 , для которой $f_0(0, 0, \dots, 0) = 1$. Введем функцию $\tilde{f}_0(x) = f_0(x, x, \dots, x)$. Для нее имеем: $\tilde{f}_0(0) = 1, \tilde{f}_0(1) = 0$ или 1. Следовательно, $\tilde{f}_0(x) = x'$ или $\tilde{f}_0(x) = 1$.

Аналогично, из f_1 , для которой $f_1(1, 1, \dots, 1) = 0$, строим функцию $\tilde{f}_1(x) = f_1(x, x, \dots, x)$. Для нее имеем: $\tilde{f}_1(1) = 0, \tilde{f}_1(0) = 1$ или 0. Следовательно, $\tilde{f}_1(x) = x'$ или $\tilde{f}_1(x) = 0$.

Таким образом, получаем одну из следующих четырех пар функций: x' и x' (1); x' и 0 (2); x' и 1 (3); 0 и 1 (4).

В каждом из случаев (2) и (3) имеем тогда по три функции x' , 0, 1 (например, если есть функции x' и 0, то константа 1 получается как $0'$).

Рассмотрим случай (1). Покажем, что и здесь можно получить обе константы 0 и 1. Для этого привлечем несамодвойственную функцию f_2 (т.е. $f_2 \notin S$). Для нее $f_2 \neq f_2^*$, т.е. $f_2(\alpha_1, \alpha_2, \dots, \alpha_n) \neq f_2'(\alpha_1', \alpha_2', \dots, \alpha_n')$ для *некоторого* набора $\alpha_1, \alpha_2, \dots, \alpha_n$ из нулей и единиц. Следовательно, для этого набора $f_2(\alpha_1, \alpha_2, \dots, \alpha_n) = f_2(\alpha_1', \alpha_2', \dots, \alpha_n')$. Построим теперь функцию $\tilde{f}_2(x)$ по следующему правилу: $\tilde{f}_2(x) = f_2(x^{\alpha_1}, x^{\alpha_2}, \dots, x^{\alpha_n})$, где

$$x^{\alpha_i} = \begin{cases} x, & \text{если } \alpha_i = 0, \\ x', & \text{если } \alpha_i = 1, \end{cases}$$

для $1 \leq i \leq n$. Для функции имеем: $\tilde{f}_2(0) = f_2(\alpha_1, \alpha_2, \dots, \alpha_n) = f_2(\alpha_1', \alpha_2', \dots, \alpha_n') = \tilde{f}_2(1)$. Следовательно, $\tilde{f}_2(x)$ — константа. Поскольку в нашем распоряжении имеется отрицание x' , то из этой константы (0 или 1) можно получить и другую константу (1 или 0 соответственно). Итак, в случае (1) имеем функции x' , 0, 1.

Рассмотрим случай (4). Здесь к константам 0 и 1 необходимо получить функцию x' . Для этого привлечем немонотонную функцию f_3 (т.е. $f_3 \notin M$). Ее немонотонность означает: найдутся такие наборы из нулей и единиц $(\alpha_1, \alpha_2, \dots, \alpha_n)$ и $(\beta_1, \beta_2, \dots, \beta_n)$, что $(\alpha_1, \alpha_2, \dots, \alpha_n) \leq (\beta_1, \beta_2, \dots, \beta_n)$, но $f(\alpha_1, \alpha_2, \dots, \alpha_n) > f(\beta_1, \beta_2, \dots, \beta_n)$. Построим функцию $\tilde{f}_3(x)$ по следующему правилу: $\tilde{f}_3(x) = f_3(x^{\alpha_1}, x^{\alpha_2}, \dots, x^{\alpha_n})$, где

$$x^{\gamma_i} = \begin{cases} 0, & \text{если } \alpha_i = \beta_i = 0, \\ 1, & \text{если } \alpha_i = \beta_i = 1, \\ x, & \text{если } \alpha_i = 0, \beta_i = 1, \end{cases}$$

для $1 \leq i \leq n$. Тогда ясно, что $\tilde{f}_3(0) > \tilde{f}_3(1)$. Следовательно, должно быть $\tilde{f}_3(0) = 1$, $\tilde{f}_3(1) = 0$. Значит, $\tilde{f}_3(x) = x'$.

Итак, из данной системы функций с помощью суперпозиций нами сконструированы функции x' , 0, 1.

Рассмотрим теперь еще не использованную нами нелинейную функцию f_4 (т.е. $f_4 \notin L$). Предположим, что x_1 — тот ее аргумент, который в разложение в полином Жегалкина функции f_4 входит нелинейно. Это означает, что f_4 может быть представлена в виде

$$f_4(x_1, x_2, \dots, x_n) = x_1 \cdot \varphi(x_2, \dots, x_n) + \psi(x_2, \dots, x_n),$$

где $\varphi \neq 0$, $\varphi \neq 1$ (в противном случае функция f_4 имела бы два различных представления полиномами Жегалкина, что невозможно). По-

этому, если $\varphi(0, \dots, 0) = a$, то найдется такой набор $\alpha_2, \dots, \alpha_n$, что $\varphi(\alpha_2, \dots, \alpha_n) = a'$. Построим функцию $\tilde{f}_4(x, y)$ по следующему правилу: $\tilde{f}_4(x, y) = x \cdot \tilde{\varphi}(y) + \tilde{\psi}(y)$, где $x = x_1$, $\tilde{\varphi}(y) = \varphi(y^{\alpha_2}, \dots, y^{\alpha_n})$, $\tilde{\psi}(y) = \psi(y^{\alpha_2}, \dots, y^{\alpha_n})$, где, в свою очередь,

$$y^{\alpha_i} = \begin{cases} 0, & \text{если } \alpha_i = 0; \\ y, & \text{если } \alpha_i = 1, \end{cases}$$

для $2 \leq i \leq n$. (Заметим, что мы можем подставлять 0 вместо x_i , так как функция 0 нами уже получена.) Тогда ясно, что $\tilde{\varphi}(0) = \varphi(0, \dots, 0) = a$, $\tilde{\varphi}(1) = \varphi(\alpha_2, \dots, \alpha_n) = a'$. Следовательно, $\tilde{\varphi}(y) = y$ или $\tilde{\varphi}(y) = y'$. Заметим, что $y' = y + 1$ (см. Задачник, № 4.47, а). Значит, $\tilde{\varphi}(y)$ можно представить в виде $\tilde{\varphi}(y) = y + b_0$, где $b_0 = 0$ или 1. Кроме того, ясно, что функцию одного аргумента $\tilde{\psi}(y)$ можно представить в виде линейного полинома Жегалкина: $\tilde{\psi}(y) = b_1 y + b_2$. Таким образом, $\tilde{f}_4(x, y)$ имеет вид: $\tilde{f}_4(x, y) = x(y + b_0) + (b_1 y + b_2) = xy + bx + cy + d$.

Рассмотрим всевозможные случаи для коэффициентов b, c, d .

Если $b = c = d = 0$, то $\tilde{f}_4(x, y) = x \cdot y$.

Если $b = 1$, то рассмотрим функцию $\tilde{f}_4'(x, y) = \tilde{f}_4(x, y') = xy' + x + cy' + d = x(y + 1) + x + c(y + 1)d = xy + x + x + cy + c + d = xy + cy + c_1$. (Заметим, что мы можем подставлять y' вместо y , так как функция «отрицание» нами уже получена.)

Если $c = c_1 = 0$, то $\tilde{f}_4'(x, y) = x \cdot y$.

Если $c = 1$, то рассмотрим функцию $\tilde{f}_4''(x, y) = \tilde{f}_4'(x', y) = x'y + y + c_1 = (x + 1)y + y + c_1 = xy + y + y + c_1 = xy + c_1$.

Если в ней $c_1 = 0$, то $\tilde{f}_4''(x, y) = x \cdot y$.

Если же $c_1 = 1$, то $\tilde{f}_4''(x, y) = xy + 1 = (x \cdot y)' = x \mid y$ (штрих Шеффера).

Итак, из функций f_0, f_1, f_2, f_3, f_4 , имеющих в данной системе функций, мы получаем с помощью суперпозиций функции x' и $x \cdot y$ или же функцию $x \mid y$. Поскольку на основании теоремы 11.2 каждая из систем булевых функций $\{', \cdot\}$ и $\{\mid\}$ полна, то и данная система булевых функций $\{f_0, f_1, \dots, f_s, \dots\}$ полна.

Теорема полностью доказана. $\square$

§ 12. Применение булевых функций к релейно-контактным схемам

Булевы функции широко применяются при описании работы дискретных управляющих систем (контактных схем, схем из функциональных элементов, логических сетей и т.д.), при исследовании некоторых электрических цепей, так называемых релейно-контактных схем.

Идея применения. Под *релейно-контактной схемой* понимается устройство из проводников и двухпозиционных контактов. Оно

может быть предназначено, например, для соединения (или разъединения) полюсов источника тока с некоторым потребителем. Контакты релейно-контактной схемы могут быть двух типов: *замыкающие* и *размыкающие*. Каждый контакт подключен к некоторому реле (переключателю). К одному реле может быть подключено несколько контактов — как замыкающих, так и размыкающих. Технически реле представляет собой катушку с металлическим сердечником (магнитопроводом), вблизи которого находится соотвествующий контакт.

Когда через катушку пропускается электрический ток, металлический сердечник намагничивается и замыкает все находящиеся при нем замыкающие контакты. Одновременно все размыкающие контакты, относящиеся к данному реле, размыкаются. Поскольку замыкающие контакты при отсутствии в реле электрического тока разомкнуты, то они называются также *нормально разомкнутыми*. Аналогично, размыкающие контакты называются также *нормально замкнутыми*. При обесточивании обмоток реле (т.е. когда реле отключается) все замыкающие контакты снова размыкаются, а все размыкающие, замыкаются.

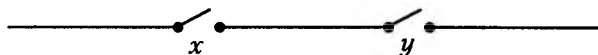
Каждому реле ставится в соответствие своя булева переменная x_1 , или x_2 , ..., или x_n , которая принимает значение 1, когда реле срабатывает, и принимает значение 0 при отключении реле. На чертеже все замыкающие контакты, подключенные к реле x , обозначаются тем же символом x , а все размыкающие контакты, подключенные к этому реле, обозначаются отрицанием x' . Это означает, что при срабатывании реле x все его замыкающие контакты x проводят ток и им сопоставляется значение 1, а все размыкающие контакты x' не проводят электрический ток и им сопоставляется значение 0. При отключенном реле x создается противоположная ситуация: все его замыкающие контакты x разомкнуты, т.е. в этот момент им сопоставляется (переменная x принимает) значение 0, а все его размыкающие контакты x' замкнуты, т.е. в этот момент им сопоставляется (другими словами, переменная x' принимает) значение 1.

Всей релейно-контактной схеме тогда ставится в соответствие булева переменная y , зависящая от булевых переменных $x_1, x_2, \dots, x_n$, сопоставленным тем реле, которые участвуют в схеме. Если при данном наборе состояний реле $x_1, x_2, \dots, x_n$ (некоторые из этих реле находятся в рабочем состоянии под током, остальные отключены, т.е. «обесточены») вся релейно-контактная схема проводит электрический ток, то переменной y ставится в соответствие (другими словами, переменная y принимает) значение 1. Если же при этом наборе состояний реле $x_1, x_2, \dots, x_n$ схема не проводит электрический ток, то считаем, что переменная y принимает значение 0. Поскольку каждый набор состояний реле $x_1, x_2, \dots, x_n$ характеризуется набором, составленным из нулей и еди-

нии и имеющим длину n , то данная релейно-контактная схема определяет некоторое правило, по которому каждому такому набору длины n , составленному из нулей и единиц, сопоставляется либо 0, либо 1. Таким образом, каждая релейно-контактная схема, в которой занято n независимых реле (контактов в ней может быть n или больше), определяет некоторую булеву функцию y от n аргументов. Она принимает значение 1 на тех и только тех наборах значений аргументов $x_1, x_2, \dots, x_n$, которые соответствуют тем состояниям реле $x_1, x_2, \dots, x_n$, при которых данная схема проводит электрический ток. Такая булева функция $y = f(x_1, x_2, \dots, x_n)$ называется *функцией проводимости* данной релейно-контактной схемы.

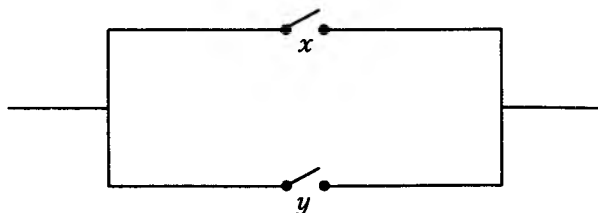
Таким образом, теория булевых функций предоставляет математические модели реальных физических релейно-контактных схем.

Рассмотрим некоторые релейно-контактные схемы и найдем их функции проводимости. Первая схема состоит из двух последовательно соединенных контактов x и y , т.е. контактов, связанных с двумя независимыми реле x и y , каждое из которых срабатывает независимо от другого:



Ясно, что данная схема проводит электрический ток тогда и только тогда, когда оба контакта x и y замкнуты, т.е. только тогда, когда оба переменных x и y принимают значение 1. Булева функция от двух аргументов x, y , удовлетворяющая такому условию, нам хорошо известна. Это конъюнкция $x \cdot y$. Таким образом, функцией проводимости релейно-контактной схемы, состоящей из двух последовательно соединенных контактов x и y , является конъюнкция $x \cdot y$. Говорят, что *последовательное соединение двух контактов* реализует конъюнкцию соответствующих этим контактам булевых переменных.

Вторая релейно-контактная схема состоит из двух параллельно соединенных контактов x и y :

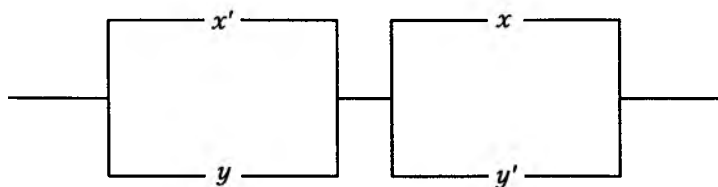


Ясно, что эта схема проводит электрический ток в том и только в том случае, когда по меньшей мере один из контактов (x или y) замкнут, т.е. лишь в случае, когда хотя бы одна из булевых переменных (x или y) принимает значение 1. Булева функция от двух

аргументов x и y , удовлетворяющая этому условию, также хорошо нам известна. Это, дизъюнкция $x \vee y$. Таким образом, функцией проводимости релейно-контактной схемы, состоящей из двух параллельно соединенных контактов x и y , является дизъюнкция $x \vee y$. Говорят, что *параллельное соединение двух контактов* реализует дизъюнкцию соответствующих этим контактам булевых переменных.

Итак, с помощью релейно-контактных схем можно реализовывать булевы функции: конъюнкцию, дизъюнкцию и отрицание. Возможна ли аналогичная реализация и других булевых функций? Ответ на поставленный вопрос позволяет дать теорема 10.5. Поскольку всякая булева функция на основании этой теоремы может быть выражена через конъюнкцию, дизъюнкцию и отрицание, причем отрицание стоит лишь непосредственно около переменных и не стоит ни около каких внутренних скобок, а конъюнкция, дизъюнкция и отрицание, как показано только что, реализуются на релейно-контактных схемах, то и *всякая булева функция может быть реализована с помощью релейно-контактной схемы*, т. е. может быть построена такая схема, для которой данная булева функция служит функцией проводимости.

Реализуем, например, в виде релейно-контактных схем булевы функции — импликацию и эквивалентность. Для этого выразим их через конъюнкцию, дизъюнкцию и отрицание. Такие выражения известны (см. теорему 9.5): $x \rightarrow y = x' \vee y$, $x \leftrightarrow y = (x \rightarrow y) \cdot (y \rightarrow x) = (x' \vee y) \cdot (y' \vee x)$. Предлагается самостоятельно нарисовать схему, реализующую функцию $x \rightarrow y$. Релейно-контактная схема, реализующая функцию $x \leftrightarrow y$, будет состоять из двух последовательно соединенных ветвей, первая из которых реализует булеву функцию $x' \vee y$, а вторая — булеву функцию $y' \vee x$. В свою очередь, первая из ветвей будет состоять из двух параллельных участков, один из которых содержит контакт x' , а второй — контакт y . Аналогично, вторая ветвь также будет состоять из двух параллельных участков, один из которых содержит контакт x , а другой — контакт y' . Изображаем полученную релейно-контактную схему (чтобы упростить рисунки, не будем изображать сами контакты, а ограничимся символом булевой переменной, соответствующей данному контакту):



Ознакомьтесь с примерами № 7.2, л, 7.3, л, разобранными в Задачнике.

Две основные задачи теории релейно-контактных схем. Составление релейно-контактных схем с заданными условиями работы называется *задачей синтеза* релейно-контактных схем и является первой важной задачей, состоящей в том, что требуется построить схему, которая проводила бы электрический ток лишь при вполне определенных задаваемых условиях. Проанализируйте приведенные в Задачнике решения задач № 7.9 и 7.20.

Естественно было бы выбирать для каждой булевой функции самую простую или одну из самых простых реализующих ее релейно-контактных схем. Поэтому упрощение релейно-контактных схем называется *задачей анализа* таких схем и является второй важной задачей теории релейно-контактных схем. Две релейно-контактные схемы, составленные из одних и тех же реле, называются *равносильными*, если одна из них проводит ток тогда и только тогда, когда другая схема проводит ток. Другими словами, две схемы, составленные из одних и тех же реле, равносильны, если они обладают одинаковыми функциями проводимости, зависящими от одних и тех же переменных. Из двух равносильных схем более простой считается та, которая содержит меньшее число контактов. Задача упрощения релейно-контактной схемы состоит в нахождении более простой равносильной ей схемы. Обычно она решается следующим образом. Для данной релейно-контактной схемы записывается ее функция проводимости. Затем эта функция с помощью тождественных преобразований, использующих известные свойства булевых функций, упрощается, т.е. сводится к функции, имеющей меньшее число вхождений переменных, нежели исходная функция. Наконец строится релейно-контактная схема, отвечающая упрощенной булевой функции. Рассмотрите решенные в Задачнике примеры № 7.5, л и 7.9.

§ 13. Релейно-контактные схемы в ЭВМ

Первая электронно-вычислительная машина была создана в 1946 г. в США. Для записи и обработки в ЭВМ числовой и символьной информации удобным с технической точки зрения оказался язык двоичных чисел — нулей и единиц. Поэтому естественно было ожидать, что методы математической науки, исследовавшей двужначные функции, рано или поздно найдут применение в процессе создания такой техники. Впервые предположение о возможности применения алгебры логики в технике было высказано в 1910 г. известным физиком П. Эренфестом (1880 — 1933). Булевы функции стали математическим аппаратом для исследования релейно-контактных схем (эта связь окончательно была осознана в 1930-х гг.), а сами схемы к середине XX в. нашли многочисленные применения в автоматической технике — в телефонии, железно-

дорожной сигнализации, централизации и блокировке, релейной защите, телемеханике и, наконец, — при проектировании быстродействующих ЭВМ. О некоторых простых, но очень важных релейно-контактных схемах, используемых в ЭВМ, и пойдет речь в настоящем параграфе.

Двоичный полусумматор. Числа в ЭВМ хранятся в двоичной системе в ячейках памяти поразрядно. С технической точки зрения в двоичной системе оказалось удобно не только хранить числа, но и выполнять над ними различные действия. Так, сложение двоичных чисел осуществляется на основе следующих правил: $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, $1 + 1 = 10$. Сложение по этим правилам делается по каждому разряду двух ячеек, в которых хранятся слагаемые. Если же происходит переполнение данного разряда (что возможно только при сложении $1 + 1$), то происходит перенос единицы в следующий разряд. Таким образом, процесс сложения в одном разряде может быть охарактеризован двумя булевыми функциями: $S(x, y)$ и $P(x, y)$, зависящими от складываемых чисел x и y . Первая функция $S(x, y)$ представляет собой значение суммы, записываемое в тот же разряд соответствующей ячейки, в котором происходит сложение. Вторая функция — функция переноса $P(x, y)$ — дает значение числа, переносимого в следующий, более старший разряд при переполнении разряда, в котором происходит сложение. Таблица истинности этих функций следующая:

x	y	$S(x, y)$	$P(x, y)$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Используя СДН-формы, выписываем для них выражения, по которым легко построить соответствующие релейно-контактные схемы: $S(x, y) = x'y \vee xy'$, $P(x, y) = xy$.

Одноразрядный двоичный сумматор. При сложении двух чисел описанные в предыдущем пункте действия совершаются лишь в первом (самом младшем) разряде ячеек, хранящих слагаемые. Во всех же остальных разрядах, начиная со второго, в процессе сложения участвуют уже не два слагаемых x_k и y_k , но еще и число, переносимое из предыдущего разряда и равное значению функции переноса $P_{k-1}(x_{k-1}, y_{k-1})$ в этом разряде. Таким образом, функция сумма S_k в k -м разряде ($k \geq 2$) зависит от трех аргументов, т.е. $S_k = S_k(x_k, y_k, P_{k-1})$. От этих же аргументов зависит и функция переноса из k -го разряда $P_k(x_k, y_k, P_{k-1})$. Составим таблицу значений этих функций:

x_k	y_k	P_{k-1}	$S_k(x_k, y_k, P_{k-1})$	$P_k(x_k, y_k, P_{k-1})$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Используя СДН-формы, найдем для них выражения, которые затем упростим, преобразуя тождественным образом:

$$S(x, y, p) = \bigvee x^\alpha y^\beta p^\gamma = x^0 y^0 p^1 \vee x^0 y^1 p^0 \vee x^1 y^0 p^0 \vee x^1 y^1 p^1 =$$

$$S(\alpha, \beta, \gamma) = 1$$

$$= x'y'p \vee x'yp' \vee xy'p' \vee xyp = (x'y' \vee xy)p' \vee (x'y \vee xy')p';$$

$$P(x, y, p) = \bigvee x^\alpha y^\beta p^\gamma = x^0 y^1 p^1 \vee x^1 y^0 p^1 \vee x^1 y^1 p^0 \vee x^1 y^1 p^1 =$$

$$P(\alpha, \beta, \gamma) = 1$$

$$= x'yp \vee xy'p \vee xyp' \vee xyp = (x'yp \vee xyp) \vee (xy'p \vee xyp) \vee (xyp' \vee xyp) =$$

$$= (x' \vee x)yp \vee (y' \vee y)xp \vee (p' \vee p)xy = xp \vee yp \vee xy.$$

Соответствующие схемы предлагается нарисовать самостоятельно. Построив такие схемы для каждого разряда и обеспечив их надлежащее соединение, можно получить схему многоразрядного двоичного сумматора, осуществляющего сложение двоичных чисел в ЭВМ.

Шифратор и дешифратор. Человек привык оперировать с числами в десятичной системе счисления. Для ЭВМ более удобна двоичная система. Поэтому важную роль в ЭВМ играют устройства, обеспечивающие взаимопонимание человека и машины, т. е. устройства, переводящие информацию с языка человека на язык машины и обратно. Такими устройствами являются, например, шифраторы, осуществляющие перевод чисел из десятичной системы в двоичную, и дешифраторы, осуществляющие обратный перевод. Покажем, как конструируется шифратор. Имеется следующее соответствие между десятичной и двоичной записями:

Десятичная запись	Двоичная запись	Десятичная запись	Двоичная запись
0	0000	5	0101
1	0001	6	0110
2	0010	7	0111
3	0011	8	1000
4	0100	9	1001

Каждую колонку из нулей и единиц в правом столбце таблицы можно мыслить себе как колонку значений одной из булевых функций: f_1, f_2, f_4, f_8 . Нужно лишь отчетливо усмотреть булеву (т.е. двузначную) природу ее аргументов.

В самом деле, можем считать, что каждая из этих функций зависит от десяти аргументов $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$. Причем зависимость следующая (она обусловлена предыдущей таблицей соответствий):

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	f_8	f_4	f_2	f_1
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	1
0	0	1	0	0	0	0	0	0	0	0	0	1	0
0	0	0	1	0	0	0	0	0	0	0	0	1	1
0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	0	0	1	0	1
0	0	0	0	0	0	1	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	1	0	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	0	0	1

Каждая из функций f_1, f_2, f_4 и f_8 зависит от десяти аргументов. Поэтому таблица их значений должна содержать (что установлено при доказательстве теоремы 10.3) 2^{10} строк. Отсутствие остальных строк в приведенной таблице означает, что на указанных десяти наборах значений аргументов $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$ функции должны принимать указанные значения, а на остальных наборах их значения могут быть какими угодно. Это, в свою очередь, означает, что в качестве каждой из функций f_1, f_2, f_4, f_8 можно взять довольно много (но все же конечное число) функций.

Используя СДН-форму, найдем, например, выражение для f_8 (считая, что на всех не указанных наборах значений ее аргументов она принимает значение 0):

$$f_8(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9) = x_0'x_1'x_2'x_3'x_4'x_5'x_6'x_7'x_8'x_9' \vee x_0'x_1'x_2'x_3'x_4'x_5'x_6'x_7'x_8'x_9 = x_0'x_1'x_2'x_3'x_4'x_5'x_6'x_7'(x_8'x_9' \vee x_8'x_9).$$

Для остальных функций f_1, f_2 и f_4 найти соответствующие выражения предлагается самостоятельно.

По учебному пособию [9.12] можно достаточно подробно познакомиться с современным применением булевых функций при конструировании ЭВМ.

§ 14. О некоторых других приложениях теории булевых функций

Важнейшее применение теории булевых функций (в теории релейно-контактных схем) рассмотрено в § 12, 13. Здесь кратко охарактеризуем еще одну сферу применения теории булевых функций, выявленную уже во второй половине XX в. Это так называемая *теория распознавания образов*. На ее примере можно увидеть, как математика пытается своими методами смоделировать еще один вид мыслительной деятельности, свойственный человеческому мозгу, и что при этом снова оказываются задействованы методы математической логики.

Диагностика (распознавание) заболеваний. Начнем с анализа одной конкретной ситуации. Как известно, различные заболевания сопровождаются теми или иными симптомами. Эта связь устанавливается экспериментально на основе многолетних медицинских обследований тысяч больных. С помощью математики эти связи можно определенным образом систематизировать, используя аппарат булевых функций. Предположим, что имеется m симптомов $S_1, S_2, \dots, S_m$ и n заболеваний $T_1, T_2, \dots, T_n$. Рассмотрим следующие булевы переменные ($i = 1, \dots, m; j = 1, \dots, n$):

$$x_i = \begin{cases} 1, & \text{если у больного обнаружен } i\text{-й симптом,} \\ 0, & \text{в противном случае;} \end{cases}$$

$$y_i = \begin{cases} 1, & \text{если у больного обнаружен } j\text{-е заболевание,} \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда связь между симптомами заболеваний и заболеваниями может быть выражена на языке алгебры логики. Например, если заболевание T_1 всегда сопровождается симптомами S_2 и S_3 , то булева функция $y_1 \rightarrow (x_2 \cdot x_3)$ тождественно равна 1. Аналогично, может быть известно, что если обнаружены симптомы S_1, S_4, S_5 , то обязательно должно быть заболевание T_2 , и, наоборот, это заболевание всегда проявляется в указанных симптомах. Следовательно, тождественно равна 1 булева функция следующего вида: $x_1 \cdot x_2 \cdot x_3 \leftrightarrow y_2$. Часто один какой-нибудь симптом (например, высокая температура) сопровождает многие заболевания, булева функция в этом случае $x_1 \rightarrow (y_1 \vee y_2 \vee y_3 \vee y_4 \vee y_5) = 1$.

Таким образом, экспериментально устанавливаются следующие булевы равенства:

$$\begin{aligned} f_1(x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n) &= 1; \\ f_2(x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n) &= 1; \\ &\dots\dots\dots \\ f_k(x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n) &= 1. \end{aligned}$$

Булевы функции $f_1, f_2, \dots, f_k$ называются *указаниями*. Каждая из них есть, по существу, некоторое составное высказывание относительно причинно-следственной связи между симптомами заболеваний и самими заболеваниями. Из этих равенств следует, что равна 1 и конъюнкция булевых функций $f_1, f_2, \dots, f_k$: $f(x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n) = f_1 f_2 \dots f_k = 1$.

Это равенство представляет собой своего рода неявное задание функций (заболеваний) $y_1, y_2, \dots, y_n$ от аргументов (симптомов) $x_1, x_2, \dots, x_m$. Задача диагностики состоит в том, чтобы явно выявить эти зависимости и применить их к конкретному больному. Для этого можно составить таблицу значений функции f . Из общего числа строк 2^{m+n} нас будут интересовать в ней лишь те, в которых для всех симптомов, выявленных у исследуемого больного, соответствующее значение x равно 1. Пусть у больного выявлены симптомы S_1, S_2, S_3 , а общее число симптомов, задействованных в нашем анализе, пять: S_1, S_2, S_3, S_4, S_5 . Тогда число строк, представляющих интерес в данном случае, равно четырем. Предположим, что эти строки таковы (для простоты примем, что исследуются три заболевания: T_1, T_2, T_3 и им соответствуют три переменные: y_1, y_2, y_3):

x_1	x_2	x_3	y_1	y_2	y_3	f
1	1	1	0	0	1	1
1	1	1	0	1	1	1
1	1	1	0	1	1	1
1	1	1	0	0	1	1

Анализ выделенных строк показывает, что во всех строках, соответствующих симптомам больного, есть заболевание y_3 (точнее, T_3) и нет заболевания y_1 (точнее, T_1), а заболевание y_2 (т.е. T_2) в одних строках есть, а в других нет. Из этого можно сделать вывод, что у больного нет заболевания T_1 , но он определенно страдает заболеванием T_3 . Относительно заболевания T_2 требуются дополнительные исследования. Для этого нужно увеличить число анализируемых симптомов, выявить дополнительные указания f_i . На практике число столбцов и строк построенной таблицы может оказаться столь большим, что ее анализ будет под силу лишь компьютеру.

Распознавание образов. Нетрудно видеть, что в самых общих чертах ситуация, рассмотренная в предыдущем пункте, может быть охарактеризована следующим образом. Имеется некоторое множество скрытых причин (болезней) и множество наблюдаемых следствий (симптомов). Кроме того, имеются высказывания, связывающие причины и следствия. Требуется, опираясь на эти высказывания, по предъявляемому набору следствий (симптомов,

наблюдаемых у данного пациента) определить возможные причины, их породившие (болезни пациента). Во второй половине XX в. сформировалась область прикладной математики, занимающаяся решением подобных проблем. Она получила название *теория распознавания образов*. В предыдущем пункте показано, как распознавать «образ болезни», но подобная ситуация встречается весьма часто и в других областях науки. В геологии, например, причины труднодоступны, так как это — залегающие на разных глубинах полезные ископаемые. Но следствия сравнительно легко наблюдаемы: это — сопутствующие минералы, выходящие на поверхность, окраска почвы, характер растительности, данные сейсморазведки, аэро- и космической фотосъемки и т.п. В химии скрытые причины — это качественный состав и строение вещества, а наблюдаемые следствия — ответы в тестовых реакциях: помутнение, окраска, запах, выделение теплоты и т.п. В биологии: малодоступные гены контролируют легко наблюдаемые признаки. В криминалистике: скрывшийся преступник оставляет следы, улики, показания свидетелей.

В разных науках такое «распознавание образов» называется по-разному; для рассмотренных это — диагностика, геологическая разведка, анализ, раскрытие преступления и т.д. С точки зрения математики здесь решается одна задача, сформулированная как «распознавание образов». Решать ее в самой общей постановке и призвана математическая теория распознавания образов. Один из методов ее решения опирается на теорию булевых функций, которая позволяет в определенном смысле автоматизировать процесс решения, используя для этой цели ЭВМ.

Глава III

ФОРМАЛИЗОВАННОЕ ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

В этой главе рассматривается аксиоматический подход к алгебре высказываний, т.е. такой же подход, какой используется при строгом построении геометрии на базе какой-либо системы аксиом, например систем Гильберта, Вейля и т.д. Алгебра высказываний предстанет как аксиоматическая теория, в определенном смысле достигнет наивысшей степени строгости изложения и совершенства. Общим вопросам аксиоматических теорий посвящены гл. V и VI, так что формализованное исчисление высказываний, которое строится в настоящей главе, будет служить примером аксиоматической теории.

Применительно к алгебре высказываний аксиоматический подход состоит в следующем. Из всех формул алгебры высказываний выделяется некоторая часть. Формулы из этой части объявляются аксиомами. Определяется некоторое правило, по которому из одних формул можно получать новые. Аксиомы выделяются, а правило определяется так, что по нему из аксиом могут быть получены все тавтологии алгебры высказываний, и только они. Таким образом, тавтологии алгебры высказываний оказываются теоремами аксиоматической теории, в результате получаем аксиоматическое построение алгебры высказываний.

В качестве системы аксиом могут быть выбраны разные части совокупности всех формул алгебры высказываний. То же относится к правилам получения новых формул. В зависимости от выбора получаются различные аксиоматизации алгебры высказываний. Общим для них является то, что все они обладают одним и тем же множеством теорем — это совокупность всех тавтологий алгебры высказываний. Мы рассмотрим лишь одну из возможных аксиоматизаций.

§ 15. Система аксиом и теория формального вывода

В настоящем параграфе будет заложена основа аксиоматической теории высказываний, определены понятия доказательства и теоремы, рассмотрены примеры доказательств теорем и развита теория формального вывода.

Начало аксиоматической теории высказываний: первоначальные понятия, система аксиом, правило вывода. К первоначальным, неопределяемым понятиям аксиоматической теории высказываний относятся следующие: $X_1, X_2, \dots, X_n$ — пропозициональные переменные; $\neg, \rightarrow$ — логические связки; $(,)$ — технические знаки. Первоначальным понятием является также понятие *формулы*, которое определяется (как и в алгебре высказываний, см. определение 2.1) индуктивным образом:

- 1) каждая пропозициональная переменная есть формула;
- 2) если F_1 и F_2 — формулы, то выражения $\neg F_1, (F_1 \rightarrow F_2)$ также являются формулами;
- 3) никаких других формул, кроме получающихся согласно пунктам 1 и 2 нет.

Следующий шаг в построении аксиоматической теории высказываний состоит в выборе системы аксиом. В качестве аксиом выбираются формулы следующих видов:

- (A1): $(F \rightarrow (G \rightarrow F))$;
 (A2): $(F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$;
 (A3): $((\neg G \rightarrow \neg F) \rightarrow ((\neg G \rightarrow F) \rightarrow G))$,

где F, G, H — произвольные формулы. Таким образом, каждое из выражений (A1), (A2), (A3) задает лишь форму аксиомы. Они превращаются в аксиомы, если вместо F, G и H подставить конкретные формулы (в частности, пропозициональные переменные). Следовательно, каждое из этих выражений задает бесконечное множество формул. Все они называются аксиомами. Поэтому каждое из выражений (A1), (A2), (A3) называют *схемой аксиом*.

Наконец, заключительный шаг, закладывающий основу аксиоматической теории высказываний, состоит в выборе *правил вывода*. Единственным правилом вывода будет служить правило заключения (или отделения, или *modus ponens*, или сокращенно MP): из формул F и $F \rightarrow G$ непосредственно следует формула G .

Как и в алгебре высказываний, внешние скобки у формулы принято не писать.

Поскольку в аксиомах не участвуют связки $\wedge, \vee, \leftrightarrow$, то их придется определить. Введем следующие определения:

- $(F \wedge G)$ означает $\neg(F \rightarrow \neg G)$;
 $(F \vee G)$ означает $(\neg F \rightarrow G)$;
 $(F \leftrightarrow G)$ означает $((F \rightarrow G) \wedge (G \rightarrow F))$.

Смысл, например, первого из определений состоит в том, что, каковы бы ни были формулы F и G , формула $(F \wedge G)$ служит обозначением для формулы $\neg(F \rightarrow \neg G)$.

Понятие вывода и его свойства. Заложив основу будущей аксиоматической теории в виде системы аксиом и правила вывода,

приступим к ее развитию, т.е. к доказательству теорем. Прежде всего уточним понятия доказательства и теоремы.

Определение 15.1. Доказательством или выводом формулы F из множества формул Γ называется такая конечная последовательность $B_1, B_2, \dots, B_s$ формул, каждая формула которой является либо аксиомой, либо формулой из Γ , либо получена из двух предыдущих формул этой последовательности по правилу МР, а последняя формула B_s совпадает с F ($B_s \equiv F$). Если имеется вывод формулы F из множества Γ , то говорят, что F выводима из Γ или что Γ выводит F , и пишут $\Gamma \vdash F$. Элементы из Γ называются гипотезами или посылками вывода. Если же имеется вывод формулы F из пустого множества гипотез, то говорят, что F выводима из аксиом (или что F доказуема), а последовательность $B_1, B_2, \dots, B_s$ называется доказательством этой формулы. Саму F называют теоремой, и пишут $\vdash F$. Таким образом, запись $\vdash F$ служит сокращением утверждения « F есть теорема».

Если множество Γ конечно: $\Gamma = \{F_1, F_2, \dots, F_m\}$, то вместо $\{F_1, F_2, \dots, F_m\} \vdash G$ будем писать $F_1, F_2, \dots, F_m \vdash G$.

Совокупность аксиом, правил вывода и всех теорем, выводимых из аксиом, и представляет собой аксиоматическую теорию высказываний (или формализованное исчисление высказываний). Наша ближайшая цель состоит в том, чтобы научиться доказывать теоремы в данной теории, т.е. научиться строить выводы формул из аксиом.

Приведем пример доказательства какой-нибудь формулы.

Пример 15.2. Доказать: $\vdash F \rightarrow F$.

Для доказательства того, что формула $F \rightarrow F$ является теоремой формализованного исчисления высказываний, нужно построить вывод (доказательство) этой формулы из аксиом. Таким выводом является, например, следующая последовательность формул:

- (1): $(F \rightarrow ((F \rightarrow F) \rightarrow F)) \rightarrow ((F \rightarrow (F \rightarrow F)) \rightarrow (F \rightarrow F));$
- (2): $F \rightarrow ((F \rightarrow F) \rightarrow F);$
- (3): $(F \rightarrow (F \rightarrow F)) \rightarrow (F \rightarrow F);$
- (4): $F \rightarrow (F \rightarrow F);$
- (5): $F \rightarrow F.$

Формула (1) представляет собой аксиому (A2), в которой в качестве формул F и H взята формула F , а в качестве формулы G взята формула $F \rightarrow F$. Формула (2) представляет собой аксиому (A1), в которой в качестве формулы G берется формула $F \rightarrow F$. Формула (3) получена из формул (1) и (2) по правилу МР. Формула (4) есть аксиома (A1). Наконец, формула (5) получена из формул (3) и (4) по правилу МР.

Таким образом, $\vdash F \rightarrow F$.

В следующей теореме отмечается несколько простых, но важных свойств понятия выводимости из гипотез.

Теорема 15.3 (свойства выводимости).

а) Если $\Gamma \vdash F$ и $\Gamma \subseteq \Delta$, то $\Delta \vdash F$;

б) $\Gamma \vdash F$ тогда и только тогда, когда в Γ существует такое конечное подмножество Δ , что $\Delta \vdash F$;

в) Если $\Gamma \vdash G$ для любой формулы G из множества Δ и $\Delta \vdash F$, то $\Gamma \vdash F$.

Доказательство. а) Данное свойство выражает следующий очевидный факт: если формула F выводима из множества посылок Γ , то она будет выводима и из всякого множества, получающегося добавлением к Γ новых посылок.

б) Достаточность вытекает из свойства (а). Обратно, если $\Gamma \vdash F$, то, по определению 15.1, существует вывод F из Γ , т.е. некоторая конечная последовательность формул, использующая, следовательно, лишь конечное число посылок из Γ . Поэтому можно считать, что именно эта конечная часть формул из Γ и выводит формулу F .

в) По условию $\Delta \vdash F$. Тогда ввиду предыдущего свойства (б) в Δ существует такое конечное подмножество Δ_0 , что $\Delta_0 \vdash F$. Пусть $\Delta_0 = \{B_1, B_2, \dots, B_k\}$. По условию, кроме того, $\Gamma \vdash B_1, \Gamma \vdash B_2, \dots, \Gamma \vdash B_k$, т.е. имеются выводы каждой из формул $B_1, B_2, \dots, B_k$ из множества гипотез Γ , представляющие собой конечные последовательности формул. Выпишем эти последовательности одну за другой и добавим к ним последовательность, являющуюся выводом формулы F из множества гипотез $\Delta_0 = \{B_1, B_2, \dots, B_k\}$. Полученная таким образом последовательность будет представлять собой вывод формулы F из множества гипотез Γ , т.е. $\Gamma \vdash F$. $\square$

Теорема о дедукции и следствия из нее. Процесс построения доказательств для тех или иных формул может оказаться достаточно сложным как в идейном, так и в техническом плане. Теорема о дедукции, о которой пойдет речь, выявляет некоторую общую закономерность при таких построениях и тем самым облегчает процесс построения доказательства, что будет видно из последующих примеров.

Теорема 15.4 (о дедукции). Если $F_1, \dots, F_{m-1}, F_m \vdash G$, то $F_1, \dots, F_{m-1} \vdash F_m \rightarrow G$. В частности, если $F \vdash G$, то $\vdash F \rightarrow G$.

Доказательство. Пусть последовательность формул

$$B_1, B_2, \dots, B_i, \dots, B_s \quad (1)$$

является выводом формулы G из гипотез $F_1, \dots, F_{m-1}, F_m$ (такая последовательность существует, поскольку, по условию, $F_1, \dots, F_{m-1}, F_m \vdash G$). Следовательно, формула B_s есть формула G , т.е. $B_s \equiv G$ ($\equiv$ — знак графического совпадения, одинаковости формул). Рассмотрим последовательность формул:

$$F_m \rightarrow B_1, F_m \rightarrow B_2, \dots, F_m \rightarrow B_i, \dots, F_m \rightarrow B_s. \quad (2)$$

На последнем месте данной последовательности стоит формула $F_m \rightarrow G$ (так как $B_s \equiv G$). Но эта последовательность, вообще говоря, не является выводом из гипотез $F_1, \dots, F_{m-1}$. Тем не менее ее можно превратить в такой вывод, если перед каждой формулой последовательности добавить подходящие формулы. Для этого покажем методом математической индукции по l , что

$$F_1, \dots, F_{m-1} \vdash F_m \rightarrow B_l. \quad (3)$$

1) $l = 1$. Покажем, что $F_1, \dots, F_{m-1} \vdash F_m \rightarrow B_1$. Для формулы B_1 как первого члена последовательности (1), являющейся выводом G из $F_1, \dots, F_{m-1}, F_m$, могут представиться следующие возможности:

а) B_1 есть либо одна из аксиом, либо одна из гипотез $F_1, \dots, F_{m-1}$. В этом случае вывод формулы $F_m \rightarrow B_1$ из гипотез $F_1, \dots, F_{m-1}$ строится так:

$$B_1, B_1 \rightarrow (F_m \rightarrow B_1), F_m \rightarrow B_1, \quad (4)$$

где вторая формула есть аксиома (A1), а третья получена из первых двух по правилу МР. Таким образом, в последовательность (2) перед первой формулой нужно добавить первую и вторую формулы из последовательности (4);

б) B_1 есть гипотеза F_m . Тогда формула $F_m \rightarrow B_1$ принимает вид $F_m \rightarrow F_m$. Но согласно примеру 15.2, эта формула выводима не только из гипотез $F_1, \dots, F_{m-1}$, но и просто из аксиом. В этом случае ее вывод, приведенный в примере 15.2, нужно вписать в последовательность (2) перед первой формулой;

2) $l \leq k$. Предположим, что утверждение (3) верно для всех $l \leq k$ и все необходимые выводы добавлены перед всеми k первыми формулами последовательности (2);

3) $l = k + 1$. Покажем теперь, что утверждение (3) верно для $l = k + 1$, т.е. справедлива выводимость: $F_1, \dots, F_{m-1} \vdash F_m \rightarrow B_{k+1}$. Для формулы B_{k+1} как члена последовательности (1), являющейся выводом G из гипотез $F_1, \dots, F_{m-1}, F_m$, могут представиться следующие возможности:

а), б) B_{k+1} есть либо одна из аксиом, либо одна из гипотез $F_1, \dots, F_{m-1}, F_m$. Данные возможности абсолютно аналогичны соответствующим возможностям из случая $l = 1$ (там лишь нужно B_1 заменить на B_{k+1});

в) B_{k+1} получена из двух предыдущих формул B_i, B_j последовательности (1) по правилу МР. Следовательно, $1 \leq i < k + 1$, $1 \leq j < k + 1$, а формула B_j имеет вид: $B_i \rightarrow B_{k+1}$, т.е. $B_j \equiv B_i \rightarrow B_{k+1}$. Поскольку $1 \leq i < k + 1$ и $1 \leq j < k + 1$, то формулы $F_m \rightarrow B_i$ и $F_m \rightarrow B_j$ стоят в последовательности (2) перед формулой $F_m \rightarrow B_{k+1}$, а следовательно, по предположению индукции, справедливы утверждения о том, что имеются выводы этих формул из гипотез $F_1, \dots$,

F_{m-1} . Выпишем эти выводы последовательно один за другим, они завершаются формулами $F_m \rightarrow B_i$ и $F_m \rightarrow (B_i \rightarrow B_{k+1})$ соответственно (напоминаем, что $B_j \equiv B_i \rightarrow B_{k+1}$):

.....
 $(\alpha) \quad F_m \rightarrow B_i$

.....
 $(\alpha + \beta) \quad F_m \rightarrow (B_i \rightarrow B_{k+1}).$

Продолжим выводы следующими формулами:

$(\alpha + \beta + 1) \quad (F_m \rightarrow (B_i \rightarrow B_{k+1})) \rightarrow ((F_m \rightarrow B_i) \rightarrow (F_m \rightarrow B_{k+1}));$

$(\alpha + \beta + 2) \quad (F_m \rightarrow B_i) \rightarrow (F_m \rightarrow B_{k+1});$

$(\alpha + \beta + 3) \quad F_m \rightarrow B_{k+1}.$

Первая из формул есть аксиома (A2), вторая формула получена из первой и формулы $(\alpha + \beta)$ по правилу МР, третья получена из второй и формулы (α) по правилу МР. Таким образом, построенная последовательность есть в этом случае вывод формулы $F_m \rightarrow B_{k+1}$ из гипотез $F_1, \dots, F_{m-1}$.

Итак, утверждение (3) верно для любого $l = 1, 2, \dots, s$. При $l = s$ получаем (напоминаем, что $B_s \equiv G$): $F_1, \dots, F_{m-1} \vdash F_m \rightarrow G$, что и требовалось доказать. $\square$

В задаче № 8.11 Задачника рассматривается процесс пополнения последовательности (2) до вывода (т.е. процесс восстановления вывода формулы $F_m \rightarrow G$ из формул $F_1, \dots, F_{m-1}$), исходя из данного вывода формулы G из формул $F_1, \dots, F_{m-1}, F_m$ применительно к конкретным формулам $F_1, \dots, F_{m-1}, F_m, G$.

Следствие 15.5. $F_1, \dots, F_{m-1}, F_m \vdash G$ тогда и только тогда, когда $F_1, \dots, F_{m-1} \vdash F_m \rightarrow G$.

Доказательство. Необходимость представляет собой теорему о дедукции. Обратно, если $F_1, \dots, F_{m-1} \vdash F_m \rightarrow G$, то существует соответствующий вывод: $B_1, \dots, B_{s-1}, F_m \rightarrow G$. Дополним его двумя формулами F_m и G . Получим последовательность $B_1, \dots, B_{s-1}, F_m \rightarrow G, F_m, G$, представляющую собой вывод формулы G из гипотез $F_1, \dots, F_{m-1}, F_m$, потому что предпоследняя формула этой последовательности есть одна из гипотез, а последняя получена из двух предшествующих ей формул по правилу МР. Следовательно, $F_1, \dots, F_{m-1}, F_m \vdash G$. $\square$

Следствие 15.6. $F_1, \dots, F_{m-1}, F_m \vdash G$ тогда и только тогда, когда $\vdash F_1 \rightarrow (F_2 \rightarrow \dots \rightarrow (F_{m-1} \rightarrow (F_m \rightarrow G)))$.

Доказательство. Данное следствие получается в результате m -кратного применения предыдущего следствия. $\square$

Применение теоремы о дедукции. С помощью теоремы о дедукции сначала будет доказана одна лемма, которая затем вместе с теоремой о дедукции будет использована для доказательства того, что ряд формул являются теоремами формализованного исчисления высказываний.

Лемма 15.7. Для любых формул F, G, H справедливы следующие выводимости:

- а) $F \rightarrow G, G \rightarrow H \vdash F \rightarrow H$;
- б) $F \rightarrow (G \rightarrow H), G \vdash F \rightarrow H$.

Доказательство. а) Покажем сначала, что $F \rightarrow G, G \rightarrow H, F \vdash H$. Для этого построим последовательность, являющуюся соответствующим выводом: $F \rightarrow G, G \rightarrow H, F, G, H$. Поясним. Первые три формулы последовательности суть гипотезы. Четвертая формула G получена из первой и третьей формул последовательности по правилу МР, а пятая — из второй и четвертой по тому же правилу. Итак, $F \rightarrow G, G \rightarrow H, F \vdash H$. Отсюда на основании теоремы о дедукции заключаем, что $F \rightarrow G, G \rightarrow H \vdash F \rightarrow H$.

б) Нетрудно видеть, что $F \rightarrow (G \rightarrow H), G, F \vdash H$, откуда требуемая выводимость следует на основании теоремы о дедукции. $\square$

Теорема 15.8. Для любых формул F, G следующие формулы являются теоремами формализованного исчисления высказываний:

- а) $\neg\neg F \rightarrow F$;
- б) $F \rightarrow \neg\neg F$;
- в) $\neg F \rightarrow (F \rightarrow G)$;
- г) $(\neg G \rightarrow \neg F) \rightarrow (F \rightarrow G)$;
- д) $(F \rightarrow G) \rightarrow (\neg G \rightarrow \neg F)$;
- е) $F \rightarrow (\neg G \rightarrow \neg(F \rightarrow G))$;
- ж) $(F \rightarrow G) \rightarrow ((\neg F \rightarrow G) \rightarrow G)$.

Доказательство. а) Обоснуем возможность доказательства (построения вывода из аксиом) этой формулы. Рассмотрим следующую последовательность формул:

- (1): $(\neg F \rightarrow \neg\neg F) \rightarrow ((\neg F \rightarrow \neg F) \rightarrow F)$ [аксиома (A3)];
- (2): $\neg F \rightarrow \neg F$ [пример 15.2];
- (3): $(\neg F \rightarrow \neg\neg F) \rightarrow F$ [(1), (2), лемма 15.7, б];
- (4): $\neg\neg F \rightarrow (\neg F \rightarrow \neg\neg F)$ [аксиома (A1)];
- (5): $\neg\neg F \rightarrow F$ [(4), (3), лемма 15.7, а].

Обратим внимание на то, что сама последовательность (1) — (5) не является выводом формулы $\neg\neg F \rightarrow F$ из аксиом. Чтобы превратить ее в вывод, нужно перед формулами (2) и (5) вписать их выводы из аксиом. Для формулы (2) это сделать нетрудно. Обоснование формулы (5) опирается на утверждение леммы 15.7 а, которое, в свою очередь, обосновано с помощью теоремы о дедукции. Поэтому, чтобы это утверждение можно было использовать в формальном выводе, его необходимо превратить в некоторую формулу, вывод которой, в свою очередь, должен быть построен на основании теоремы о дедукции. Продумайте самостоятельно эти взаимосвязи.

б) Строим последовательность формул, которая также выводом не является, а служит лишь обоснованием возможности по-

строения такого вывода, но которую можно дополнить до вывода без принципиальных трудностей:

- (1): $(\neg\neg\neg F \rightarrow \neg F) \rightarrow ((\neg\neg\neg F \rightarrow F) \rightarrow \neg\neg F)$ [аксиома (A3)];
- (2): $\neg\neg\neg F \rightarrow \neg F$ [теорема 15.8, а];
- (3): $(\neg\neg\neg F \rightarrow F) \rightarrow \neg\neg F$ [правило МР: (1), (2)];
- (4): $F \rightarrow (\neg\neg\neg F \rightarrow F)$ [аксиома (A1)];
- (5): $F \rightarrow \neg\neg F$ [лемма 15.7, а: (4), (3)].

в) В двух предыдущих доказательствах теорема о дедукции применялась опосредованно через лемму 15.7. В настоящей задаче происходит прямое применение этой теоремы. Это делается следующим образом. Покажем сначала, что $\neg F, F \vdash G$. Приводим соответствующий вывод, обосновать который предлагается самостоятельно (это уже действительно вывод, но пока еще вывод из гипотез — вывод формулы G из гипотез $\neg F, F$):

- (1): $\neg F$;
- (2): F ;
- (3): $F \rightarrow (\neg G \rightarrow F)$;
- (4): $\neg F \rightarrow (\neg G \rightarrow \neg F)$;
- (5): $\neg G \rightarrow F$;
- (6): $\neg G \rightarrow \neg F$;
- (7): $(\neg G \rightarrow \neg F) \rightarrow ((\neg G \rightarrow F) \rightarrow G)$;
- (8): $(\neg G \rightarrow F) \rightarrow G$;
- (9): G .

Итак, $\neg F, F \vdash G$. Тогда по теореме о дедукции $\neg F \vdash F \rightarrow G$. Применяя еще раз теорему о дедукции, получаем $\vdash \neg F \rightarrow (F \rightarrow G)$.

г) Покажем, что $\neg G \rightarrow \neg F, F \vdash G$. Для этого строим соответствующий вывод (обоснуйте его самостоятельно):

- (1): $\neg G \rightarrow \neg F$;
- (2): F ;
- (3): $(\neg G \rightarrow \neg F) \rightarrow ((\neg G \rightarrow F) \rightarrow G)$;
- (4): $(\neg G \rightarrow F) \rightarrow G$;
- (5): $F \rightarrow (\neg G \rightarrow F)$;
- (6): $\neg G \rightarrow F$;
- (7): G .

Итак, $\neg G \rightarrow \neg F, F \vdash G$. Применив теперь дважды теорему о дедукции, получаем требуемый результат.

д) Покажем сначала, что $F \rightarrow G \vdash \neg G \rightarrow \neg F$. Строим последовательность формул, которая выводом не является (снова обращаясь к лемме 15.7 и еще к доказанным выше теоремам), но может быть дополнена до такового:

- (1): $F \rightarrow G$ [использована гипотеза];
- (2): $\neg\neg F \rightarrow F$ [теорема 15.8, а];
- (3): $\neg\neg F \rightarrow G$ [лемма 15.7, а: (2), (1)];

- (4): $G \rightarrow \neg\neg G$ [теорема 15.8, б];
 (5): $\neg\neg F \rightarrow \neg\neg G$ [лемма 15.7, а: (3), (4)];
 (6): $(\neg\neg G \rightarrow \neg\neg F) \rightarrow (\neg F \rightarrow \neg G)$ [теорема 15.8, з];
 (7): $\neg F \rightarrow \neg G$ [правило МР: (5), (6)].

Применив теорему о дедукции, получаем требуемое утверждение.

е) По правилу МР имеем $F, F \rightarrow G \vdash G$. Тогда по теореме о дедукции: $F \vdash (F \rightarrow G) \rightarrow G$. Применяем еще раз теорему о дедукции: $\vdash F \rightarrow ((F \rightarrow G) \rightarrow G)$. Далее, по пункту д) настоящей теоремы имеем (взяв в качестве F формулу $F \rightarrow G$, а в качестве G — саму G): $((F \rightarrow G) \rightarrow G) \rightarrow (\neg G \rightarrow \neg(F \rightarrow G))$. Из этих двух последних утверждений на основании леммы 15.7, а получаем $\vdash F \rightarrow (\neg G \rightarrow \neg(F \rightarrow G))$.

ж) Покажем сначала, что $F \rightarrow G, \neg F \rightarrow G \vdash G$. В самом деле, строим соответствующую последовательность (определите самостоятельно, что это — вывод из гипотез или обоснование возможности его построения):

- (1): $F \rightarrow G$;
 (2): $\neg F \rightarrow G$;
 (3): $(F \rightarrow G) \rightarrow (\neg G \rightarrow \neg F)$;
 (4): $\neg G \rightarrow \neg F$;
 (5): $(\neg F \rightarrow G) \rightarrow (\neg G \rightarrow \neg\neg F)$;
 (6): $\neg G \rightarrow \neg\neg F$;
 (7): $(\neg G \rightarrow \neg\neg F) \rightarrow ((\neg G \rightarrow \neg F) \rightarrow G)$;
 (8): $(\neg G \rightarrow \neg F) \rightarrow G$;
 (9): G .

Итак, $F \rightarrow G, \neg F \rightarrow G \vdash G$. Следовательно, по теореме о дедукции $F \rightarrow G \vdash (\neg F \rightarrow G) \rightarrow G$. Еще раз применяя теорему о дедукции, получаем: $(F \rightarrow G) \rightarrow ((\neg F \rightarrow G) \rightarrow G)$.

Производные правила вывода. Аксиоматическая теория высказываний развита довольно глубоко: теорема о дедукции, вскрыв важное свойство выводимости, оказалась мощным средством, облегчающим доказательства того, что та или иная формула является теоремой формализованного исчисления высказываний. Следующим шагом на этом пути служит выявление дальнейших закономерностей процесса выведения одних формул из других и формулировка таких закономерностей в виде правил вывода. Получаемые вторичные правила вывода носят название *производных правил вывода*. Разделим их на две группы и сформулируем их в двух теоремах: в одной — производные правила введения логических связок, в другой — производные правила удаления таких связок. Для формулировки правил будет использоваться символическая запись. Например, правило

$$\frac{\Gamma \vdash F; \Gamma \vdash F \rightarrow G}{\Gamma \vdash G}$$

состоит в следующем: «Если $\Gamma \vdash F$ и $\Gamma \vdash F \rightarrow G$, то $\Gamma \vdash G$ ».

Теорема 15.9 (правила введения логических связок). *Справедливы следующие производные правила вывода, называемые правилами введения логических связок (где Γ — некоторое, возможно и пустое, множество формул):*

а) введение импликации ($\rightarrow$ -вв):

$$\frac{\Gamma, F \vdash G}{\Gamma \vdash F \rightarrow G};$$

б) введение конъюнкции ($\wedge$ -вв):

$$\frac{\Gamma \vdash F; \Gamma \vdash G}{\Gamma \vdash F \wedge G};$$

в) введение дизъюнкции ($\vee$ -вв):

$$\frac{\Gamma \vdash F}{\Gamma \vdash F \vee G}, \quad \frac{\Gamma \vdash G}{\Gamma \vdash F \vee G};$$

г) введение отрицания (приведение к абсурду) ($\neg$ -вв):

$$\frac{\Gamma, F \vdash G; \Gamma, F \vdash \neg G}{\Gamma \vdash \neg F}.$$

Доказательство. а) Данное правило есть не что иное, как теорема о дедукции (теорема 15.4).

б) Обосновать правило предлагается самостоятельно. Напомним только, что запись $F \wedge G$, согласно определению, означает $\neg(F \rightarrow \neg G)$.

в) Обоснуем первое правило. При доказательстве теоремы 15.8, в показано, что $\neg F, F \vdash G$, или $F, \neg F \vdash G$. Отсюда, по теореме о дедукции, заключаем, что $F \vdash \neg F \rightarrow G$, т.е. на основании определения логической связки дизъюнкции $F \vdash F \vee G$. Поэтому если $\Gamma \vdash F$, то отсюда, в силу теоремы 15.3, в, заключаем, что $\Gamma \vdash F \vee G$.

Обосновать второе правило введения дизъюнкции предлагается самостоятельно.

г) Пусть дано, что $\Gamma, F \vdash G$ и $\Gamma, F \vdash \neg G$. Тогда, по теореме о дедукции, $\Gamma \vdash F \rightarrow G$ и $\Gamma \vdash F \rightarrow \neg G$. Выпишем одну за другой обе последовательности формул, представляющие собой выводы формул $F \rightarrow G$ и $F \rightarrow \neg G$ из множества посылок Γ :

$$\begin{array}{l} \dots\dots\dots \\ (\alpha) \quad \quad \quad F \rightarrow G; \end{array}$$

$$\begin{array}{l} \dots\dots\dots \\ (\alpha + \beta) \quad \quad F \rightarrow \neg G. \end{array}$$

Продолжим полученную последовательность следующим образом:

- $(\alpha + \beta + 1) \quad (F \rightarrow G) \rightarrow (\neg G \rightarrow \neg F)$ [использована теорема 15.8, ∂];
- $(\alpha + \beta + 2) \quad \neg G \rightarrow \neg F$ [MP: $(\alpha), (\alpha + \beta + 1)$];
- $(\alpha + \beta + 3) \quad (\neg G \rightarrow \neg F) \rightarrow (\neg\neg F \rightarrow \neg\neg G)$ [теорема 15.8, ∂];
- $(\alpha + \beta + 4) \quad \neg\neg F \rightarrow \neg\neg G$ [MP: $(\alpha + \beta + 2), (\alpha + \beta + 3)$];
- $(\alpha + \beta + 5) \quad (F \rightarrow \neg G) \rightarrow (\neg\neg G \rightarrow \neg F)$ [теорема 15.8, ∂];
- $(\alpha + \beta + 6) \quad \neg\neg G \rightarrow \neg F$ [MP: $(\alpha + \beta), (\alpha + \beta + 5)$];
- $(\alpha + \beta + 7) \quad (\neg\neg G \rightarrow \neg F) \rightarrow (\neg\neg F \rightarrow \neg\neg\neg G)$ [теорема 15.8, ∂];
- $(\alpha + \beta + 8) \quad \neg\neg F \rightarrow \neg\neg\neg G$ [MP: $(\alpha + \beta + 6), (\alpha + \beta + 7)$];
- $(\alpha + \beta + 9) \quad \neg\neg\neg G \rightarrow \neg G$ [теорема 15.8, a];
- $(\alpha + \beta + 10) \quad \neg\neg F \rightarrow \neg G$ [лемма 15.7 a : $(\alpha + \beta + 8), (\alpha + \beta + 9)$];
- $(\alpha + \beta + 11) \quad (\neg\neg F \rightarrow \neg G) \rightarrow ((\neg\neg F \rightarrow \neg G) \rightarrow \neg F)$ [аксиома (A3)];
- $(\alpha + \beta + 12) \quad (\neg\neg F \rightarrow \neg G) \rightarrow \neg F$ [MP: $(\alpha + \beta + 4), (\alpha + \beta + 11)$];
- $(\alpha + \beta + 13) \quad \neg F$ [MP: $(\alpha + \beta + 10), (\alpha + \beta + 12)$].

Тем самым доказано, что $\Gamma \vdash \neg F$. $\square$

Теорема 15.10 (правила удаления логических связок). *Справедливы следующие производные правила вывода, называемые правилами удаления логических связок (где Γ — некоторое, возможно и пустое, множество формул):*

а) удаление импликации ($\rightarrow$ -уд):

$$\frac{\Gamma \vdash F; \Gamma \vdash F \rightarrow G}{\Gamma \vdash G};$$

б) удаление конъюнкции ($\wedge$ -уд):

$$\frac{\Gamma \vdash F \wedge G}{\Gamma \vdash F}, \quad \frac{\Gamma \vdash F \wedge G}{\Gamma \vdash G};$$

в) удаление конъюнкции ($\wedge$ -уд):

$$\frac{\Gamma, F, G \vdash H}{\Gamma, F \wedge G \vdash H};$$

г) удаление дизъюнкции (Генцен):

$$\frac{\Gamma \vdash F \vee G; \Gamma, F \vdash H; \Gamma, G \vdash H}{\Gamma \vdash H};$$

д) удаление дизъюнкции (Клини):

$$\frac{\Gamma, F \vdash H; \Gamma, G \vdash H}{\Gamma, F \vee G \vdash H};$$

е) сильное удаление отрицания (сильное $\neg$ -уд):

$$\frac{\Gamma \vdash \neg\neg F}{\Gamma \vdash F};$$

ж) слабое удаление отрицания (слабое $\neg$ -уд):

$$\frac{\Gamma \vdash F; \Gamma \vdash \neg F}{\Gamma \vdash G}.$$

Доказательство. а) Это правило получается непосредственно на основании правила вывода МР.

б) Обоснуем второе из двух правил удаления конъюнкции, предоставив сделать обоснование первого правила самостоятельно. Пусть $\Gamma \vdash F \wedge G$. Покажем, что $F \wedge G \vdash G$. Напомним, что по определению конъюнкции запись $F \wedge G$ означает $\neg(F \rightarrow \neg G)$. Поэтому нужно показать, что $\neg(F \rightarrow \neg G) \vdash G$. Строим соответствующий вывод:

(1): $\neg(F \rightarrow \neg G)$	[использована гипотеза];
(2): $\neg(F \rightarrow \neg G) \rightarrow (\neg G \rightarrow \neg(F \rightarrow \neg G))$	[аксиома (A1)];
(3): $\neg G \rightarrow \neg(F \rightarrow \neg G)$	[МР: (1), (2)];
(4): $(\neg G \rightarrow \neg(F \rightarrow \neg G)) \rightarrow ((\neg G \rightarrow (F \rightarrow \neg G)) \rightarrow G)$	[аксиома (A3)];
(5): $(\neg G \rightarrow (F \rightarrow \neg G)) \rightarrow G$	[МР: (3), (4)];
(6): $\neg G \rightarrow (F \rightarrow \neg G)$	[аксиома (A1)];
(7): G	[МР: (5), (6)].

Итак, $\Gamma \vdash F \wedge G$ и $F \wedge G \vdash G$. Следовательно, по теореме 15.3, $\forall$ заключаем, что $\Gamma \vdash G$.

е) Пусть $\Gamma \vdash \neg\neg F$. Ввиду теоремы 15.8, а имеем $\vdash \neg\neg F \rightarrow F$, что на основании следствия 15.6 из теоремы о дедукции дает выводимость $\neg\neg F \vdash \rightarrow F$. Следовательно, из двух выводимостей $\Gamma \vdash \neg\neg F$ и $\neg\neg F \vdash \rightarrow F$ по теореме 15.3, $\forall$ заключаем, что $\Gamma \vdash F$.

Остальные правила вывода рассматриваются в Задачнике (см. № 8.19, 8.20). Там же в задачах № 8.21 и 8.22 приведены примеры доказательств с использованием производных правил вывода. $\square$

§ 16. Полнота и другие свойства формализованного исчисления высказываний

Если при изложении материала § 15 рассмотрение велось как бы изнутри аксиоматической теории высказываний в процессе развития темы, то ознакомление с наукой об аксиоматической теории высказываний строят, опираясь на другой подход. Установив ряд важных свойств этой теории: полноту, разрешимость, непротиворечивость.

Доказуемость формулы и ее тождественная истинность (синтаксис и семантика). В основе формализованного исчисления высказываний лежат понятия, относящиеся к так называемой области синтаксиса, т.е. понятия, представляющие собой некие абстрактные, лишенные смысла знаки и формальные действия с ними: алфавит, формула, аксиома, правило вывода, доказательство, теорема. Эти понятия принято называть *синтаксическими*.

В то же время алгебра высказываний, изложенная в гл. I, пронизана содержательным смыслом: за каждой пропозициональной переменной стоит конкретное высказывание нашего языка, каждая формула может превращаться в конкретное составное высказывание, некоторые формулы могут превращаться только в истинные высказывания (тавтологии) и т.д. В данной сфере, являющейся областью семантики, каждое понятие наполнено каким-то внутренним содержанием, смыслом. Понятия истины и лжи, тождественной истинности и тождественной ложности формул, равносильности и логического следования формул считают понятиями *семантическими*.

Каково же взаимоотношение между формализованным исчислением высказываний и алгеброй высказываний, между синтаксисом и семантикой? Перекинуть мостик от одной области к другой и призвана теорема полноты, о которой пойдет речь в настоящем параграфе. Оказывается, формализованное исчисление высказываний построено так, что всякая его теорема является тавтологией (тождественно истинной формулой) алгебры высказываний, и, обратно, для всякой тавтологии алгебры высказываний можно построить ее вывод из аксиом формализованного исчисления высказываний, т.е. доказать, что она является теоремой исчисления. В этом состоит *теорема полноты*. Таким образом, теорема полноты как бы свяжет абстрактную аксиоматическую теорию высказываний и содержательную алгебру высказываний, теорию с практикой, и тем самым продемонстрирует адекватность отражения абстрактной теорией наших практических знаний о высказываниях языка.

Сформулируем и докажем первую часть теоремы полноты.

Теорема 16.1. *Всякая доказуемая в формализованном исчислении высказываний формула является тождественно истинной формулой (или тавтологией) алгебры высказываний. Символически: $\vdash F \Rightarrow \models F$.*

Доказательство. Пусть формула F доказуема в формализованном исчислении высказываний и последовательность $B_1, B_2, \dots, B_s$ представляет собой вывод формулы F из аксиом. Покажем, что F — тавтология. Доказательство будем вести индукцией по длине s вывода этой формулы:

1) $s = 1$. Тогда последовательность-вывод состоит из единственной формулы B_1 , которая, следовательно, может быть на основании определения вывода только аксиомой. Все три аксиомы (A1),

(A2) и (A3) являются тавтологиями алгебры высказываний на основании теорем 3.1, з, 3.3, а, 3.3, л соответственно;

2) $s \leq n$. Предположим теперь, что все формулы, имеющие вывод длины $s \leq n$, являются тавтологиями. Это предположение индукции;

3) $s = n + 1$. Покажем, что всякая формула, имеющая вывод длины $s = n + 1$, также является тавтологией. В самом деле, пусть F — произвольная формула и $B_1, B_2, \dots, B_n, B_{n+1} \equiv F$ — ее вывод длины $n + 1$. На основании предположения индукции первые n членов данной последовательности — тавтологии. Рассмотрим формулу B_{n+1} . По определению вывода, она может быть либо аксиомой (и тогда она является тавтологией, как было отмечено в первой части доказательства), либо получена из двух предыдущих членов этой последовательности B_i и B_j ($1 \leq i \leq n - 1, 2 \leq j \leq n$) по правилу МР. Во втором случае тогда $B_j \equiv B_i \rightarrow B_{n+1}$ и, кроме того, обе формулы B_i и B_j являются тавтологиями на основании предположения индукции. Итак, $\equiv B_i \equiv B_i \rightarrow B_{n+1}$. Следовательно, по теореме 3.5 (правило заключения) $\equiv B_{n+1}$.

Итак, какой бы длины ни имела вывод в формализованном исчислении высказываний формула, она будет тавтологией алгебры высказываний. $\square$

Для доказательства второй части теоремы полноты (т.е. теоремы, обратной к только что доказанной теореме) понадобится одна лемма, которой и посвящается следующий пункт.

Лемма о выводимости. Пусть $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ — упорядоченный набор длины n , составленный из нулей и единиц, т.е. каждое $\sigma_i = 0$ или 1 ($i = 1, 2, \dots, n$). Из доказательства теоремы 10.3 известно, что всего таких наборов имеется 2^n штук.

Определение 16.2. σ -Двойником, где $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$, для формулы $F(X_1, X_2, \dots, X_n)$ называется или сама эта формула, если она превращается в истинное высказывание $F(A_1, A_2, \dots, A_n)$ при подстановке вместо ее пропозициональных переменных $X_1, X_2, \dots, X_n$ таких высказываний $A_1, A_2, \dots, A_n$ соответственно, что $\lambda(A_1) = \sigma_1, \lambda(A_2) = \sigma_2, \dots, \lambda(A_n) = \sigma_n$, или формула $\neg F(X_1, X_2, \dots, X_n)$, если при указанной подстановке она превращается в ложное высказывание $F(A_1, A_2, \dots, A_n)$. Обозначение σ -двойника для формулы $F(X_1, X_2, \dots, X_n)$ следующее: $F^\sigma(X_1, X_2, \dots, X_n)$. Тогда символически данное определение можно записать так:

$$F^\sigma(X_1, X_2, \dots, X_n) = \begin{cases} F(X_1, X_2, \dots, X_n), & \text{если } F(\sigma_1, \sigma_2, \dots, \sigma_n) = 1, \\ \neg F(X_1, X_2, \dots, X_n), & \text{если } F(\sigma_1, \sigma_2, \dots, \sigma_n) = 0. \end{cases}$$

Пример 16.3. Найти σ -двойники для формул

$$F(X_1, X_2, X_3, X_4) \equiv (X_1 \rightarrow \neg X_2) \vee (X_3 \wedge (\neg X_1 \leftrightarrow X_4)),$$

$$G(X_1, X_2, X_3, X_4) \equiv (X_1 \vee \neg X_3) \leftrightarrow (X_2 \wedge (\neg X_3 \rightarrow \neg X_4)),$$

если $\sigma = (0, 1, 1, 0)$.

Находим сначала значения этих формул при подстановке вместо переменных X_1, X_2, X_3, X_4 значений 0, 1, 1, 0 соответственно:

$$F(0, 1, 1, 0) = (0 \rightarrow \neg 1) \vee (1 \wedge (\neg 0 \leftrightarrow 0)) = (0 \rightarrow 0) \vee (1 \wedge (1 \leftrightarrow 0)) = 1 \vee (1 \wedge 0) = 1 \vee 0 = 1;$$

$$G(0, 1, 1, 0) = (0 \vee \neg 1) \leftrightarrow (1 \wedge (\neg 1 \rightarrow \neg 0)) = (0 \vee 0) \leftrightarrow \leftrightarrow (1 \wedge (0 \rightarrow 1)) = 0 \leftrightarrow (1 \wedge 1) = 0 \leftrightarrow 1 = 0.$$

Тогда, по определению σ -двойника, имеем

$$F^\sigma(X_1, X_2, \dots, X_n) \equiv (X_1 \vee \neg X_3) \leftrightarrow (X_2 \wedge (\neg X_3 \rightarrow \neg X_4)),$$

$$G^\sigma(X_1, X_2, \dots, X_n) \equiv \neg((X_1 \vee \neg X_3) \leftrightarrow (X_2 \wedge (\neg X_3 \rightarrow \neg X_4))).$$

Лемма 16.4 (о выводимости). Для всякой формулы $F(X_1, X_2, \dots, X_n)$ и всякого набора $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$, где $\sigma_i = 0$ или 1 ($i = 1, 2, \dots, n$), справедлива следующая выводимость:

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash F^\sigma(X_1, X_2, \dots, X_n),$$

где

$$X_i^{\sigma_i} = \begin{cases} X_i, & \text{если } \sigma_i = 1, \\ \neg X_i, & \text{если } \sigma_i = 0. \end{cases}$$

Доказательство. Для доказательства применим индукцию по числу l логических связок, использованных при построении формулы F :

1) $l = 0$ (в формуле F нет логических связок). В этом случае формула F есть пропозициональная переменная, например X_1 . Тогда $F^\sigma = X_1^\sigma$, и утверждение леммы принимает следующую очевидную форму: $X_1^\sigma \vdash X_1^\sigma$;

2) $l \leq k$. Предположим, что утверждение леммы справедливо для всех формул с числом логических связок $l \leq k$;

3) $l = k + 1$. Покажем тогда, что утверждение леммы будет справедливо и для любой формулы с числом логических связок $l = k + 1$. Пусть $F(X_1, X_2, \dots, X_n)$ — произвольная такая формула. Тогда на основании определения формулы формализованного исчисления высказываний (см. первый пункт § 15) F имеет один из следующих двух видов: $F \equiv \neg G$ или $F \equiv G \rightarrow H$. Рассмотрим последовательно эти две возможности.

Пусть сначала $F \equiv \neg G$. Тогда формула $G(X_1, X_2, \dots, X_n)$ содержит $\leq k$ логических связок, и для нее, по предположению индукции, будет справедлива выводимость

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash G^\sigma(X_1, X_2, \dots, X_n).$$

Покажем, что $G^\sigma \vdash F^\sigma$, т.е. $G^\sigma \vdash (\neg G)^\sigma$. В самом деле, если набор $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ таков, что $G(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$, то $\neg G(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$. Далее, по определению 16.2 σ -двойника

имеем $G^\sigma = \neg G$ и $(\neg G)^\sigma = \neg G$. В этом случае требуемая выводимость принимает следующую очевидную форму: $\neg G \vdash \neg G$. Если же набор $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ таков, что $G(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$, то $\neg G(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$ и соответствующие σ -двойники таковы: $G^\sigma = G$ и $(\neg G)^\sigma = \neg \neg G$. В этом случае требуемая выводимость принимает форму $G \vdash \neg \neg G$. Данная выводимость действительно справедлива на основании теоремы 15.8, б и следствия 15.5 из теоремы о дедукции.

Итак, $X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash G^\sigma (X_1, X_2, \dots, X_n)$ и $G^\sigma \vdash F^\sigma$. Тогда, в силу теоремы 15.3, в, $X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash F^\sigma (X_1, X_2, \dots, X_n)$.

Рассмотрим теперь вторую возможность: $F \equiv G \rightarrow H$. Снова каждая из формул G и H содержит $\leq k$ логических связок; для каждой из них будет справедливо предположение индукции:

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash G^\sigma (X_1, X_2, \dots, X_n);$$

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash H^\sigma (X_1, X_2, \dots, X_n).$$

Покажем, что $G^\sigma, H^\sigma \vdash F^\sigma$, т.е. $G^\sigma, H^\sigma \vdash (G \rightarrow H)^\sigma$. Расшифруем значения σ -двойников во всех случаях, которые могут представиться:

1) набор $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ таков, что $G(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$ и $H(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$. Тогда $G(\sigma_1, \sigma_2, \dots, \sigma_n) \rightarrow H(\sigma_1, \sigma_2, \dots, \sigma_n) = 0 \rightarrow 0 = 1$ и σ -двойники имеют вид: $G^\sigma \equiv \neg G$, $H^\sigma \equiv \neg H$, $(G \rightarrow H)^\sigma \equiv G \rightarrow H$. Требуемая выводимость принимает следующий вид: $\neg G, \neg H \vdash G \rightarrow H$. Покажем, что это действительно так. В самом деле, на основании теоремы 15.8, в, имеем $\vdash \neg G \rightarrow (G \rightarrow H)$. Тогда, по следствию 15.5 из теоремы о дедукции, заключаем, что $\neg G \vdash G \rightarrow H$. Применив теорему 15.3, а, получаем $\neg G, \neg H \vdash G \rightarrow H$;

2) набор $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ таков, что $G(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$ и $H(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$. Тогда $G(\sigma_1, \sigma_2, \dots, \sigma_n) \rightarrow H(\sigma_1, \sigma_2, \dots, \sigma_n) = 0 \rightarrow 1 = 1$, и σ -двойники имеют в этом случае следующий вид: $G^\sigma \equiv \neg G$, $H^\sigma \equiv H$, $(G \rightarrow H)^\sigma \equiv G \rightarrow H$. Требуемая выводимость принимает следующий вид: $\neg G, H \vdash G \rightarrow H$. Ее доказательство ничем не отличается от доказательства выводимости в предыдущем случае;

3) набор $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ таков, что $G(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$ и $H(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$. Тогда $G(\sigma_1, \sigma_2, \dots, \sigma_n) \rightarrow H(\sigma_1, \sigma_2, \dots, \sigma_n) = 1 \rightarrow 0 = 0$ и σ -двойники имеют следующий вид: $G^\sigma \equiv G$, $H^\sigma \equiv \neg H$, $(G \rightarrow H)^\sigma \equiv \neg(G \rightarrow H)$. Требуемая выводимость принимает следующий вид: $G, \neg H \vdash \neg(G \rightarrow H)$. Покажем, что это действительно так. Ясно, что справедливы выводимости $G, \neg H, G \rightarrow H \vdash \neg H$ и $G, \neg H, G \rightarrow H \vdash H$ (первая очевидна, а вторая следует на основе правила МР: $G, G \rightarrow H \vdash H$). Из них, по правилу введения отрицания (теорема 15.9, з), получаем $G, \neg H \vdash \neg(G \rightarrow H)$;

4) набор $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ таков, что $G(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$ и $H(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$. Тогда $G(\sigma_1, \sigma_2, \dots, \sigma_n) \rightarrow H(\sigma_1, \sigma_2, \dots, \sigma_n) = 1 \rightarrow 1 = 1$ и σ -двойники имеют вид: $G^\sigma \equiv G$, $H^\sigma \equiv H$, $(G \rightarrow H)^\sigma \equiv G \rightarrow H$. Требуемая выводимость принимает следующий вид: $G, H \vdash G \rightarrow H$.

Проверим, что это действительно так. Рассмотрим последовательность формул $H, H \rightarrow (G \rightarrow H), G \rightarrow H$. Первую формулу последовательности будем считать гипотезой. Вторая формула представляет собой аксиому (A1) формализованного исчисления высказываний, а третья получена из двух предыдущих по правилу МР. Следовательно, рассматриваемая последовательность есть вывод ее последней формулы $G \rightarrow H$ из гипотезы H . Итак, $H \vdash G \rightarrow H$. Вспоминая теорему 15.3, а, заключаем, что $G, H \vdash G \rightarrow H$.

Итак, рассмотренные четыре случая приводят к заключению: для любого набора σ нулей и единиц справедлива выводимость $G^\sigma, H^\sigma \vdash F^\sigma$, которая вместе с выводимостями (1) и (2) дает следующую выводимость: $X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash F^\sigma(X_1, X_2, \dots, X_n)$.

Тем самым сделан шаг индукции, и можно заключить, что утверждение леммы справедливо для любой формулы F . $\square$

Полнота формализованного исчисления высказываний. В первом пункте настоящего параграфа было сказано, что полнота формализованного исчисления высказываний состоит в совпадении множества доказуемых формул с множеством тавтологий. Включение первого множества во второе (первая часть теоремы полноты) было установлено в теореме 16.1. Теперь нами все подготовлено к тому, чтобы доказать вторую часть теоремы о полноте формализованного исчисления высказываний.

Теорема 16.5. *Всякая тождественно истинная формула (или тавтология) алгебры высказываний доказуема в формализованном исчислении высказываний. Символически: $\models F \Rightarrow \vdash F$.*

Доказательство. Пусть формула $F(X_1, X_2, \dots, X_n)$ является тавтологией алгебры высказываний. На основании леммы 16.4 о выводимости, имеем $X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash F^\sigma(X_1, X_2, \dots, X_n)$ для любого набора $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ из нулей и единиц. Поскольку формула $F(X_1, X_2, \dots, X_n)$ при любой подстановке превращается в истинное высказывание (она — тавтология), то для любого набора $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n)$ σ -двойником формулы F будет сама эта формула, т.е. $F^\sigma = F$ для любого σ . Тогда $X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_n^{\sigma_n} \vdash F(X_1, X_2, \dots, X_n)$. В частности, для $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_{n-1}, 1)$ имеем (в этом случае $X_n^{\sigma_n} = X_n^1 = X_n$)

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-1}^{\sigma_{n-1}}, X_n \vdash F(X_1, X_2, \dots, X_n), \quad (1)$$

а для $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_{n-1}, 0)$ имеем (в этом случае $X_n^{\sigma_n} = X_n^0 = \neg X_n$)

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-1}^{\sigma_{n-1}}, \neg X_n \vdash F(X_1, X_2, \dots, X_n). \quad (2)$$

Из выводимостей (1) и (2) по правилу удаления дизъюнкции (теорема 15.10, δ) получаем $X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-1}^{\sigma_{n-1}}, X_n \vee \neg X_n \vdash F(X_1, X_2, \dots, X_n)$. Поскольку формула $X_n \vee \neg X_n$ выводима из аксиом (см. определение связки $\vee$ в начале § 15 и пример 15.2), то ее можно исключить из числа посылок последней выводимости. Тогда

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-1}^{\sigma_{n-1}} \vdash F(X_1, X_2, \dots, X_n).$$

Далее нужно брать в качестве σ наборы следующих видов: $\sigma = (\sigma_1, \sigma_2, \dots, 1, \sigma_n)$ и $\sigma = (\sigma_1, \sigma_2, \dots, 0, \sigma_n)$, для которых соответственно получим

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-2}^{\sigma_{n-2}}, X_{n-1} \vdash F(X_1, X_2, \dots, X_n),$$

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-2}^{\sigma_{n-2}}, \neg X_{n-1} \vdash F(X_1, X_2, \dots, X_n).$$

Отсюда, также по правилу удаления дизъюнкции, получаем

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-2}^{\sigma_{n-2}}, X_{n-1} \vee \neg X_{n-1} \vdash F(X_1, X_2, \dots, X_n)$$

и далее

$$X_1^{\sigma_1}, X_2^{\sigma_2}, \dots, X_{n-2}^{\sigma_{n-2}} \vdash F(X_1, X_2, \dots, X_n).$$

Проделав n раз эту процедуру, придем к заключению, что $\vdash F$, т.е. формула F доказуема в формализованном исчислении высказываний. $\square$

Объединив теоремы 16.1 и 16.5, получим теорему о полноте.

Теорема 16.6 (о полноте формализованного исчисления высказываний). *Формула тогда и только тогда доказуема в формализованном исчислении высказываний (является теоремой исчисления), когда она является тавтологией алгебры высказываний. Символически: $\vdash F \Leftrightarrow \models F$.*

Теорема адекватности. Теорема адекватности является обобщением предыдущей теоремы о полноте и вытекает из нее.

Теорема 16.7 (адекватности). *Формула G выводима в формализованном исчислении высказываний из конечного множества гипотез Γ тогда и только тогда, когда она является логическим следствием всех формул из этого множества. Символически:*

$$F_1, F_2, \dots, F_m \vdash G \Leftrightarrow F_1, F_2, \dots, F_m \models G.$$

Доказательство. Пусть $F_1, F_2, \dots, F_m \vdash G$. Тогда, по следствию 15.6 из теоремы о дедукции, данное утверждение эквивалентно тому, что

$$\vdash F_1 \rightarrow (F_2 \rightarrow \dots \rightarrow (F_{m-1} \rightarrow (F_m \rightarrow G)) \dots).$$

Это утверждение, в свою очередь, эквивалентно, на основании теоремы полноты, следующему:

$$\models F_1 \rightarrow (F_2 \rightarrow \dots \rightarrow (F_{m-1} \rightarrow (F_m \rightarrow G)) \dots).$$

Теперь можно использовать результаты алгебры высказываний. На основании теоремы 4.4, z последняя формула равносильна формуле

$$(F_1 \wedge F_2 \wedge \dots \wedge F_m) \rightarrow G.$$

(Точнее, на основании этой теоремы можно утверждать равносильность данных формул лишь при $m = 2$, но ясно, что утверждение нетрудно распространить и на произвольное натуральное число m , например, методом математической индукции, что рекомендуется проделать самостоятельно; см. также № 1.29, z Задачника). Тогда из тождественной истинности одной из формул и их равносильности заключаем, что и вторая формула также будет тавтологией (см. замечание 4.7). Итак,

$$\models (F_1 \wedge F_2 \wedge \dots \wedge F_m) \rightarrow G.$$

Это утверждение на основании теоремы 6.4 эквивалентно следующему: $F_1, F_2, \dots, F_m \models G$, что и требовалось доказать. $\square$

Непротиворечивость формализованного исчисления высказываний. Непротиворечивость — важнейшее свойство, которым должна обладать аксиоматическая теория. Противоречивая теория никакой ценности не имеет.

Определение 16.8. Аксиоматическая теория называется *непротиворечивой*, если ни для какого утверждения A , сформулированного в терминах этой теории, само утверждение A и его отрицание $\neg A$ не могут быть одновременно теоремами данной теории. Если для некоторого утверждения A теории оба утверждения A и $\neg A$ — теоремы этой теории, то аксиоматическая теория называется *противоречивой*.

Применительно к формализованному исчислению высказываний непротиворечивость означает, что в нем не существует такой формулы F , что сама формула и ее отрицание $\neg F$ являются теоремами формализованного исчисления высказываний, т. е. выводимы из аксиом. Следующая теорема утверждает, что это действительно так.

Теорема 16.9 (о непротиворечивости формализованного исчисления высказываний). *Формализованное исчисление высказываний есть непротиворечивая аксиоматическая теория.*

Доказательство. Допустим противное, т. е. предположим, что формализованное исчисление высказываний противоречиво. Значит, имеется такая формула F , что F и $\neg F$ являются теоремами формализованного исчисления высказываний. Тогда по теореме 16.1 каждая из формул F и $\neg F$ является тавтологией алгебры высказываний. Но последнее невозможно на основании определения тавтологии. Следовательно, формализованное исчисление высказываний непротиворечиво. $\square$

Разрешимость формализованного исчисления высказываний. **Определение 16.10.** Аксиоматическая теория называется *разрешимой*, если

существует алгоритм, позволяющий для любого утверждения, сформулированного в терминах теории, ответить на вопрос, будет или нет это утверждение теоремой данной теории.

Теорема 16.11 (разрешимости формализованного исчисления высказываний). *Формализованное исчисление высказываний есть разрешимая аксиоматическая теория.*

Доказательство. Для доказательства теоремы нужно указать алгоритм, позволяющий для каждой формулы формализованного исчисления высказываний отвечать на вопрос, можно или нельзя вывести ее из аксиом. Такой алгоритм есть. На основании теоремы 16.6 о полноте формализованного исчисления высказываний доказуемость формулы в формализованном исчислении высказываний эквивалентна тождественной истинности данной формулы в алгебре высказываний. Для проверки последнего свойства нужно составить таблицу истинности формулы. Если последний столбец таблицы будет состоять лишь из единиц, то формула является тавтологией, а следовательно, и теоремой формализованного исчисления высказываний. Если же там встретятся нули, то формула — не тавтология, а значит, и не теорема. $\square$

§ 17. Независимость системы аксиом формализованного исчисления высказываний

В этом параграфе будет подвергнута анализу основа аксиоматической теории высказываний, т.е. система аксиом, на которой она базируется, для установления важного ее свойства.

Понятие независимости. После того как теория построена (§ 15) и установлен ряд ее свойств (§ 16), следует обратиться к ее истокам — к системе аксиом — для решения ряда вопросов. Почему в качестве аксиом выбраны именно эти формулы? Можно ли взять другие формулы в качестве аксиом? (Уже отмечалось, что имеется множество других аксиоматик для аксиоматической теории высказываний.) Можно ли сократить число аксиом до двух или одной? Можно ли из данной системы аксиом безболезненно исключить одну или две формулы? Ответу на последний вопрос и посвящается настоящий параграф.

Определение 17.1. Аксиома A из системы аксиом Σ называется *независящей от остальных аксиом* этой системы, если ее нельзя вывести (доказать) из множества $\Sigma \setminus \{A\}$ всех остальных аксиом системы Σ . Система аксиом Σ называется *независимой*, если каждая ее аксиома не зависит от остальных.

Из определения следует, как нужно доказывать независимость той или иной аксиомы от остальных аксиом данной системы. Нужно смоделировать одновременно все аксиомы данной системы, кроме той, независимость которой доказывается, т.е. построить модель, в которой бы выполнялись все аксиомы данной системы,

кроме анализируемой аксиомы. Это означает, что каждому первоначальному понятию и отношениям между понятиями нужно придать конкретное содержание посредством каких-то конкретных предметов и отношений между ними. Причем сделать это нужно так, чтобы выбранные конкретные предметы и отношения между ними обладали свойствами, сформулированными в аксиомах из системы $\Sigma \setminus \{A\}$, и не обладали бы свойством A . Такая совокупность конкретных предметов и отношений между ними называется *моделью системы аксиом* $\Sigma \setminus \{A\}$. Наличие ее доказывает независимость аксиомы A от аксиом из $\Sigma \setminus \{A\}$. В самом деле, ведь если A можно было бы вывести из $\Sigma \setminus \{A\}$, то во всякой модели, в которой выполнялись бы все аксиомы из $\Sigma \setminus \{A\}$, непременно выполнялась бы и аксиома A , и такой модели, в которой выполнялись бы все аксиомы из $\Sigma \setminus \{A\}$ и не выполнялась A , просто не существовало бы.

Докажем, что система аксиом (A1), (A2), (A3) формализованного исчисления высказываний независима с помощью построения соответствующих моделей.

Независимость аксиомы (A1). Доказательство осуществляется построением модели, в которой выполняются аксиомы (A2) и (A3), но не выполняется аксиома (A1).

Лемма 17.2. *Аксиома (A1) не зависит от остальных аксиом (A2) и (A3) формализованного исчисления высказываний.*

Доказательство. Рассмотрим трехэлементное множество $M = \{0, 1, 2\}$ и введем в нем две операции. Первая операция — унарная, сопоставляющая каждому элементу $A \in M$ элемент из M , обозначаемый $\neg A$; вторая — бинарная, сопоставляющая любым двум элементам $A, B \in M$ элемент из M , обозначаемый $A \rightarrow B$. Причем сопоставление осуществляется по правилам, определяемым следующими таблицами:

A	$\neg A$
0	1
1	1
2	0

A	B	$A \rightarrow B$
0	0	0
0	1	2
0	2	2
1	0	2
1	1	2
1	2	0
2	0	0
2	1	0
2	2	0

Если теперь всем переменным, входящим в формулу формализованного исчисления высказываний, придать некоторые значе-

ния из M , то согласно введенным правилам сама формула примет некоторое значение из M . Формулу, всегда принимающую значение 0, назовем *выделенной*.

Во-первых, можно показать, что всякая формула, получающаяся по схеме аксиомы (A2), является выделенной. Для этого составим таблицу значений формулы (A2) (предпоследний столбец соответствует формуле $K \equiv (F \rightarrow G) \rightarrow (F \rightarrow H)$):

F	G	H	$G \rightarrow H$	$F \rightarrow (G \rightarrow H)$	$F \rightarrow G$	$F \rightarrow H$	K	(A2)
0	0	0	0	0	0	0	0	0
0	0	1	2	2	0	2	2	0
0	0	2	2	2	0	2	2	0
0	1	0	2	2	2	0	0	0
0	1	1	2	2	2	2	0	0
0	1	2	0	0	2	2	0	0
0	2	0	0	0	2	0	0	0
0	2	1	0	0	2	2	0	0
0	2	2	0	0	2	2	0	0
1	0	0	0	2	2	2	0	0
1	0	1	2	0	2	2	0	0
1	0	2	2	0	2	0	0	0
1	1	0	2	0	2	2	0	0
1	1	1	2	0	2	2	0	0
1	1	2	0	2	2	0	0	0
1	2	0	0	2	0	2	2	0
1	2	1	0	2	0	2	2	0
1	2	2	0	2	0	0	2	0
2	0	0	0	0	0	0	0	0
2	0	1	2	0	0	0	0	0
2	0	2	2	0	0	0	0	0
2	1	0	2	0	0	0	0	0
2	1	1	2	0	0	0	0	0
2	1	2	0	0	0	0	0	0
2	2	0	0	0	0	0	0	0
2	2	1	0	0	0	0	0	0
2	2	2	0	0	0	0	0	0

Во-вторых, необходимо показать, что всякая формула, получающаяся по схеме аксиомы (A3), также является выделенной. Предлагается самостоятельно составить таблицу значений форму-

лы (A3) и убедиться в том, что в ее последнем столбце стоят лишь нули (в таблице будет девять строк).

В-третьих, покажем, что правило вывода МР сохраняет свойство выделенности, т. е. если формулы F и $F \rightarrow G$ выделенные, то и формула G — выделенная. В самом деле, в таблице, определяющей операцию $\rightarrow$ над элементами множества $M = \{0, 1, 2\}$, видим, что формулы F и $F \rightarrow G$ принимают одновременно значение 0 только в первой строке. Но в этой строке и формула G также принимает значение 0.

Итак, на основании трех доказанных утверждений можно сделать следующий вывод: всякая формула, выводимая из аксиом (A2) и (A3) с помощью правила МР, является выделенной.

Теперь, чтобы убедиться, что формула (A1) не может быть выведена из аксиом (A2) и (A3) с помощью правила МР, нужно установить, что она не является выделенной. В самом деле, если, например, F принимает значение 1, а G принимает значение 2, то вычисляем значение формулы (A1): $F \rightarrow (G \rightarrow F) = 1 \rightarrow (2 \rightarrow 1) = 1 \rightarrow 0 = 2 \neq 0$.

Требуемая модель построена, и лемма тем самым полностью доказана. $\square$

Независимость аксиомы (A2). Здесь строится модель, в которой выполняются аксиомы (A1) и (A3), но не выполняется аксиома (A2).

Лемма 17.3. *Аксиома (A2) не зависит от аксиом (A1) и (A3) формализованного исчисления высказываний.*

Доказательство. Снова рассмотрим трехэлементное множество $M = \{0, 1, 2\}$, но операции $\neg$ и $\rightarrow$ над его элементами зададим по-другому, с помощью следующих таблиц:

A	$\neg B$
0	1
1	0
2	1

A	B	$A \rightarrow B$
0	0	0
0	1	2
0	2	1
1	0	0
1	1	2
1	2	0
2	0	0
2	1	0
2	2	0

Снова назовем формулу исчисления высказываний *выделенной*, если при всякой подстановке вместо ее переменных любых элементов из M она принимает значение 0. Предлагается самостоятельно проверить, что всякая формула, построенная как по схеме

аксиом (A1), так и по схеме аксиом (A3), является выделенной. Нетрудно также видеть, что правило вывода МР сохраняет свойство выделенности, т.е. если формулы F и $F \rightarrow G$ выделенные, то и формула G — выделенная. Следовательно, всякая формула, выводимая из аксиом (A1) и (A3) с помощью правила МР, является выделенной.

Теперь, чтобы убедиться, что формула (A2) не может быть выведена из аксиом (A1) и (A3) с помощью правила МР, нужно установить, что (A2) не является выделенной. Действительно, если, например, F придать значение 0, $G = 0$ и $H = 1$, то (A2) примет значение 2. $\square$

Независимость аксиомы (A3). Метод построения соответствующей модели не единственный путь доказательства независимости той или иной аксиомы от остальных аксиом данной системы. Покажем независимость аксиомы (A3) другим методом.

Лемма 17.4. *Аксиома (A3) не зависит от остальных аксиом (A1) и (A2) формализованного исчисления высказываний.*

Доказательство. Пусть F — произвольная формула формализованного исчисления высказываний. Обозначим через $h(F)$ формулу, полученную из F стиранием всех вхождений знака $\neg$ в формуле F . Легко понять, что для всякого частного случая F схем (A1) и (A2) формула $h(F)$ есть тавтология алгебры высказываний. Далее, правило вывода МР обладает следующим свойством: если $h(F \rightarrow G)$ и $h(F)$ — тавтологии, то и $h(G)$ — тавтология (так как $h(F \rightarrow G)$ совпадает с формулой $h(F) \rightarrow h(G)$). Следовательно, всякая формула F , выводимая из (A1) и (A2) с помощью правила МР, имеет в качестве $h(F)$ тавтологию.

Убедимся, что формула (A3) не выводима из (A1), (A2) с помощью правила МР. Для этого нужно проверить, что какая-либо конкретная формула F , получающаяся по схеме (A3), имеет в качестве $h(F)$ формулу, не являющуюся тавтологией. Действительно, формула $h[(\neg X \rightarrow \neg X) \rightarrow ((\neg X \rightarrow X) \rightarrow X)]$ есть следующая $(X \rightarrow X) \rightarrow ((X \rightarrow X) \rightarrow X)$. Нетрудно проверить, что последняя формула не является тавтологией. (Найдите ее значение при $X = 0$.) Следовательно, формула (A3) не выводима из (A1) и (A2). $\square$

Независимость системы аксиом. Из лемм 17.2—17.4 вытекает следующая теорема.

Теорема 17.5. *Система аксиом (A1), (A2), (A3) формализованного исчисления высказываний независима.*

Глава IV

ЛОГИКА ПРЕДИКАТОВ

Предикаты вслед за высказываниями являются следующим важным предметом, исследуемым математической логикой. Понятие предиката обобщает понятие высказывания, а теория предикатов представляет собой более тонкий инструмент, по сравнению с теорией высказываний, для изучения закономерностей процессов умозаключения и логического следования, составляющих предмет математической логики. В настоящей главе рассматриваются основы теории предикатов.

§ 18. Основные понятия, связанные с предикатами

Понятие предиката. В высказывании все четко: это — конкретное утверждение о конкретных объектах — истинное или ложное. Предикат — предложение, похожее на высказывание, но все же им не являющееся: о нем нельзя судить, истинно оно или ложно. Дадим точное определение.

Определение 18.1. Определенным на множествах $M_1, M_2, \dots, M_n$ n -местным предикатом называется предложение, содержащее n переменных $x_1, x_2, \dots, x_n$, превращающееся в высказывание при подстановке вместо этих переменных любых конкретных элементов из множеств $M_1, M_2, \dots, M_n$ соответственно.

Для n -местного предиката будем использовать обозначение $P(x_1, x_2, \dots, x_n)$. Переменные $x_1, x_2, \dots, x_n$ называют *предметными*, а элементы множеств $M_1, M_2, \dots, M_n$, которые эти переменные пробегает, — конкретными предметами. Всякий n -местный предикат $P(x_1, x_2, \dots, x_n)$, определенный на множествах $M_1, M_2, \dots, M_n$, представляет собой функцию n аргументов, заданную на указанных множествах и принимающую значения в множестве всех высказываний. Поэтому предикат называют также *функцией-высказыванием*.

Рассмотрим пример. Предложение «Река x впадает в озеро Байкал» является одноместным предикатом, определенным над множеством всех названий рек. Подставив вместо предметной переменной x название «Баргузин», получим высказывание «Река Баргузин впадает в озеро Байкал». Это высказывание истинно. Под-

ставив вместо предметной переменной x название «Днепр», получим ложное высказывание «Река Днепр впадает в озеро Байкал».

Другой п р и м е р. Предложение (выражение) « $x^2 + y^2 \leq 9$ » является двухместным предикатом, заданным над множествами R, R . Множества, на которых задан двухместный предикат, совпадают (говорят, что «двухместный предикат задан на множестве R^2 »). Пара действительных чисел 2, 2 превращает данный предикат в истинное высказывание: « $2^2 + 2^2 \leq 9$ », а пара чисел 2, 3 — в ложное: « $2^2 + 3^2 \leq 9$ ».

Отметим еще один подход к понятию предиката. Как отмечалось, предикат $P(x_1, x_2, \dots, x_n)$, определенный на множествах $M_1, M_2, \dots, M_n$, превращается в конкретное высказывание $P(a_1, a_2, \dots, a_n)$, если вместо предметных переменных $x_1, x_2, \dots, x_n$ подставить в него конкретные предметы (элементы $a_1, a_2, \dots, a_n$) из множеств $M_1, M_2, \dots, M_n$ соответственно. Это высказывание может быть либо истинным, либо ложным, т.е. его логическое значение равно 1 или 0. Следовательно, данный предикат определяет функцию n аргументов, заданную на множествах $M_1, M_2, \dots, M_n$ и принимающую значение в двухэлементном множестве $\{0, 1\}$. Иногда эту функцию и называют предикатом.

Классификация предикатов. Определение 18.2. Предикат $P(x_1, x_2, \dots, x_n)$, заданный на множествах $M_1, M_2, \dots, M_n$, называется:

а) *тождественно истинным*, если при любой подстановке вместо переменных $x_1, x_2, \dots, x_n$ любых конкретных предметов $a_1, a_2, \dots, a_n$ из множеств $M_1, M_2, \dots, M_n$ соответственно он превращается в истинное высказывание $P(a_1, a_2, \dots, a_n)$;

б) *тождественно ложным*, если при любой подстановке вместо переменных $x_1, x_2, \dots, x_n$ любых конкретных предметов из множеств $M_1, M_2, \dots, M_n$ соответственно он превращается в ложное высказывание;

в) *выполнимым (опровержимым)*, если существует по меньшей мере один набор конкретных предметов $a_1, a_2, \dots, a_n$ из множеств $M_1, M_2, \dots, M_n$ соответственно, при подстановке которых вместо соответствующих предметных переменных в предикат $P(x_1, x_2, \dots, x_n)$ последний превратится в истинное (ложное) высказывание $P(a_1, a_2, \dots, a_n)$.

Приведем п р и м е р ы. Одноместный предикат «Город x расположен на берегу реки Волги», определенный на множестве названий городов, является выполнимым, потому что существуют города, названия которых превращают данный предикат в истинное высказывание, или, иначе, удовлетворяют этому предикату (например, Ульяновск, Саратов и т.д.). Но данный предикат не будет тождественно истинным, потому что существуют города, названия которых превращают его в ложное высказывание, или, иначе, не удовлетворяют этому предикату (например, Прага, Якутск и т.д.). Этот же предикат являет собой пример опровержимого, но не тождественно ложного предиката (продумайте!).

В другом примере одноместный предикат « $\sin^2 x + \cos^2 x = 1$ », определенный на множестве действительных чисел, тождественно истинный. Наконец, двухместный предикат « $x^2 + y^2 < 0$ », заданный также на множестве действительных чисел, является тождественно ложным предикатом, потому что любая пара действительных чисел превращает его в ложное высказывание (не удовлетворяет ему).

Отметим некоторые достаточно очевидные закономерности взаимосвязей между предикатами различных типов (рекомендуется осмыслить их): 1) каждый тождественно истинный предикат является выполнимым, но обратное неверно; 2) каждый тождественно ложный предикат является опровержимым, но обратное неверно; 3) каждый не тождественно истинный предикат будет опровержимым, но, вообще говоря, не будет тождественно ложным; 4) каждый не тождественно ложный предикат будет выполнимым, но, вообще говоря, не будет тождественно истинным.

Множество истинности предиката. *Определение 18.3.* Множеством истинности предиката $P(x_1, x_2, \dots, x_n)$, заданного на множествах $M_1, M_2, \dots, M_n$, называется совокупность всех упорядоченных n -систем $(a_1, a_2, \dots, a_n)$, в которых $a_1 \in M_1, a_2 \in M_2, \dots, a_n \in M_n$, таких, что данный предикат обращается в истинное высказывание $P(a_1, a_2, \dots, a_n)$ при подстановке $x_1 = a_1, x_2 = a_2, \dots, x_n = a_n$. Это множество будем обозначать P^+ . Таким образом,

$$P^+ = \{(a_1, a_2, \dots, a_n) : \lambda(P(a_1, a_2, \dots, a_n)) = 1\}.$$

Множество P^+ истинности n -местного предиката $P(x_1, x_2, \dots, x_n)$ представляет собой n -арное отношение между элементами множеств $M_1, M_2, \dots, M_n$. Если предикат $P(x)$ — одноместный, заданный над множеством M , то его множество истинности P^+ является подмножеством множества M : $P^+ \subseteq M$.

Например, множеством истинности двухместного предиката «Точка x принадлежит прямой y », заданного на множестве E всех точек плоскости и на множестве F всех прямых этой плоскости, является бинарное отношение принадлежности (инцидентности) между точками и прямыми плоскости. Другой пример. Множество истинности двухместного предиката $S(x, y)$: « $x^2 + y^2 = 9$ », заданного на множестве R^2 , есть множество всех таких пар действительных чисел, которые являются координатами точек плоскости, образующими окружность с центром в начале координат и радиуса 3. Наконец, если $A(x)$: « $|a| > 2$ » — одноместный предикат над R , то $A^+ =] -\infty, -2 [\cup] 2, +\infty [$.

В терминах множества истинности легко выразить понятия, связанные с классификацией предикатов (определение 18.2). В самом деле, n -местный предикат $P(x_1, x_2, \dots, x_n)$, заданный на множествах $M_1, M_2, \dots, M_n$, будет:

а) тождественно истинным тогда и только тогда, когда $P^+ = M_1 \times M_2 \times \dots \times M_n$;

- б) тождественно ложным тогда и только тогда, когда $P^+ = \emptyset$;
 в) выполнимым тогда и только тогда, когда $P^+ \neq \emptyset$;
 г) опровержимым тогда и только тогда, когда $P^+ \neq M_1 \times M_2 \times \dots \times M_n$.

На языке множеств истинности еще более отчетливо проясняются закономерности взаимосвязей между предикатами различных типов, отмеченные в конце предыдущего пункта. Проанализируйте их еще раз.

Равносильность и следование предикатов. *Определение 18.4.* Два n -местных предиката $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$, заданных над одними и теми же множествами $M_1, M_2, \dots, M_n$, называются *равносильными*, если набор предметов (элементов) $a_1 \in M_1, a_2 \in M_2, \dots, a_n \in M_n$ превращает первый предикат в истинное высказывание $P(a_1, a_2, \dots, a_n)$ в том и только в том случае, когда этот набор предметов превращает второй предикат в истинное высказывание $Q(a_1, a_2, \dots, a_n)$.

Другими словами (на языке множеств истинности), предикаты $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$ равносильны тогда и только тогда, когда их множества истинности совпадают: $P^+ = Q^+$.

Утверждение о равносильности двух предикатов P и Q символически будем записывать так: $P \Leftrightarrow Q$. Отношение равносильности предикатов является отношением эквивалентности, так что совокупность всех n -местных предикатов, определенных на множествах $M_1, M_2, \dots, M_n$, распадается на непересекающиеся классы равносильных предикатов (все они определяют одну и ту же функцию, заданную на множествах $M_1, M_2, \dots, M_n$ и принимающую значения в двухэлементном множестве $\{0, 1\}$). Переход от предиката P_1 к равносильному ему предикату P_2 называется *равносильным преобразованием* первого. Это понятие очень важно для школьной математики, потому что изучаемые в ней уравнения и неравенства представляют собой частные виды предикатов. Решение уравнения и неравенства есть поиск их множеств истинности. При таком поиске мы продельваем над уравнением и неравенством различные преобразования, и здесь важно, чтобы эти преобразования были равносильными, т. е. чтобы найденное множество оказалось бы множеством истинности именно исходного уравнения или неравенства. Аналогична ситуация при решении систем уравнений или неравенств.

Рассмотрим простой пример. Пусть требуется решить уравнение (найти множество истинности предиката): $4x - 2 = -3x - 9$. Преобразуем его равносильным образом: $4x - 2 = -3x - 9 \Leftrightarrow 4x + 3x = -9 + 2 \Leftrightarrow x = -1$. Ответ: $\{-1\}$ — множество всех решений данного уравнения (множество истинности данного предиката).

Отметим следующее немаловажное обстоятельство: может быть так, что два предиката равносильны, если их рассматривать над одним множеством, и неравносильны, если их рассматривать над

другим (в частности, объемлющим первое) множеством. Такова, например, ситуация с предикатами: $\sqrt{x \cdot y} = 15$ и $\sqrt{x} \cdot \sqrt{y} = 15$ (см. № 9.22, 2 Задачника).

Определение 18.5. Предикат $Q(x_1, x_2, \dots, x_n)$, заданный над множествами $M_1, M_2, \dots, M_n$, называется *следствием* предиката $P(x_1, x_2, \dots, x_n)$, заданного над теми же множествами, если он превращается в истинное высказывание на всех тех наборах значений предметных переменных из соответствующих множеств, на которых в истинное высказывание превращается предикат $P(x_1, x_2, \dots, x_n)$.

Другими словами (в терминах множеств истинности), можно сказать, что предикат Q является следствием предиката P тогда и только тогда, когда $P^+ \subseteq Q^+$.

Утверждение о том, что предикат Q является следствием предиката P , будем символически записывать так: $P \Rightarrow Q$.

Например, одноместный предикат, определенный на множестве натуральных чисел, « n делится на 3» является следствием одноместного предиката, определенного на том же множестве, « n делится на 6». Из двух предикатов, упомянутых перед последним определением, первый будет следствием второго, если считать, что оба предиката заданы на множестве Z целых чисел.

Язык множеств истинности позволяет установить взаимосвязь между понятиями равносильности и следования предикатов: два предиката, определенные на одних и тех же множествах, равносильны тогда и только тогда, когда каждый из них является следствием другого. Кроме того, этот же язык дает возможность без труда установить следующие простые теоремы.

Теорема 18.6. *Каждые два тождественно истинных (тождественно ложных) предиката, заданных на одних и тех же множествах, равносильны. Обратно, всякий предикат, равносильный тождественно истинному (тождественно ложному) предикату, сам является тождественно истинным (тождественно ложным) предикатом.*

Теорема 18.7. *Каждый тождественно истинный n -местный предикат является следствием любого другого n -местного предиката, определенного на тех же множествах. Каждый n -местный предикат является следствием любого тождественно ложного n -местного предиката, определенного на тех же множествах.*

Теорема 18.8. *Пусть $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$ — два n -местных предиката, определенные на одних и тех же множествах, такие, что $Q(x_1, x_2, \dots, x_n)$ есть следствие $P(x_1, x_2, \dots, x_n)$. Тогда:*

- а) если $P(x_1, x_2, \dots, x_n)$ тождественно истинный (выполнимый), то и $Q(x_1, x_2, \dots, x_n)$ тождественно истинный (выполнимый);*
- б) если $Q(x_1, x_2, \dots, x_n)$ тождественно ложный (опровержимый), то и $P(x_1, x_2, \dots, x_n)$ тождественно ложный (опровержимый).*

Доказательство теоремы 18.8, а. Поскольку $P \Rightarrow Q$, поэтому $P^+ \subseteq Q^+$. Если теперь P тождественно истинный предикат, то $P^+ = M_1 \times M_2 \times \dots \times M_n$ (где $M_1, M_2, \dots, M_n$ — множества,

на которых определены n -местные предикаты P и Q). Но $Q^+ \subseteq M_1 \times M_2 \times \dots \times M_n$. Поэтому $Q^+ = M_1 \times M_2 \times \dots \times M_n$, а, значит, предикат Q — тождественно истинный предикат. Если же P — выполнимый предикат, то $P^+ \neq \emptyset$. Но $P^+ \subseteq Q^+$. Тогда $Q^+ \neq \emptyset$ и Q — выполнимый предикат.

б) Пусть Q — тождественно ложный предикат. Тогда $Q^+ = \emptyset$. Но $P^+ \subseteq Q^+$, поэтому $P^+ = \emptyset$. Следовательно, предикат P — тождественно ложный. Наконец, пусть Q — опровержимый предикат. Тогда $Q^+ \neq M_1 \times M_2 \times \dots \times M_n$. Поскольку, кроме того, $P^+ \subseteq Q^+$ и $P^+ \subseteq M_1 \times M_2 \times \dots \times M_n$, то $P^+ \neq M_1 \times M_2 \times \dots \times M_n$. Следовательно, предикат P — опровержимый. $\square$

Отыщите самостоятельно в настоящем и предыдущем пунктах данного параграфа утверждения, обосновывающие остальные сформулированные теоремы.

§ 19. Логические операции над предикатами

Над предикатами можно проделывать те же самые логические операции, что и над высказываниями: отрицание, конъюнкцию, дизъюнкцию, импликацию, эквивалентность. Рассмотрим эти операции в их связи с операциями над множествами (см. § 8).

Отрицание предиката. *Определение 19.1.* Отрицанием n -местного предиката $P(x_1, x_2, \dots, x_n)$, определенного на множествах $M_1, M_2, \dots, M_n$, называется новый n -местный предикат, определенный на тех же множествах, обозначаемый $\neg P(x_1, x_2, \dots, x_n)$ (читается: «неверно, что $P(x_1, x_2, \dots, x_n)$ »), который превращается в истинное высказывание при всех тех и только тех значениях предметных переменных, при которых исходное высказывание превращается в ложное высказывание.

Другими словами, предикат $\neg P(x_1, x_2, \dots, x_n)$ таков, что для любых предметов $a_1 \in M_1, a_2 \in M_2, \dots, a_n \in M_n$ высказывание $\neg P(a_1, a_2, \dots, a_n)$ является отрицанием высказывания $P(a_1, a_2, \dots, a_n)$.

Например, нетрудно понять, что отрицанием одноместного предиката « $x \leq 3$ », определенного на множестве R , является одноместный предикат « $x > 3$ », определенный на том же множестве R . Отрицанием предиката «Река x впадает в озеро Байкал» является предикат «Река x не впадает в озеро Байкал» (оба одноместных предиката определены на множестве названий рек). Отрицанием предиката « $\sin^2 x + \cos^2 x = 1$ » является предикат « $\sin^2 x + \cos^2 x \neq 1$ » ($x, y \in R$).

Теорема 19.2. Для n -местного предиката $P(x_1, x_2, \dots, x_n)$, определенного на множествах $M_1, M_2, \dots, M_n$, множество истинности его отрицания $\neg P(x_1, x_2, \dots, x_n)$ совпадает с дополнением множества истинности данного предиката: $(\neg P)^+ = \overline{P^+}$.

(Здесь следует понимать, что дополнение рассматривается в множестве $M_1 \times M_2 \times \dots \times M_n$, т.е. $(\neg P)^+ = (M_1 \times M_2 \times \dots \times M_n) \setminus P^+$.)

Доказательство. Согласно определениям 19.1, 18.3 и определению дополнения множества имеем

$$(\neg P)^+ = \{(a_1, a_2, \dots, a_n) : \lambda(P(a_1, a_2, \dots, a_n)) = 0\} = \\ = \{(a_1, a_2, \dots, a_n) : (a_1, a_2, \dots, a_n) \notin P^+\} = \overline{P^+} = (M_1 \times M_2 \times \dots \times M_n) \setminus P^+,$$

что и требовалось доказать. $\square$

Следствие 19.3. *Отрицание предиката будет тождественно истинным тогда и только тогда, когда исходный предикат тождественно ложен.*

Доказательство. В § 18 (пункт «Множество истинности предиката») тождественная истинность предиката выражена на языке множества истинности; она означает, что $(\neg P)^+ = M_1 \times M_2 \times \dots \times M_n$. Подставим в это равенство значение для $(\neg P)^+$ из настоящей теоремы:

$$(M_1 \times M_2 \times \dots \times M_n) \setminus P^+ = M_1 \times M_2 \times \dots \times M_n.$$

Вспоминая определение разности двух множеств (см. § 8) и учитывая, что $P^+ \subseteq M_1 \times M_2 \times \dots \times M_n$, заключаем, что $P^+ = \emptyset$. Значит, предикат $P(x_1, x_2, \dots, x_n)$ тождественно ложен. Следствие доказано. $\square$

Рассмотрим еще один п р и м е р. Требуется выяснить, является ли предикат $O(f) : \langle f \text{ — нечетная функция} \rangle$ отрицанием предиката $E(f) : \langle f \text{ — четная функция} \rangle$ (оба одноместных предиката определены на множестве всех действительных функций одного действительного аргумента). Множество истинности O^+ предиката $O(f)$ не является дополнением множества истинности E^+ предиката $E(f)$, потому что не всякая функция, не являющаяся четной, будет непременно нечетной. Другими словами, существуют функции, не являющиеся одновременно ни четными, ни нечетными (приведите пример!). Следовательно, предикат $O(f)$ не есть отрицание предиката $E(f)$.

Замечание 19.4. В алгебре высказываний существенным было не содержание высказывания, а лишь его значение истинности, т.е. отождествлялись (не различались) между собой, с одной стороны, все истинные высказывания, а с другой — все ложные. В некотором смысле аналогичная ситуация имеется и в алгебре предикатов: здесь не различают равносильные предикаты. Подходя с такой точки зрения к определению 19.1 отрицания предиката, можем за отрицание данного предиката $P(x_1, x_2, \dots, x_n)$ принять любой из равносильных предикатов, удовлетворяющих этому определению. Например, отрицанием предиката « $|x| > 2$ », заданного на R , является каждый из следующих (равносильных между собой) предикатов: « $|x| \leq 2$ », « $(x \geq -2) \vee (x \leq 2)$ », « $x \in [-2, 2]$ », а отрицанием предиката « $x^2 \geq 0$ », также определенного на R (этот предикат тождественно истинный), является каждый из следующих предикатов: « $\sin x = 2$ », « $x^2 < 0$ », « $e^x < 0$ », « $|x| < 0$ » и т.д.

Сделанное замечание следует иметь в виду при рассмотрении и остальных логических операций в настоящем параграфе.

Конъюнкция двух предикатов. Определение 19.5. Конъюнкцией n -местного предиката $P(x_1, x_2, \dots, x_n)$, определенного на множествах $M_1, M_2, \dots, M_n$, и m -местного предиката $Q(y_1, y_2, \dots, y_m)$, определенного на множествах $N_1, N_2, \dots, N_m$, называется новый $(n + m)$ -местный предикат, определенный на множествах $M_1, M_2, \dots, M_n, N_1, N_2, \dots, N_m$, обозначаемый $P(x_1, x_2, \dots, x_n) \wedge Q(y_1, y_2, \dots, y_m)$ (читается « $P(x_1, x_2, \dots, x_n)$ и $Q(y_1, y_2, \dots, y_m)$ »), который превращается в истинное высказывание при всех тех и только тех значениях предметных переменных, при которых оба исходных предиката превращаются в истинные высказывания.

Другими словами, предикат $P(x_1, x_2, \dots, x_n) \wedge Q(y_1, y_2, \dots, y_m)$ таков, что для любых предметов $a_1 \in M_1, a_2 \in M_2, \dots, a_n \in M_n$ и $b_1 \in N_1, b_2 \in N_2, \dots, b_m \in N_m$ высказывание $P(a_1, a_2, \dots, a_n) \wedge Q(b_1, b_2, \dots, b_m)$ является конъюнкцией высказываний $P(a_1, a_2, \dots, a_n)$ и $Q(b_1, b_2, \dots, b_m)$.

Например, конъюнкцией двух одноместных предикатов « $x > -3$ » и « $x < 3$ », определенных на R , будет одноместный предикат « $(x > -3) \wedge (x < 3)$ », записываемый короче в виде: « $-3 < x < 3$ », который равносильен предикату « $|x| < 3$ » (см. замечание 19.4). Другой пример. Конъюнкцией двух одноместных предикатов « $x = 0$ » и « $y = 0$ », заданных на R , является двухместный предикат « $(x = 0) \wedge (y = 0)$ », заданный на R^2 , который равносильен предикату « $x^2 + y^2 = 0$ », определенному также на R^2 .

Операцию конъюнкции можно применять к предикатам, имеющим общие переменные. В этом случае число переменных в новом предикате равно числу $n + m - k$, где n — число переменных первого предиката, m — число переменных второго предиката, k — число переменных общих для обоих предикатов. Именно таков первый из только что рассмотренных двух примеров. Более того, если оба предиката определены на одних и тех же множествах и зависят от одних и тех же переменных, то для них справедлива следующая теорема.

Теорема 19.6. Для n -местных предикатов $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$, определенных на множествах $M_1, M_2, \dots, M_n$, множество истинности конъюнкции $P(x_1, x_2, \dots, x_n) \wedge Q(x_1, x_2, \dots, x_n)$ совпадает с пересечением множеств истинности исходных предикатов:

$$(P \wedge Q)^+ = P^+ \cap Q^+.$$

Доказательство. Согласно определениям 19.5, 18.3 и определению пересечения множеств имеем

$$\begin{aligned} (P \wedge Q)^+ &= \{(a_1, a_2, \dots, a_n) : \lambda(P(a_1, a_2, \dots, a_n) \wedge \\ &\wedge Q(a_1, a_2, \dots, a_n)) = 1\} = \{(a_1, a_2, \dots, a_n) : \lambda(P(a_1, a_2, \dots, a_n) = 1 \text{ и } \\ &\lambda(Q(a_1, a_2, \dots, a_n)) = 1\} = \{(a_1, a_2, \dots, a_n) : \lambda(P(a_1, a_2, \dots, a_n) = 1\} \cap \\ &\cap \{(a_1, a_2, \dots, a_n) : \lambda(Q(a_1, a_2, \dots, a_n)) = 1\} = P^+ \cap Q^+. \end{aligned}$$

Следствие 19.7. Конъюнкция двух предикатов тождественно истинна тогда и только тогда, когда оба данных предиката тождественно истинны.

Доказательство. Согласно § 18 (пункт «Множество истинности предиката») тождественная истинность предиката $P \wedge Q$ означает, что $(P \wedge Q)^+ = M_1 \times M_2 \times \dots \times M_n$. Тогда на основании теоремы $P^+ \cap Q^+ = M_1 \times M_2 \times \dots \times M_n$, т.е. пересечение двух подмножеств P^+ и Q^+ множества $M_1 \times M_2 \times \dots \times M_n$ совпадает с самим этим множеством. Следовательно, $P^+ = Q^+ = M_1 \times M_2 \times \dots \times M_n$, а это означает, что предикаты P и Q тождественно истинны. $\square$

Значительный раздел школьной математики составляют системы уравнений и неравенств. При их решении используется теорема 19.6. Пусть, например, требуется решить систему неравенств $|x| < 3$, $x \geq 2$. Для этого нужно найти множество истинности предиката « $(|x| < 3) \wedge (x \geq 2)$ », определенного на R . Используем теорему 19.6:

$$(|x| < 3) \wedge (x \geq 2)^+ = (|x| < 3)^+ \cap (x \geq 2)^+ =]-3, 3[\cap [2, +\infty[= [2, 3[.$$

Таким образом, решением данной системы является множество (полуинтервал) $[2, 3[$.

Следует отметить, что в предикаты $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$, о которых идет речь в теореме 19.6, некоторые предметные переменные могут в действительности не входить, т.е., как говорят, быть фиктивными. Это нужно понимать так, что значение истинности высказывания, в которое превращается данный предикат, не зависит от того, какие предметы подставляются вместо таких (фиктивных) переменных. При решении систем уравнений и неравенств данная ситуация встречается часто. Так, например, решения системы уравнений $x + y = 1$, $y + z = 2$, $z + x = 3$ образуют множество, состоящее из одной упорядоченной тройки чисел $(1, 0, 2)$, хотя первое уравнение не зависит от z , второе — от x , а третье — от y .

Дизъюнкция двух предикатов. Определение 19.8. Дизъюнкцией n -местного предиката $P(x_1, x_2, \dots, x_n)$, определенного на множествах $M_1, M_2, \dots, M_n$, и m -местного предиката $Q(y_1, y_2, \dots, y_m)$, определенного на множествах $N_1, N_2, \dots, N_m$, называется новый $(n + m)$ -местный предикат, определенный на множествах $M_1, M_2, \dots, M_n, N_1, N_2, \dots, N_m$, обозначаемый $P(x_1, x_2, \dots, x_n) \vee Q(y_1, y_2, \dots, y_m)$ (читается « $P(x_1, x_2, \dots, x_n)$ или $Q(y_1, y_2, \dots, y_m)$ »), который превращается в истинное высказывание при всех тех и только тех значениях предметных переменных, при которых в истинное высказывание превращается по меньшей мере один из исходных предикатов.

Другими словами, предикат $P(x_1, x_2, \dots, x_n) \vee Q(y_1, y_2, \dots, y_m)$ таков, что для любых предметов $a_1 \in M_1, a_2 \in M_2, \dots, a_n \in M_n$ и $b_1 \in N_1, b_2 \in N_2, \dots, b_m \in N_m$ высказывание $P(a_1, a_2, \dots, a_n) \vee Q(b_1, b_2, \dots, b_m)$

$b_2, \dots, b_m)$ является дизъюнкцией высказываний $P(a_1, a_2, \dots, a_n)$ и $Q(b_1, b_2, \dots, b_m)$.

Операцию дизъюнкции, как и операцию конъюнкции (см. абзац перед теоремой 19.6), можно применять, в частности к предикатам, имеющим общие переменные. Например, дизъюнкцией двух одноместных предикатов « x — четное число» и « x — простое число», определенных на N , является одноместный предикат, определенный на N : « x — четное или простое число».

Дизъюнкцией одноместных предикатов « $x \neq 0$ » и « $y \neq 0$ », определенных на R , является двухместный предикат « $(x \neq 0) \vee (y \neq 0)$ », определенный на R^2 , который равносильен предикату « $x^2 + y^2 \neq 0$ » над R^2 .

Следующая теорема аналогична теореме 19.6.

Теорема 19.9. Для n -местных предикатов $P(x_1, x_2, \dots, x_n)$ и $Q(x_1, x_2, \dots, x_n)$, определенных на множествах $M_1, M_2, \dots, M_n$, множество истинности дизъюнкции $P(x_1, x_2, \dots, x_n) \vee Q(x_1, x_2, \dots, x_n)$ совпадает с объединением множеств истинности исходных предикатов:

$$(P \vee Q)^+ = P^+ \cup Q^+.$$

Доказательство аналогично доказательству теоремы 19.6, поэтому предлагаем провести его самостоятельно. $\square$

Следствие 19.10. Дизъюнкция двух предикатов есть выполнимый предикат тогда и только тогда, когда по меньшей мере один из данных предикатов выполнен.

Доказательство. Согласно § 18 (пункт «Множество истинности предиката») выполнимость предиката $P \vee Q$ означает, что $(P \vee Q)^+ \neq \emptyset$. Отсюда на основании теоремы 19.9 $P^+ \cup Q^+ \neq \emptyset$. Последнее возможно в том и только в том случае, если $P^+ \neq \emptyset$ или $Q^+ \neq \emptyset$, т.е. если выполним предикат P или выполним предикат Q . $\square$

Следствие 19.11. Дизъюнкция двух предикатов тождественно ложна тогда и только тогда, когда оба данных предиката тождественно ложны.

Доказательство предлагается провести самостоятельно.

Например, пусть требуется решить уравнение $x^2 - x - 6 = 0$, т.е. найти множество истинности этого предиката, определенного на R . Находим его, применяя теорему 19.9. Тогда

$$\{x : x^2 - x - 6 = 0\} = \{x : (x + 2)(x - 3) = 0\} = \{x : (x + 2 = 0) \vee (x - 3 = 0)\} = \{x : x + 2 = 0\} \cup \{x : x - 3 = 0\} = \{-2\} \cup \{3\} = \{-2, 3\}.$$

В другом примере дизъюнкция $(x^2 + y^2 < 0) \vee (xy = 0)$ двух двухместных предикатов, определенных на R^2 , есть выполнимый предикат, потому что выполним один из них: $xy = 0$ (проверьте).

Свойства отрицания, конъюнкции и дизъюнкции. После введения трех операций над предикатами возникают вопросы: как они влияют на равносильность предикатов и каковы закономерности

образования с помощью этих операций равносильных предикатов? Аналогичны вопросы для следования предикатов. Ответ дает следующая теорема.

Теорема 19.12. *Если во всех формулах теоремы 3.2 под P , Q , R понимать предикаты, определенные на соответствующих множествах, знак $\Leftrightarrow$ всюду заменить знаком $\Leftrightarrow$, а знак $\rightarrow$ — знаком $\Rightarrow$, то получим верные утверждения о предикатах.*

Доказательство. Рассмотрим, например, вторую из формул δ) теоремы 3.2. Она превращается в следующее утверждение: $(P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$, означающее равносильность предикатов $P \vee (Q \wedge R)$ и $(P \vee Q) \wedge (P \vee R)$ независимо от предикатов P , Q , R . Проверим, верно ли данное утверждение. В самом деле, каждый из двух предикатов при любой подстановке вместо предметных переменных конкретных предметов из соответствующих множеств превращается в такое высказывание, которое на основании тавтологии из теоремы 3.2, δ имеет одинаковые значения истинности. На основании определения равносильности предикатов это и означает, что данные предикаты равносильны. $\square$

Импликация и эквивалентность двух предикатов. Импликация $P(x_1, x_2, \dots, x_n) \rightarrow Q(y_1, y_2, \dots, y_m)$ определяется как такой предикат, что для любых предметов $a_1 \in M_1, a_2 \in M_2, \dots, a_n \in M_n$ и $b_1 \in N_1, b_2 \in N_2, \dots, b_m \in N_m$ высказывание $P(a_1, a_2, \dots, a_n) \rightarrow Q(b_1, b_2, \dots, b_m)$ является импликацией высказываний $P(a_1, a_2, \dots, a_n)$ и $Q(b_1, b_2, \dots, b_m)$. Аналогично определяется эквивалентность двух предикатов. Нетрудно проверить, что импликация двух предикатов, зависящих от одних и тех же переменных, есть тождественно истинный предикат тогда и только тогда, когда ее заключение является следствием посылки, а эквивалентность тождественно истинна, если и только если исходные предикаты равносильны. Свойства этих операций над предикатами, подобно свойствам операций отрицания, конъюнкции и дизъюнкции над предикатами (см. теорему 19.12), получаются из соответствующих тавтологий теоремы 3.3. Так, если P , Q , R — предикаты, то, например,

$$a) (P \rightarrow (Q \rightarrow R)) \Rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R));$$

$$\delta) (\neg Q \wedge (P \rightarrow Q)) \Rightarrow \neg P;$$

$$n) (P \leftrightarrow Q) \Leftrightarrow (Q \leftrightarrow P)$$

и т.д. Аналогично, из тавтологий теоремы 3.4 получаются равносильности, выражающие одни логические операции над предикатами через другие. Например,

$$a) (P \rightarrow Q) \Leftrightarrow (\neg P \vee Q);$$

$$в) (P \wedge Q) \Leftrightarrow \neg(\neg P \wedge \neg Q);$$

$$ж) (P \leftrightarrow Q) \Leftrightarrow ((P \rightarrow Q) \wedge (Q \rightarrow P))$$

и так далее для любых предикатов P , Q , R .

§ 20. Кванторные операции над предикатами

Рассмотренные в предыдущем параграфе операции над предикатами в определенном смысле аналогичны соответствующим операциям над высказываниями. Специфика природы предикатов позволяет ввести такие операции над ними, которые не имеют аналогов среди операций над высказываниями. Имеются в виду две кванторные операции над предикатами (или операции квантификации) — квантор общности и квантор существования, о которых и пойдет речь в настоящем параграфе.

Квантор общности. Известно, что для превращения одноместного предиката в высказывание нужно подставить вместо его переменной какой-нибудь конкретный предмет из области задания предиката. Имеется еще один способ для такого превращения — это применение к предикату операций связывания квантором общности или квантором существования. Каждая из этих операций ставит в соответствие одноместному предикату некоторое высказывание, истинное или ложное в зависимости от исходного предиката.

Определение 20.1. Операцией связывания квантором общности называется правило, по которому каждому одноместному предикату $P(x)$, определенному на множестве M , сопоставляется высказывание, обозначаемое $(\forall x)(P(x))$ (читается: «для всякого [значения] x $P(x)$ [истинное высказывание]»), которое истинно в том и только в том случае, когда предикат $P(x)$ тождественно истинен, и ложно в противном случае,

$$\lambda[(\forall x)(P(x))] = \begin{cases} 1, & \text{если } P(x) \text{ — тождественно истинный предикат,} \\ 0, & \text{если } P(x) \text{ — опровержимый предикат.} \end{cases}$$

При чтении высказывания $(\forall x)(P(x))$ слова в квадратных скобках могут опускаться. Высказывание $(\forall x)(P(x))$ называется *универсальным высказыванием* для предиката $P(x)$. Символ $\forall$ происходит от первой буквы англ. *all* — «все». Сам символ $(\forall x)$ также называют квантором общности по переменной x .

Например, рассмотрим два одноместных предиката на множестве N : « $1 \leq x$ » и « $x|30$ ». Первый предикат тождественно истинный, поэтому применение к нему операции связывания квантором общности дает истинное высказывание: $(\forall x)(1 \leq x)$ — «для всякого x число 1 не превосходит x ». Второй предикат опровержим, поэтому операция связывания квантором общности, примененная к нему, дает ложное высказывание: $(\forall x)(x|30)$ — «для любого x число x является делителем числа 30».

В выражении $(\forall x)(P(x))$ переменная x уже перестает быть переменной в обычном смысле этого слова, т. е. вместо нее невозможно подставлять какие бы то ни было конкретные значения. Считают,

что переменная x *связанная*, кажущаяся или немая. Такая ситуация уже встречалась в математике: переменные могут быть связаны не только квантором. Так, связанными являются переменные в следующих выражениях:

$$\int_0^2 x dx, \lim_{n \rightarrow \infty} \frac{1}{n}, \{x : x \geq 0\}.$$

Это означает, что каждое из приведенных выражений не зависит от связанных переменных, т.е. сущность выражения не изменится, если связанную переменную обозначить любой другой буквой. Так, первое из трех выражений вне зависимости от переменной равно 2, второе равно 0, а третье — действительная полупрямая $[0; +\infty[$. Аналогично, высказывание $(\forall x)(1 \leq x)$ может быть прочитано так: «1 не превосходит всякое натуральное число» — и в таком виде оно вообще не содержит переменных.

Если одноместный предикат $P(x)$ задан на конечном множестве $M = \{a_1, a_2, \dots, a_m\}$, то нетрудно понять, что высказывание $(\forall x)(P(x))$ эквивалентно (имеет то же логическое значение) конъюнкции $P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n)$. В самом деле, по определению 20.1 истинность высказывания $(\forall x)(P(x))$ означает, что предикат тождественно истинен, т.е. каждое из высказываний $P(a_1), P(a_2), \dots, P(a_n)$, в которые этот предикат превращается, истинно. Последнее равносильно истинности конъюнкции $P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n)$.

Следовательно, для предикатов, заданных на конечном множестве, операция связывания квантором общности может быть выражена через конъюнкцию. Для предикатов, заданных на бесконечном множестве, такого сделать нельзя, и в этом случае операция связывания квантором общности является существенно новой.

Можно подметить еще одну особенность операции связывания квантором общности по сравнению с операциями из предыдущего параграфа. Те операции ставили в соответствие одному или двум предикатам новый предикат, а операция связывания квантором общности сопоставляет предикату высказывание. На это можно сказать следующее. Во-первых, каждое высказывание для достижения большей общности сейчас и в дальнейшем можно рассматривать как предикат, содержащий 0 предметных переменных, т.е. как нульместный предикат. Во-вторых, мы пока применяли квантор общности лишь к одноместным предикатам. Переходим к рассмотрению вопроса о применении операции связывания квантором общности к предикатам с любым числом предметных переменных; такая операция предстанет операцией в полном смысле слова: предикатам она будет сопоставлять предикаты.

Определение 20.2. Операцией связывания квантором общности по переменной x_1 называется правило, по которому каждому n -местному ($n \geq 2$) предикату $P(x_1, x_2, \dots, x_n)$, определенному на множествах $M_1, M_2, \dots, M_n$, ставится в соответствие новый $(n-1)$ -местный предикат, обозначаемый $(\forall x_1)(P(x_1, x_2, \dots, x_n))$ (читается: «для всех x_1 $P(x_1, x_2, \dots, x_n)$ »), который для любых предметов $a_2 \in M_2, \dots, a_n \in M_n$ превращается в высказывание $(\forall x_1)(P(x_1, a_2, \dots, a_n))$, истинное в том и только в том случае, когда одноместный предикат $P(x_1, a_2, \dots, a_n)$, определенный на множестве M_1 , тождественно истинен, и ложное в противном случае. Другими словами:

$$\lambda[(\forall x_1)(P(x_1, a_2, \dots, a_n))] = \begin{cases} 1, & \text{если } P(x_1, a_2, \dots, a_n) \text{ — тождественно} \\ & \text{истинный предикат от } x_1, \\ 0, & \text{если } P(x_1, a_2, \dots, a_n) \text{ — опровержимый} \\ & \text{предикат от } x_1. \end{cases}$$

Например, рассмотрим двухместный предикат « $y \leq x$ », определенный на множестве N^2 . Применим к нему квантор общности по переменной x . Получим одноместный предикат $(\forall x)(y \leq x)$, зависящий от переменной y . Этот предикат может превратиться как в истинное высказывание (при $y = 1$), так и в ложное (при подстановке вместо y любых натуральных чисел, кроме 1).

В другом примере двухместный предикат « $(x+y)^2 = x^2 + 2xy + y^2$ », определенный на R^2 , тождественно истинен. Поэтому применение к нему квантора общности по любой переменной, например по y , дает одноместный предикат (по x), который будет тождественно истинным $(\forall y)((x+y)^2 = x^2 + 2xy + y^2)$.

Заметим в заключение, что к $(n-1)$ -местному предикату $(\forall x_1)(P(x_1, x_2, \dots, x_n))$, зависящему от переменных $x_2, \dots, x_n$, можно снова применить операцию связывания квантором общности по одной из свободных переменных. В результате получится $(n-2)$ -местный предикат и т. д.

Например, применив к одноместному предикату $(\forall x)(y \leq x)$, где $x, y \in R$, квантор общности по переменной y , получим нульместный предикат, т. е. высказывание $(\forall y)(\forall x)(y \leq x)$. Ясно, что полученное высказывание ложно, потому что предикат $(\forall x)(y \leq x)$ опровержим. Применив квантор общности по переменной x к одноместному предикату из второго примера, получим истинное высказывание $(\forall x)(\forall y)((x+y)^2 = x^2 + 2xy + y^2)$.

Квантор существования. Как и в предыдущем пункте, начнем рассмотрение с операции связывания квантором существования, применяемой к одноместному предикату.

Определение 20.3. Операцией связывания квантором существования называется правило, по которому каждому одноместному предикату $P(x)$, определенному на множестве M , ставится в соответствие высказывание, обозначаемое $(\exists x)(P(x))$ (читается: «существует

[значение] x , такое, что $P(x)$ [истинное высказывание]»), которое ложно в том и только в том случае, когда $P(x)$ тождественно ложен, и истинно в противном случае, т.е.

$$\lambda[(\exists x)(P(x))] = \begin{cases} 0, & \text{если } P(x) \text{ — тождественно ложный предикат,} \\ 1, & \text{если } P(x) \text{ — выполнимый предикат.} \end{cases}$$

При чтении высказывания $(\exists x)(P(x))$ слова в квадратных скобках могут опускаться. Высказывание $(\exists x)(P(x))$ называется *экзистенциальным высказыванием* для предиката $P(x)$. Символ $\exists$ происходит от первой буквы англ. *exist* — «существовать». Сам символ $\exists x$ также называют *квантором существования по переменной x* .

Например, рассмотрим два одноместных предиката, определенных на множестве N : « $x = x + 1$ » и « $x|30$ ». Первый предикат тождественно ложный, поэтому применение к нему операции связывания квантором существования дает ложное высказывание: $(\exists x)(x = x + 1)$ — «существует натуральное число, равное себе плюс 1». Второй предикат выполним, поэтому операция связывания квантором существования, примененная к нему, дает истинное высказывание: $(\exists x)(x|30)$ — «существует натуральное число, делящее число 30».

Подобно выражению $(\forall x)(P(x))$, в выражении $(\exists x)(P(x))$ переменная x также перестает быть переменной в обычном смысле слова: это — *связанная переменная*.

Если одноместный предикат $P(x)$ задан на конечном множестве $M = \{a_1, a_2, \dots, a_m\}$, то высказывание $(\exists x)(P(x))$ эквивалентно (имеет то же логическое значение) дизъюнкции $P(a_1) \vee P(a_2) \vee \dots \vee P(a_m)$. В самом деле, по определению 20.3 ложность высказывания $(\exists x)(P(x))$ означает, что предикат $P(x)$ тождественно ложен, т.е. каждое из высказываний $P(a_1), P(a_2), \dots, P(a_m)$, в которые данный предикат может превратиться, ложно. Последнее равносильно ложности дизъюнкции $P(a_1) \vee P(a_2) \vee \dots \vee P(a_m)$.

Значит, для предикатов, заданных на конечном множестве, операция связывания квантором существования может быть выражена через дизъюнкцию. Для предикатов, заданных на бесконечном множестве, такого сделать нельзя, и в этом случае операция связывания квантором существования является существенно новой.

Наконец рассмотрим вопрос о применении операции связывания квантором существования к предикатам с любым числом предметных переменных.

Определение 20.4. Операцией *связывания квантором существования по переменной x_1* называется правило, по которому каждому n -местному ($n \geq 2$) предикату $P(x_1, x_2, \dots, x_n)$, определенному на множествах $M_1, M_2, \dots, M_n$, ставится в соответствие новый $(n-1)$ -местный предикат, обозначаемый $(\exists x_1)(P(x_1, x_2, \dots, x_n))$ (чи-

тается: «существует такой x_1 , что $P(x_1, x_2, \dots, x_n)$, который для любых предметов $a_2 \in M_2, \dots, a_n \in M_n$ превращается в высказывание $(\exists x_1)(P(x_1, a_2, \dots, a_n))$, ложное в том и только в том случае, когда одноместный предикат $P(x_1, a_2, \dots, a_n)$, определенный на множестве M_1 , тождественно ложен, и истинное в противном случае, т.е.

$$\lambda[(\exists x_1)(P(x_1, a_2, \dots, a_n))] = \begin{cases} 0, & \text{если } P(x_1, a_2, \dots, a_n) \text{ — тождественно} \\ & \text{ложный предикат от } x_1, \\ 1, & \text{если } P(x_1, a_2, \dots, a_n) \text{ — выполнимый} \\ & \text{предикат от } x_1. \end{cases}$$

Например, рассмотрим двухместный предикат « $y \leq x$ », определенный на R^2 . Применим к нему квантор существования по переменной x . Получим одноместный предикат $(\exists x)(y \leq x)$, зависящий от переменной y . Этот предикат всегда превращается в истинное высказывание, если вместо y подставлять конкретные числа, т.е. он является тождественно истинным предикатом.

В другом примере двухместный предикат « $x^2 + y^2 < 0$ », определенный на R^2 , тождественно ложен. Поэтому применение к нему квантора существования по любой переменной, например по x , дает одноместный (по y) предикат, который будет тождественно ложным: $(\exists x)(x^2 + y^2 < 0)$.

Заметим в заключение, что к $(n-1)$ -местному предикату $(\exists x_1)(P(x_1, x_2, \dots, x_n))$, зависящему от переменных $x_2, \dots, x_n$, можно снова применить одну из операций квантификации — квантор общности или квантор существования по одной из свободных переменных. В результате получим $(n-2)$ -местные предикаты, например $(\forall x_2)(\exists x_1)(P(x_1, x_2, \dots, x_n))$ и $(\exists x_2)(\exists x_1)(P(x_1, x_2, \dots, x_n))$.

Так, применив к тождественно истинному одноместному предикату $(\exists x)(y \leq x)$, заданному на N , квантор общности, получим истинное высказывание: $(\forall y)(\exists x)(y \leq x)$ — «Для всякого натурального числа существует большее него натуральное число». Применив к тому же одноместному предикату квантор существования, получим также истинное высказывание: $(\exists y)(\exists x)(y \leq x)$ — «Существуют два натуральных числа, из которых одно не превосходит другое». Далее, применив к выполнимому одноместному предикату $(\forall x)(y \leq x)$, заданному на N , квантор существования, получим истинное высказывание $(\exists y)(\forall x)(y \leq x)$ — «Существует наименьшее натуральное число». Наконец, применив квантор существования к одноместному тождественно ложному предикату $(\exists x)(x^2 + y^2 < 0)$, получим ложное высказывание: $(\exists y)(\exists x)(x^2 + y^2 < 0)$.

Численные кванторы. В математике часто встречаются выражения вида «по меньшей мере n » («хотя бы n »), «не более чем n », « n и только n » («ровно n », «точно n »), где n — натуральное число. Эти выражения называют численными кванторами. Они имеют

чисто логический смысл, потому что их можно выразить без числительных на языке кванторов общности и существования, без логических операций над предикатами и знака $=$, обозначающего тождество (совпадение) объектов. Рассмотрим ряд случаев.

1) $n = 1$. Предложение «По меньшей мере один объект обладает свойством P » имеет тот же смысл, что и предложение «Существует объект, обладающий свойством P », т.е.

$$(\exists x)(P(x)). \quad (1)$$

Далее, предложение «Не более чем один объект обладает свойством P » равнозначно по смыслу предложению «Если есть объекты, обладающие свойством P , то они совпадают», т.е.

$$(\forall x)(\forall y)[(P(x) \wedge P(y)) \rightarrow x = y]. \quad (2)$$

Наконец, предложение «Один и только один объект обладает свойством P » равнозначно конъюнкции высказываний (1) и (2):

$$(\exists x)(P(x)) \wedge (\forall x)(\forall y)[(P(x) \wedge P(y)) \rightarrow x = y]. \quad (3)$$

Сопоставление одноместному предикату $P(x)$ высказывания (3) носит название операции связывания *квантором существования и единственности*, а само высказывание (3) иногда обозначают так:

$$(\exists! x)(P(x)). \quad (4)$$

Символ $\exists! x$ называют *квантором существования и единственности* по переменной x .

Например, используя этот квантор, запишем высказывание: «Всякая сходящаяся последовательность имеет точно один предел»:

$$(\forall \{a_n\})((\exists a)(a = \lim a_n) \rightarrow (\exists! a)(a = \lim a_n)).$$

2) $n = 2$. Предложение «По меньшей мере два объекта обладают свойством P » означает то же, что и предложение «Существуют два различных объекта, обладающих свойством P », т.е.

$$(\exists x)(\exists y)(P(x) \wedge P(y) \wedge x \neq y). \quad (5)$$

Далее, предложение «Не более чем два объекта обладают свойством P » равнозначно по смыслу предложению «Каковы бы ни были объекты x, y, z , если все они обладают свойством P , то по меньшей мере два из них совпадают», которое символически записывается так:

$$(\forall x)(\forall y)(\forall z)[(P(x) \wedge P(y) \wedge P(z)) \rightarrow (x = y \vee x = z \vee y = z)]. \quad (6)$$

Наконец, предложение «Два и только два объекта обладают свойством P » совпадает по смыслу с конъюнкцией высказываний (5) и (6).

Совершенно аналогично выражаются через обычные кванторы и логические операции численные кванторы при $n > 2$. Рекомендуется самостоятельно записать соответствующие выражения для $n = 3$.

Ограниченные кванторы. Нередки в математической практике обороты следующего вида: «Всякий объект, обладающий свойством P , обладает также и свойством Q » и «Среди объектов, обладающих свойством P , существует объект, обладающий также и свойством Q ». Первое высказывание равнозначно по смыслу высказыванию «Всякий объект, если он обладает свойством P , то он обладает и свойством Q », которое на языке логики предикатов записывается так:

$$(\forall x)(P(x) \rightarrow Q(x)). \quad (7)$$

Сопоставление двум данным одноместным предикатам $P(x)$ и $Q(x)$ высказывания (7) носит название операции связывания *ограниченным квантором общности*, а само высказывание (7) иногда обозначают

$$(\forall P(x))(Q(x)). \quad (8)$$

Символ $\forall P(x)$ также называют ограниченным квантором общности.

Например, высказывание «Для всякого $x > 1$ справедливо $\ln x > 0$ » на языке логики предикатов записывается как $(\forall x)(x > 1 \rightarrow \ln x > 0)$, а с использованием ограниченного квантора общности записывается в виде $(\forall x > 1)(\ln x > 0)$.

Второе из приведенных в начале настоящего пункта высказываний равнозначно по смыслу высказыванию «Существует объект, обладающий свойством P и обладающий свойством Q », которое на языке логики предикатов записывается так:

$$(\exists x)(P(x) \wedge Q(x)). \quad (9)$$

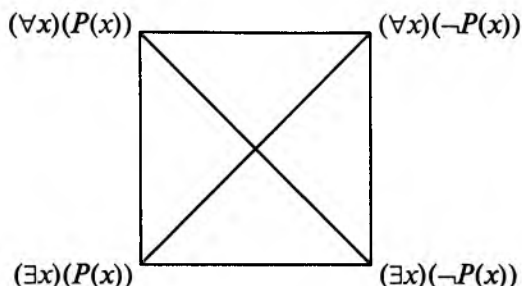
Сопоставление двум данным одноместным предикатам $P(x)$ и $Q(x)$ высказывания (9) носит название операции связывания *ограниченным квантором существования*, а само высказывание (9) иногда обозначается

$$(\exists P(x))(Q(x)). \quad (10)$$

Символ $\exists P(x)$ также называют ограниченным квантором существования.

Например, (ложное) высказывание «Существует действительное число, квадрат которого равен -1 » на языке логики предикатов запишется так: $(\exists x)(x \in R \wedge x^2 = -1)$, или с использованием ограниченного квантора существования запишется в виде $(\exists x \in R)(x^2 = -1)$.

Логический квадрат. Кванторные операции (или операции квантификации) над предикатами — важнейший принципиальный шаг, отличающий теорию предикатов от теории высказываний. Систему взаимоотношений между универсальными и экзистенциальными высказываниями, возникающими при определении операций взятия квантора общности и квантора существования, схематично представляют в виде следующего так называемого «логического квадрата»:



Универсальные высказывания $(\forall x)(P(x))$ и $(\forall x)(\neg P(x))$, стоящие в двух верхних вершинах квадрата, не могут быть (ни для какого предиката $P(x)$) одновременно истинными (хотя конечно же могут быть одновременно ложными). Говорят, что эти высказывания являются *противными* или *контрарными*. Экзистенциальные высказывания $(\exists x)(P(x))$ и $(\exists x)(\neg P(x))$, стоящие в двух нижних вершинах квадрата, наоборот, не могут быть (ни для какого предиката $P(x)$) одновременно ложными (хотя конечно же могут быть одновременно истинными). Говорят, что эти высказывания *субпротивны* (или *субконтрарны*). Высказывания, стоящие в вершинах каждой диагонали квадрата, противоречат одно другому, т.е. одно является отрицанием другого. Наконец, под каждым из универсальных высказываний, стоящих у верхних вершин, стоит высказывание у нижней вершины, следующее из него, т.е. такое, что импликация этих высказываний (для любого предиката $P(x)$) является истинным высказыванием.

В заключение отметим, что кванторы в явном виде впервые были введены немецким математиком Готтлобом Фреге в работе «Begriffsschrift» («Исчисление понятий», 1879). В 1885 г. английский логик Чарльз Пирс ввел термины «квантор», «квантификация», происшедшие соответственно от лат. *quantum* — «сколько» и лат. *quantum + facio* — «делать». Это означает, что квантор показывает, о скольких (всех или некоторых) объектах говорится в том или ином предложении. Символику для кванторов в виде перевернутых латинских букв ввел итальянский математик Дж. Пеано в 90-е гг. XIX в. После использования кванторов математиками Пеано, Шрёдером, Расселом они стали широко использоваться.

§ 21. Формулы логики предикатов

В алгебре высказываний мы подробно изучили (§ 2—6) одно из важнейших ее понятий и инструментов — понятие формулы алгебры высказываний. Теперь наша задача состоит в том, чтобы определить и изучить соответствующее понятие в логике предикатов, а затем на его основе продемонстрировать, насколько тоньше и точнее язык и логика предикатов отражают процессы человеческого мышления, нежели это делают язык и логика высказываний.

Понятие формулы логики предикатов. Это понятие вводится аналогично понятию формулы алгебры высказываний. Сначала задается *алфавит* символов, из которых будут составляться формулы:

предметные переменные: x, y, z, x_i, y_i, z_i ($i \in N$);

нульместные предикатные переменные: P, Q, R, P_i, Q_i, R_i ($i \in N$);

n -местные ($n \geq 1$) предикатные переменные: $P(, \dots,), Q(, \dots,), R(, \dots,), P_i(, \dots,), Q_i(, \dots,), R_i(, \dots,)$ ($i \in N$) с указанием числа свободных мест в них;

символы логических операций: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$;

кванторы: $\forall, \exists$;

вспомогательные символы: $(,)$ — скобки; $,$ — запятая.

Теперь дадим определение формулы логики предикатов, которое также носит индуктивный характер.

Определение 21.1 (формулы логики предикатов). 1) Каждая нульместная предикатная переменная есть *формула*;

2) если $P(, \dots,)$ — n -местная предикатная переменная, то $P(x_1, \dots, x_n)$ есть *формула*, в которой все предметные переменные $x_1, \dots, x_n$ свободны;

3) если F — формула, то $\neg F$ — также *формула*. Свободные (связанные) предметные переменные в формуле $\neg F$ те и только те, которые являются свободными (связанными) в F ;

4) если F_1, F_2 — формулы и если предметные переменные, входящие одновременно в обе эти формулы, свободны в каждой из них, то выражения $(F_1 \wedge F_2), (F_1 \vee F_2), (F_1 \rightarrow F_2), (F_1 \leftrightarrow F_2)$ также являются *формулами*. При этом предметные переменные, свободные (связанные) хотя бы в одной из формул F_1, F_2 , называются *свободными (связанными)* и в новых формулах;

5) если F — формула и x — предметная переменная, входящая в F свободно, то выражения $(\forall x)(F)$ и $(\exists x)(F)$ также являются *формулами*, в которых переменная x связанная, а все остальные предметные переменные, входящие в формулу F свободно или связано, остаются и в новых формулах соответственно такими же;

6) никаких других формул логики предикатов, кроме получающихся согласно пп. 1—5, нет.

Формулы, определенные в п. 1 и п. 2, называются *элементарными* (или *атомарными*). Формулы, не являющиеся элементарными, называются *составными*.

Например, P , $Q(x, y, z)$, $R(x_1, x_2)$ — элементарные формулы, а $(\exists y)(P(x, y, z))$, $(\forall x)(\exists y)(P(x, y, z))$, $((\forall x)(P(x)) \wedge Q) \rightarrow \neg(\exists y)(R(x, y))$ — составные формулы. При этом в первой составной формуле предметная переменная y связана, а переменные x, z — свободные. Во второй составной формуле свободна лишь переменная z , остальные — связаны. В третьей составной формуле первое вхождение переменной x связано, а второе — свободно. Переменная y связана. Последнюю формулу более целесообразно было бы записать в следующем виде (заменяя связанную переменную x какой-нибудь буквой, не входящей в данную формулу): $((\forall z)(P(z)) \wedge Q) \rightarrow \neg(\exists y)(R(x, y))$.

Как и в алгебре высказываний, договоримся внешние скобки у формулы не писать, если только она не является частью более сложной формулы. Отметим кстати, что на основании пунктов 1, 3 и 4 сформулированного определения всякая формула алгебры высказываний будет также и формулой логики предикатов.

В формулах вида $(\forall \xi)(F)$ и $(\exists \xi)(F)$ формула F называется *областью действия квантора* $\forall \xi$ или $\exists \xi$ соответственно. Тогда ясно, что вхождение предметной переменной в формулу будет связанным, если эта переменная находится в области действия квантора по этой переменной.

Формулы, в которых нет свободных предметных переменных, называются *замкнутыми*, а формулы, содержащие свободные предметные переменные, — *открытыми*. Так, все приведенные выше формулы логики предикатов, кроме формулы P , являются открытыми.

Примеры замкнутых формул: P , $(\forall z)(R(z))$, $(\exists x)(\forall y)(P(x, y))$, $(\forall x)(Q(x)) \rightarrow \neg(\forall x)(\exists x)(R(x, y))$.

Классификация формул логики предикатов. Если в формулу логики предикатов вместо каждой предикатной переменной подставить конкретный предикат, определенный на некотором выбранном множестве M , то формула превратится в конкретный предикат, заданный над множеством M . При этом, если исходная формула была замкнутой, то полученный конкретный предикат окажется нульместным, т. е. будет высказыванием. Если же исходная формула была открытой, т. е. содержала свободные вхождения предметных переменных, то в результате подстановки получим предикат, зависящий от некоторых предметных переменных. Если теперь подставить вместо этих предметных переменных конкретные предметы из множества M , то полученный предикат, а следовательно, и исходная формула превратятся в конкретное высказывание.

Превращение формулы логики предикатов в высказывание описанным выше способом (а также само получаемое высказывание)

называется *интерпретацией* этой формулы на множестве M . Итак, если формула логики предикатов замкнутая, т. е. не содержит свободных предметных переменных, то ее интерпретация состоит из одного этапа и сводится к подстановке вместо всех предикатных переменных конкретных предикатов, в результате чего формула превращается в конкретное высказывание (нульместный предикат). Если же формула логики предикатов открытая, т. е. содержит ряд свободных предметных переменных, то ее интерпретация состоит из двух этапов. Во-первых, вместо всех предикатных переменных необходимо подставить конкретные предикаты, в результате чего формула превратится в конкретный предикат, зависящий от такого количества предметных переменных, сколько было свободных предметных переменных в исходной формуле. Во-вторых, нужно придать значение каждой предметной переменной, от которой зависит получившийся предикат, в результате чего этот предикат (и, значит, вся исходная формула) превратится в конкретное высказывание (истинное или ложное).

Пример 21.2. Дадим интерпретацию формуле $(\forall x)(\exists y)(P(x, y))$. В качестве множества M возьмем множество всех мужчин, а вместо предикатной переменной $P(x, y)$ подставим конкретный предикат, определенный на M : « x есть отец y ». Тогда исходная формула превратится в следующее (очевидно, ложное) высказывание $(\forall x)(\exists y)(x \text{ есть отец } y)$ — «у каждого мужчины есть сын». Этой же формуле можно дать и другую интерпретацию. Возьмем в качестве M множество N всех натуральных чисел, а вместо предикатной переменной $P(x, y)$ подставим предикат « $x < y$ », определенный на N^2 . Тогда исходная формула превратится в (очевидно, истинное) высказывание $(\forall x)(\exists y)(x < y)$ — «Для каждого натурального числа существует большее по сравнению с ним натуральное число».

Пример 21.3. В предыдущем примере была рассмотрена интерпретация замкнутой формулы. Дадим интерпретацию открытой формуле $(\exists z)(P(x, y, z) \rightarrow Q(x, y, z)) \rightarrow R$. В качестве множества M возьмем множество N всех натуральных чисел. Вместо предикатных переменных $P(x, y, z)$ и $Q(x, y, z)$ подставим трехместные предикаты « $x \cdot y = z$ » и « $x + y = z$ » соответственно, а вместо нульместного предиката R подставим (ложное) высказывание « $2 = 4$ ». Тогда данная формула превратится в двухместный предикат (от предметных переменных x, y):

$$(\exists z)(x \cdot y = z \rightarrow x + y = z) \rightarrow 2 = 4.$$

Посмотрим, в какие высказывания может превращаться данный предикат при подстановке вместо его переменных x и y конкретных предметов (чисел) из N . Нетрудно понять, что двухместный предикат $(\exists z)(x \cdot y = z \rightarrow x + y = z)$ превращается в истинное

высказывание при любой подстановке вместо его предметных переменных x и y натуральных чисел. В самом деле, для натуральных m и n получаем высказывание

$$(\exists z)(m \cdot n = z \rightarrow m + n = z).$$

Одноместный предикат (зависит от z) $m \cdot n = z \rightarrow m + n = z$, стоящий под знаком квантора $\exists z$, выполним, потому что всегда можно найти такое натуральное число k , что $m \cdot n \neq k$ и $m + n \neq k$, т.е. высказывания $m \cdot n = k$ и $m + n = k$ будут ложны, а значит, высказывание $m \cdot n = k \rightarrow m + n = k$ — истинно. А раз так, то высказывание $(\exists z)(m \cdot n = z \rightarrow m + n = z)$ истинно. Поэтому высказывание $(\exists z)(m \cdot n = z \rightarrow m + n = z) \rightarrow 2 = 4$, в которое превращается данный предикат, ложно. Итак, исходная открытая формула логики предикатов превращена в тождественно ложный предикат. Нетрудно понять, что если вместо предикатных переменных $P(x, y, z)$ и $Q(x, y, z)$ подставить только что рассмотренные предикаты, а вместо нульместной предикатной переменной R — любое истинное высказывание, то исходная формула превратится в тождественно истинный предикат.

Сформулируем классификационные определения для формул логики предикатов.

Определение 21.4. Формула логики предикатов называется *выполнимой (опровержимой)* на множестве M , если при некоторой подстановке вместо предикатных переменных конкретных предикатов, заданных на этом множестве, она превращается в выполнимый (опровержимый) предикат.

Другими словами, формула выполнима (опровержима) на M , если существует истинная (ложная) ее интерпретация на M . Формула из примера 21.2 является как выполнимой, так и опровержимой. Еще один пример такой формулы приведен в Задачнике, № 9.35, л. А в задаче № 9.54 подробно разбирается пример формулы, выполнимой на множестве из трех элементов и невыполнимой ни на каком множестве из двух элементов.

Определение 21.5. Формула логики предикатов называется *тождественно истинной (тождественно ложной)* на множестве M , если при всякой подстановке вместо предикатных переменных любых конкретных предикатов, заданных на этом множестве, она превращается в тождественно истинный (тождественно ложный) предикат.

В задачах № 9.53, 9.58 Задачника приводятся примеры формул, тождественно истинных на одних множествах, но не являющихся таковыми на других множествах.

Определение 21.6. Формула логики предикатов называется *общезначимой, или тавтологией (тождественно ложной или противоречием)*, если при всякой подстановке вместо предикатных переменных любых конкретных предикатов, заданных на каких угодно

множествах, она превращается в тождественно истинный (тождественно ложный) предикат. (Тот факт, что формула F является тавтологией, обозначается, как и в алгебре высказываний, $\models F$.)

Так, формула из примера 21.3 не является тавтологией, потому что хотя при одной подстановке она и превратилась в тождественно истинный предикат, при другой она оказалась превращенной в предикат тождественно ложный. Поэтому данная формула не является и противоречием.

Пример 21.7. Покажем, что формула $\neg P(x) \wedge (\forall y)(P(y))$ является противоречием, т.е. тождественно ложной. В самом деле, допустим противное: на некотором множестве M имеется конкретный предикат $A(x)$, такой, что данная формула превращается в выполнимый предикат (от x) $\neg A(x) \wedge (\forall y)(A(y))$. Последнее означает: найдется предмет $a \in M$, такой, что высказывание $\neg A(a) \wedge (\forall y)(A(y))$ истинно. Истинность конъюнкции дает истинность высказываний $\neg A(a)$ и $(\forall y)(A(y))$. Из истинности первого следует, что высказывание $A(a)$ ложно, а из истинности второго — что предикат $A(y)$ тождественно истинный и, значит, для любого предмета из M , в том числе и для $a \in M$, высказывание $A(a)$ истинно. Получаем противоречие, исключающее предположение о непротиворечивости исходной формулы. Следовательно, она тождественно ложна.

Нахождение тавтологий является одной из важнейших задач логики предикатов, как и алгебры высказываний. Но если в алгебре высказываний имеется общий метод определения, является или нет данная формула тавтологией (это — метод составления таблицы истинности для формулы), то в логике предикатов такого общего метода не существует. Каждая формула подлежит изучению индивидуальным методом на тождественную истинность. Дело здесь в том, что каждое высказывание имеет только одно из двух логических значений: «истина» или «ложь», тогда как значение предиката зависит от *выбора* значений его предметных переменных, который, вообще говоря, можно сделать бесконечным числом способов. Мы вернемся к этой проблеме в § 23 при рассмотрении ее для формул некоторых частных видов.

Тавтологии логики предикатов. Рассмотрим наиболее важные тавтологии логики предикатов. О значении тавтологий алгебры высказываний подробно говорилось в § 3. Все сказанное там сохраняет свое значение и для тавтологий логики предикатов. Но, как уже отмечалось, язык логики предикатов более тонок, а поэтому тавтологии логики предикатов более тонко отражают процессы логических умозаключений.

Рассмотрение тавтологий логики предикатов начнем с установления того, что простейшие ее тавтологии получаются из тавтологий алгебры высказываний, а тавтологии алгебры высказываний образуют часть тавтологий логики предикатов.

Теорема 21.8. *Всякая формула, получающаяся из тавтологии алгебры высказываний заменой входящих в нее пропозициональных переменных произвольными предикатными переменными, является тавтологией логики предикатов.*

Доказательство. Пусть $F(X_1, X_2, \dots, X_n)$ — тавтология алгебры высказываний и $P_1(x_1, x_2, \dots, x_{m_1}), P_2(y_1, y_2, \dots, y_{m_2}), \dots, P_n(z_1, z_2, \dots, z_{m_n})$ — предикатные переменные. Подставим их в данную формулу вместо пропозициональных переменных $X_1, X_2, \dots, X_n$ соответственно. Получим формулу логики предикатов: $F(P_1(x_1, \dots, x_{m_1}), \dots, P_n(z_1, \dots, z_{m_n}))$. Если теперь вместо предикатных переменных подставить произвольные конкретные предикаты $A_1(x_1, x_2, \dots, x_{m_1}), \dots, A_n(z_1, z_2, \dots, z_{m_n})$, то формула превратится в конкретный предикат $F(A_1(x_1, \dots, x_{m_1}), \dots, A_n(z_1, \dots, z_{m_n}))$. Этот предикат тождественно истинный, потому что подстановка вместо предметных переменных $x_1, \dots, x_{m_1}, \dots, z_1, \dots, z_{m_n}$ любых конкретных предметов $a_1, \dots, a_{m_1}, \dots, c_1, \dots, c_{m_n}$ из соответствующих множеств превращает данный предикат в высказывание $F(A_1(x_1, \dots, x_{m_1}), \dots, A_n(z_1, \dots, z_{m_n}))$, которое может быть получено также в результате подстановки в исходную тавтологию $F(X_1, X_2, \dots, X_n)$ алгебры высказываний вместо пропозициональных переменных $X_1, X_2, \dots, X_n$ конкретных высказываний $A_1(a_1, \dots, a_{m_1}), \dots, A_n(c_1, \dots, c_{m_n})$ соответственно и потому истинно. Следовательно, формула $F(P_1, P_2, \dots, P_n)$ логики предикатов также является тавтологией. Теорема доказана. $\square$

В последующих теоремах приводятся наиболее важные тавтологии логики предикатов, не сводящиеся к тавтологиям алгебры высказываний. Все такие тавтологии содержат кванторы.

Теорема 21.9 (законы де Моргана для кванторов). *Следующие формулы логики предикатов являются тавтологиями:*

- а) $\neg(\forall x)(P(x)) \leftrightarrow (\exists x)(\neg P(x))$;
- б) $\neg(\exists x)(P(x)) \leftrightarrow (\forall x)(\neg P(x))$.

Доказательство. Докажем тождественную истинность формулы а). (Тождественную истинность формулы б) предлагается проверить самостоятельно.) Данная формула замкнута, т.е. не имеет свободных предметных переменных. Поэтому, подставив в эту формулу вместо предикатной переменной $P(x)$ любой конкретный одноместный предикат $A(x)$, определенный на некотором множестве M , получим высказывание

$$\neg(\forall x)(A(x)) \leftrightarrow (\exists x)(\neg A(x)). \quad (1)$$

Для доказательства его истинности нужно убедиться, что обе части эквивалентности одновременно истинны или одновременно ложны. В самом деле, высказывание $\neg(\forall x)(A(x))$ истинно тогда и только тогда, когда высказывание $(\forall x)(A(x))$ ложно, что возможно на основании определения 20.1 тогда и только тогда, когда предикат $A(x)$ опровержим. Далее, опровержимость предиката

$A(x)$ означает выполнимость его отрицания $\neg A(x)$ (обдумайте это!), что равносильно на основании определения 20.3 истинности высказывания $(\exists x)(\neg A(x))$. Итак, высказывание $\neg(\forall x)(A(x))$ истинно тогда и только тогда, когда истинно высказывание $(\exists x)(\neg A(x))$. Следовательно, высказывание (1) истинно, что и доказывает тождественную истинность формулы а). $\square$

Непосредственно из этой теоремы и закона двойного отрицания (теорема 3.1, в) вытекает следствие.

Следствие 21.10 (выражение кванторов одного через другой). *Следующие формулы логики предикатов являются тавтологиями:*

$$а) (\forall x)(P(x)) \leftrightarrow \neg(\exists x)(\neg P(x));$$

$$б) (\exists x)(P(x)) \leftrightarrow \neg(\forall x)(\neg P(x)).$$

Заметим, что законы де Моргана для кванторов напоминают аналогичные законы для конъюнкции и дизъюнкции в алгебре высказываний. Можно считать, что эти законы для кванторов представляют собой обобщения соответствующих законов для конъюнкции и дизъюнкции, подобно тому как сами операции квантификации являются обобщениями операций конъюнкции и дизъюнкции, что отмечалось в § 20.

Теорема 21.11 (законы пренесения кванторов через конъюнкцию и дизъюнкцию). *Следующие формулы логики предикатов являются тавтологиями:*

$$а) (\forall x)(P(x) \wedge Q(x)) \leftrightarrow (\forall x)(P(x)) \wedge (\forall x)(Q(x));$$

$$б) (\exists x)(P(x) \vee Q(x)) \leftrightarrow (\exists x)(P(x)) \vee (\exists x)(Q(x));$$

$$в) (\forall x)(P(x) \vee Q) \leftrightarrow (\forall x)(P(x)) \vee Q;$$

$$г) (\exists x)(P(x) \wedge Q) \leftrightarrow (\exists x)(P(x)) \wedge Q.$$

Доказательство. а) Подставим вместо предикатных переменных $P(x)$ и $Q(x)$ конкретные предикаты $A(x)$ и $B(x)$, определенные на некотором множестве M . Формула превратится в высказывание

$$(\forall x)(A(x) \wedge B(x)) \leftrightarrow (\forall x)(A(x)) \wedge (\forall x)(B(x)). \quad (1)$$

Докажем его истинность. На основании определения 20.1 высказывание $(\forall x)(A(x) \wedge B(x))$ истинно тогда и только тогда, когда предикат $A(x) \wedge B(x)$ тождественно истинен, что на основании следствия 19.7 возможно в том и только в том случае, когда оба предиката $A(x)$ и $B(x)$ тождественно истинны. Далее, тождественная истинность предикатов $A(x)$ и $B(x)$ равносильна, ввиду определения 20.1, истинности высказываний $(\forall x)(A(x))$ и $(\forall x)(B(x))$ соответственно, что равносильно истинности их конъюнкции $(\forall x)(A(x)) \wedge (\forall x)(B(x))$. Итак, левая и правая части эквивалентности (1) одновременно истинны и одновременно ложны, что дает истинность всего высказывания (1) и тождественную истинность доказываемой формулы.

Тождественную истинность формул б) и в) предлагается доказать в качестве упражнения.

г) В этой формуле Q — нульместная предикатная переменная. Поэтому подставим в данную формулу вместо $P(x)$ конкретный одноместный предикат $A(x)$, определенный на некотором множестве M , а вместо Q — конкретное высказывание B . Формула превратится в высказывание

$$(\exists x)(A(x) \wedge B) \leftrightarrow (\exists x)(A(x)) \wedge B. \quad (2)$$

Докажем его истинность. Действительно, на основании определения 20.3 высказывание $(\exists x)(A(x) \wedge B)$ истинно тогда и только тогда, когда предикат $A(x) \wedge B$ выполним. Последнее возможно, если и только если предикаты $A(x)$ и B выполнимы. (Напомним, что в конце предыдущего параграфа было условлено под выполнимостью нульместного предиката (высказывания) понимать его истинность.) Далее, выполнимость предиката $A(x)$ и истинность высказывания B равносильны истинности высказываний $(\exists x)(A(x))$ и B , а значит, и истинности их конъюнкции $(\exists x)(A(x)) \wedge B$. Следовательно, высказывание (2) истинно для любых $A(x)$ и B , а поэтому рассматриваемая формула — тавтология. $\square$

Полезно проанализировать и сопоставить между собой тавтологии, связанные с пронесением кванторов через различные логические операции, представленные в теоремах 21.11 и 21.12. Особая важность этих тавтологий будет обнаружена в § 22, где рассматриваются равносильные преобразования формул логики предикатов. Здесь же мы имеем следующее. Квантор общности безоговорочно проносится через конъюнкцию, а также выносится из обоих членов конъюнкции (эта процедура важна для будущих равносильных преобразований формул), а квантор существования — через дизъюнкцию (теорема 21.11, а, б). Проблемы начинаются при столкновении квантора общности с дизъюнкцией и квантора существования с конъюнкцией. Здесь общезначимыми являются формулы не с эквивалентностями, а с импликацией (см. Задачник, № 9.43, в, г):

$$= (\exists x)(P(x) \wedge Q(x)) \rightarrow ((\exists x)(P(x)) \wedge (\exists x)(Q(x))); \quad (3)$$

$$= ((\forall x)(P(x)) \vee (\forall x)(Q(x))) \rightarrow (\forall x)(P(x) \vee Q(x)). \quad (4)$$

Оставив читателю проведение доказательств общезначимости приведенных формул, укажем примеры предикатов, которые показывают необщезначимость формул, являющихся обратными импликациями по отношению к данным. Для формулы (3) такими предикатами могут служить, например, следующие предикаты, заданные над множеством всех вещественных чисел R : « $x < 1$ » и « $x > 2$ ». Они посылку обратной импликации превращают в истинное высказывание $(\exists x)(x < 1) \wedge (\exists x)(x > 2)$, а заключение — в ложное высказывание $(\exists x)(x < 1 \wedge x > 2)$. Для формулы (4) подойдут предикаты, также заданные над R : « $x \leq 0$ » и « $x > 0$ », превращающие посылку

обратной импликации в истинное высказывание $(\forall x)(x \leq 0 \vee x > 0)$, а следствие — в ложное высказывание $(\forall x)(x \leq 0) \vee (\forall x)(x > 0)$.

Отметим, что тем не менее равносильное пронесение квантора общности через дизъюнкцию и квантора существования через конъюнкцию возможно. Это тот случай, когда один из членов дизъюнкции или конъюнкции не зависит от той предметной переменной, квантор по которой проносится (см. теорему 21.11, в, г).

Теорема 21.12 (законы пронесения кванторов через импликацию).
Следующие формулы логики предикатов являются тавтологиями:

- а) $(\forall x)(P(x) \rightarrow Q) \leftrightarrow ((\exists x)(P(x)) \rightarrow Q)$;
- б) $(\exists x)(P(x) \rightarrow Q) \leftrightarrow ((\forall x)(P(x)) \rightarrow Q)$;
- в) $(\forall x)(Q \rightarrow P(x)) \leftrightarrow (Q \rightarrow (\forall x)(P(x)))$;
- г) $(\exists x)(Q \rightarrow P(x)) \leftrightarrow (Q \rightarrow (\exists x)(P(x)))$.

Доказательство. Отметим, что предикатная переменная Q в этих формулах может быть не только нульместной, но и любой n -местной, важно лишь, чтобы в нее не входила предметная переменная x . Итак, пусть Q есть $Q(y_1, \dots, y_n)$. Будем считать для краткости, что Q есть одноместная предикатная переменная $Q(y)$. Тогда:

а) предположим, что данная формула не является тавтологией. В этом случае существуют такие конкретные предикаты $A(x)$ и $B(y)$, определенные на множествах M и M_1 соответственно, что предикат (от y)

$$(\forall x)(A(x) \rightarrow B(y)) \leftrightarrow ((\exists x)(A(x)) \rightarrow B(y))$$

опровержим, т.е. обращается в ложное высказывание при подстановке вместо предметной переменной y некоторого конкретного предмета $b \in M_1$:

$$\lambda[(\forall x)(A(x) \rightarrow B(b)) \leftrightarrow ((\exists x)(A(x)) \rightarrow B(b))] = 0.$$

Эквивалентность ложна, если ее члены принимают разные значения истинности, т.е. здесь могут представиться две возможности:

первая

$$\lambda[(\forall x)(A(x) \rightarrow B(b))] = 1; \quad (1)$$

$$\lambda[(\exists x)(A(x)) \rightarrow B(b)] = 0 \quad (2)$$

и вторая

$$\lambda[(\forall x)(A(x) \rightarrow B(b))] = 0; \quad (3)$$

$$\lambda[(\exists x)(A(x)) \rightarrow B(b)] = 1. \quad (4)$$

Рассмотрим первую возможность. Из формулы (2), по определению 1.7 импликации, имеем

$$\lambda[(\exists x)(A(x))] = 1; \quad (5)$$

$$\lambda[B(b)] = 0. \quad (6)$$

Далее, из формулы (5) и по определению 20.3 квантора существования заключаем, что предикат $A(x)$ выполним, т. е.

$$\lambda[A(a)] = 1 \quad (7)$$

для некоторого $a \in M$. Вернемся к соотношению (1). По определению 20.1 квантора общности предикат $A(x) \rightarrow B(b)$ тождественно истинен. В частности, если вместо предметной переменной x подставить $a \in M$, то получим истинное высказывание $\lambda[A(a) \rightarrow B(b)] = 1$. Но, учитывая (6) и (7), получаем $\lambda[A(a) \rightarrow B(b)] = \lambda[A(a)] \rightarrow \lambda[B(b)] = 1 \rightarrow 0 = 0$. Противоречие.

Рассмотрим вторую возможность, выраженную в соотношениях (3), (4). Из формулы (3), на основании определения 20.1 квантора общности, следует, что предикат $A(x) \rightarrow B(b)$ опровержим, т. е. $\lambda[A(a) \rightarrow B(b)] = 0$ для некоторого $a \in M$. Тогда по определению импликации 1.7 получим

$$\lambda[A(a)] = 1, \lambda[B(b)] = 0. \quad (8)$$

Учитывая второе из соотношений (8), из соотношения (4) заключаем, что $\lambda[(\exists x)(A(x))] = 0$. Последнее означает тождественную ложность предиката $A(x)$ (см. определение 20.3). В частности, для предмета $a \in M$ имеем $\lambda[A(a)] = 0$, что противоречит первому из соотношений (8).

Итак, в каждом случае приходим к противоречию, доказывающему невозможность сделанного предположения. Следовательно, данная формула — тавтология.

г) Предположим, что данная формула не является тавтологией. Тогда существуют такие конкретные предикаты $A(x)$ и $B(y)$, определенные на множествах M и M_1 соответственно, что предикат (от y) $(\exists x)(B(y) \rightarrow A(x)) \leftrightarrow (B(y) \rightarrow (\exists x)(A(x)))$ опровержим, т. е. обращается в ложное высказывание при подстановке вместо предметной переменной y некоторого конкретного предмета b из M_1 :

$$\lambda[(\exists x)(B(b) \rightarrow A(x)) \leftrightarrow (B(b) \rightarrow (\exists x)(A(x)))] = 0.$$

Эквивалентность ложна в двух случаях. Во-первых, когда

$$\lambda[(\exists x)(B(b) \rightarrow A(x))] = 1; \quad (1)$$

$$\lambda[B(b) \rightarrow (\exists x)(A(x))] = 0, \quad (2)$$

и, во-вторых, когда

$$\lambda[(\exists x)(B(b) \rightarrow A(x))] = 0; \quad (3)$$

$$\lambda[B(b) \rightarrow (\exists x)(A(x))] = 1. \quad (4)$$

Рассмотрим первый случай. Из соотношения (2), по определению 1.7 импликации, заключаем:

$$\lambda[B(b)] = 1; \quad (5)$$

$$\lambda[(\exists x)(A(x))] = 0. \quad (6)$$

Соотношение (6) свидетельствует о том, что предикат $A(x)$ тождественно ложен (определение 20.3). Далее, соотношение (1) показывает, на основании того же определения 20.3, что предикат $B(b) \rightarrow A(x)$ выполним. Учитывая соотношение (5), получаем: существует такой элемент $a \in M$, что $\lambda[A(a)] = 1$. Последнее противоречит доказанной выше тождественной ложности предиката $A(x)$.

Получить противоречие во втором случае, выраженном в соотношениях (3), (4), предлагается самостоятельно. Таким образом, рассматриваемая формула — тавтология.

Докажите тождественную истинность двух оставшихся формул. $\square$

Проанализируем теперь ситуацию, связанную с пронесением кванторов через импликацию, а также с их вынесением за знак импликации. В случаях, когда один из членов импликации (посылка или заключение) не зависит от той предметной переменной, по которой проносится квантор, равносильность также возможна. Но ситуация здесь несколько отличается от той, которая имеет место в случаях конъюнкции и дизъюнкции. Если от предметной переменной, стоящей под знаком квантора, не зависит посылка импликации, то соответствующий квантор без изменения проносится к заключению импликации (теорема 21.12, в). Если же от предметной переменной, стоящей под знаком квантора, не зависит заключение импликации, то соответствующий квантор при пронесении его к посылке импликации переворачивается, т.е. меняется на противоположный: квантор общности — на квантор существования, а квантор существования — на квантор общности (теорема 21.12, а, б).

В ситуации с импликацией имеет место одна интересная тавтология: если оба члена импликации зависят от переменной, стоящей под знаком квантора, то через импликацию можно равносильным образом пронести квантор существования, но при постановке его перед посылкой он поменяется на квантор общности (см. Задачник, № 9.45, з):

$$\models (\exists x)(P(x) \rightarrow Q(x)) \leftrightarrow ((\forall x)(P(x)) \rightarrow (\exists x)(Q(x))).$$

В то же время, если мы рассмотрим аналогичную формулу для квантора общности: $(\forall x)(P(x) \rightarrow Q(x)) \leftrightarrow ((\exists x)(P(x)) \rightarrow (\forall x)(Q(x)))$, то она уже не будет тавтологией. Тавтологией будет лишь импликация:

$$\models ((\exists x)(P(x)) \rightarrow (\forall x)(Q(x))) \rightarrow (\forall x)(P(x) \rightarrow Q(x)).$$

Докажите это самостоятельно. То, что обратная импликация не будет тавтологией, подтверждает пример двух предикатов $P(x)$: « x делится на 4» и $Q(x)$: « x четно», заданных над множеством натуральных чисел (см. Задачник, № 9.45, л).

Отметим далее, что, используя импликацию, квантор общности можно следующими двумя способами пронести через импли-

кацию предикатов, каждый из которых зависит от переменной, стоящей под знаком квантора (см. Задачник, № 9.45, *д*, *е*):

$$= (\forall x)(P(x) \rightarrow Q(x)) \rightarrow ((\forall x)(P(x)) \rightarrow (\forall x)(Q(x)));$$

$$= (\forall x)(P(x) \rightarrow Q(x)) \rightarrow ((\exists x)(P(x)) \rightarrow (\exists x)(Q(x))).$$

Проверьте, что формулы действительно являются тавтологиями, а обратные импликации таковыми не являются.

В то же время аналогичная конструкция с квантором существования $(\exists x)(P(x) \rightarrow Q(x)) \rightarrow ((\exists x)(P(x)) \rightarrow (\exists x)(Q(x)))$ уже не будет тавтологией (см. Задачник, № 9.45, *ж*). Пример: $P(x)$: « x — четно», $Q(x)$: « $x < 1$ », $x \in N$. Не будет тавтологией и обратная импликация. Пример: $P(x)$: « $x > 2$ », $Q(x)$: « $x < 1$ », $x \in R$.

Теорема 21.13 (законы удаления квантора общности и введения квантора существования). *Следующие формулы логики предикатов являются тавтологиями:*

$$а) (\forall x)(P(x)) \rightarrow P(y);$$

$$б) P(y) \rightarrow (\exists x)(P(x)).$$

Доказательство. Проверим, что формула *а*) тождественно истинна (соответствующую проверку для формулы *б*) выполнить самостоятельно). Предположим, что формула *а*) не тождественно истинна. Это значит: существует такой предикат $A(x)$, определенный на некотором множестве M , что предикат (от y) $(\forall x)(A(x)) \rightarrow A(y)$ опровержим, т.е. превращается в ложное высказывание при подстановке вместо y некоторого $a \in M$: $\lambda[(\forall x)(A(x)) \rightarrow A(a)] = 0$. Последнее означает, что

$$\lambda[(\forall x)(A(x))] = 1; \quad (1)$$

$$\lambda[A(a)] = 0. \quad (2)$$

Из соотношения (1) заключаем, что предикат $A(x)$ тождественно истинный. Но это противоречит соотношению (2). Следовательно, сделанное предположение неверно, и данная формула — тавтология. $\square$

Теорема 21.14 (законы коммутативности для кванторов). *Следующие формулы логики предикатов являются тавтологиями:*

$$а) (\forall x)(\forall y)(P(x, y)) \leftrightarrow (\forall y)(\forall x)(P(x, y));$$

$$б) (\exists x)(\exists y)(P(x, y)) \leftrightarrow (\exists y)(\exists x)(P(x, y));$$

$$в) (\exists y)(\forall x)(P(x, y)) \rightarrow (\forall x)(\exists y)(P(x, y)).$$

Доказательство. Тождественная истинность первых двух формул достаточно очевидна (проверьте самостоятельно).

Предположим, что формула *в*) — не тавтология. Тогда существует такой предикат $A(x, y)$, определенный на множествах M_1 и M_2 , что высказывание $(\exists y)(\forall x)(A(x, y)) \rightarrow (\forall x)(\exists y)(A(x, y))$ ложно. Импликация ложна, если и только если

$$\lambda[(\exists y)(\forall x)(A(x, y))] = 1; \quad (1)$$

$$\lambda[(\forall x)(\exists y)(A(x, y))] = 0. \quad (2)$$

Из соотношения (1) по определению квантора существования следует, что предикат (от y) $(\forall x)(A(x, y))$ выполним, т.е. $\lambda[(\forall x)(A(x, b))] = 1$ для некоторого $b \in M_2$. Последнее, по определению 20.1 квантора общности, означает, что предикат $A(x, b)$ тождественно истинен на M_1 . Следовательно, тождественно истинным на M_1 будет и одноместный (от x) предикат $(\exists y)(A(x, y))$. Но тогда, по определению квантора общности, $\lambda[(\forall x)(\exists y)(A(x, y))] = 1$, что противоречит соотношению (2). Следовательно, данная формула — тавтология. Теорема доказана. $\square$

Во всех доказанных тавтологиях предикатные переменные нульместны, одноместны или (в последней теореме) двухместны. Сохранится ли тождественная истинность этих формул, если считать, что входящие в них предикатные переменные зависят от произвольного числа предметных переменных? Положительный ответ содержится в следующей теореме.

Теорема 21.15. *Если в тавтологиях теорем 21.9—21.14 считать, что предикатные переменные зависят от произвольного конечного числа предметных переменных, то полученные формулы будут также тавтологиями логики предикатов.*

Доказательство. При доказательстве теоремы 21.12 уже была предпринята попытка к расширению смысла приведенных там тавтологий: под предикатной переменной Q понималась n -местная предикатная переменная $Q(y_1, y_2, \dots, y_n)$. Можно было бы и под одноместной предикатной переменной $P(x)$ понимать m -местную предикатную переменную $P(x_1, x_2, \dots, x_m)$, а квантор общности рассматривать по x_1 , считая, что x_1 не входит в число предметных переменных предикатной переменной $Q(y_1, y_2, \dots, y_n)$.

Докажем, например, тождественную истинность формулы из теоремы 21.11, в, считая P m -местной предикатной переменной $P(x_1, x_2, \dots, x_m)$, а Q — n -местной предикатной переменной $Q(y_1, y_2, \dots, y_n)$. Причем пусть x_1 не содержится среди предметных переменных $y_1, y_2, \dots, y_n$, хотя некоторые (или все) из переменных $x_2, \dots, x_m$ могут содержаться среди переменных $y_1, y_2, \dots, y_n$. Итак, требуется доказать тождественную истинность формулы

$$\begin{aligned} & (\forall x_1)(P(x_1, x_2, \dots, x_m) \vee Q(y_1, y_2, \dots, y_n)) \leftrightarrow \\ & \leftrightarrow (\forall x_1)(P(x_1, x_2, \dots, x_m)) \vee Q(y_1, y_2, \dots, y_n). \end{aligned} \quad (1)$$

Подставим вместо предикатных переменных P и Q конкретные предикаты $A(x_1, x_2, \dots, x_m)$ и $B(y_1, y_2, \dots, y_n)$, определенные на множествах $M_1, M_2, \dots, M_m$ и $N_1, N_2, \dots, N_n$ соответственно. Получим $(m-1+n)$ -местный предикат

$$\begin{aligned} & (\forall x_1)(A(x_1, x_2, \dots, x_m) \vee B(y_1, y_2, \dots, y_n)) \leftrightarrow \\ & \leftrightarrow (\forall x_1)(A(x_1, x_2, \dots, x_m)) \vee B(y_1, y_2, \dots, y_n), \end{aligned} \quad (2)$$

определенный на множествах $M_2, \dots, M_m, N_1, N_2, \dots, N_n$ (в случае, если некоторые переменные $x_2, \dots, x_m$ встречаются среди пере-

менных $y_1, y_2, \dots, y_n$, «местность» полученного предиката будет меньше). Докажем тождественную истинность данного предиката. Для этого проверим, что он превратится в истинное высказывание для произвольных элементов $a_2, \dots, a_m, b_1, b_2, \dots, b_n$ множеств $M_2, \dots, M_m, N_1, N_2, \dots, N_n$ соответственно. Действительно, рассмотрим одноместный (от x_1) предикат $A(x_1, a_2, \dots, a_m)$, определенный на множестве M_1 и полученный из предиката $A(x_1, x_2, \dots, x_m)$ в результате подстановки вместо предметных переменных $x_2, \dots, x_m$ элементов $a_2, \dots, a_m$ соответственно, и высказывание $B(b_1, b_2, \dots, b_n)$. Подставим их в тавтологию теоремы 21.11, в вместо одноместной предикатной переменной $P(x)$ и нульместной предикатной переменной Q соответственно. Получим истинное высказывание

$$(\forall x_1)(A(x_1, a_2, \dots, a_m) \vee B(b_1, b_2, \dots, b_n)) \leftrightarrow \\ \leftrightarrow (\forall x_1)(A(x_1, a_2, \dots, a_m)) \vee B(b_1, b_2, \dots, b_n).$$

Это же высказывание получится, если в предикат (2) подставить вместо его предметных переменных $x_2, \dots, x_m, y_1, y_2, \dots, y_n$ элементы $a_2, \dots, a_m, b_1, b_2, \dots, b_n$ соответственно. Итак, любые предикаты превращают формулу (1) в тождественно истинный предикат. Следовательно, эта формула — тавтология. $\square$

Замечание 21.16. В распространении взгляда на тавтологии, выраженного в теоремах 21.9 — 21.14, можно пойти еще дальше: считать, что буквы P и Q представляют собой произвольные формулы логики предикатов, а не просто n -местные предикатные переменные (представляющие собой на основании определения 21.1 так называемые элементарные или атомарные формулы). Получаемые формулы также будут тавтологиями логики предикатов.

Рекомендуется самостоятельно проделать пропущенные доказательства тождественной истинности формул логики предикатов в теоремах настоящего параграфа. Такая работа позволит глубже проникнуть в сущность понятий «для всех» и «существует», научит различать их и выделять в математической практике. Эти знания и навыки будут способствовать более отчетливому осознанию будущими учителями математики природы математических понятий, строения доказательств математических теорем, образованию значительного пласта логической и общематематической культуры.

§ 22. Равносильные преобразования формул и логическое следование формул логики предикатов

Понятие равносильности формул. Определение 22.1. Две формулы, F и H логики предикатов называются *равносильными на множестве M* , если при любой подстановке в эти формулы вместо

предикатных переменных любых конкретных предикатов, определенных на M , формулы превращаются в равносильные предикаты. Если две формулы равносильны на любых множествах, то их будем называть просто *равносильными*. Равносильность формул будем обозначать так: $F \equiv H$.

Приведем пример двух неравносильных формул логики предикатов. Покажем, что $(\forall x)(P(x) \vee Q(x)) \not\equiv (\forall x)(P(x)) \vee (\forall x)(Q(x))$. В самом деле, подставим вместо предикатных переменных $P(x)$ и $Q(x)$ конкретные предикаты $A(x)$ и $B(x)$, определенные на множестве N соответственно, где $A(x)$ есть « x — четно», а $B(x)$ есть « x — нечетно». Тогда левая формула превратится в высказывание (нульместный предикат) «каждое натуральное число либо нечетно, либо четно», которое истинно. Правая формула превращается в высказывание (нульместный предикат) «либо каждое натуральное число четно, либо каждое натуральное число нечетно», которое ложно.

Нетрудно понять на основании определений 22.1 и 21.6, что формулы F и H равносильны тогда и только тогда, когда формула $F \leftrightarrow H$ является тавтологией: $F \equiv H \Leftrightarrow F \leftrightarrow H$.

Это замечание вместе с теоремами 21.9 — 21.14 позволяет указать наиболее важные примеры равносильных формул (см. Задачник, № 9.49).

Как и в алгебре высказываний, можно заменять одну равносильную формулу другой. Переход от одной равносильной формулы к другой называется *равносильным преобразованием* исходной формулы. В процессе равносильных преобразований формул логики предикатов могут использоваться равносильности, известные из алгебры высказываний.

Приведенная форма для формул логики предикатов. Равносильные преобразования позволяют приводить формулы к тому или иному более удобному виду. Один из таких видов носит название приведенной формы.

Определение 22.2. Приведенной формой для формулы логики предикатов называется такая равносильная ей формула, в которой из операций алгебры высказываний имеются только операции $\neg$, $\wedge$, $\vee$, причем знаки отрицания относятся лишь к предикатным переменным и к высказываниям.

Теорема 22.3. Для каждой формулы логики предикатов существует приведенная форма.

Доказательство. Проведем доказательство методом математической индукции по числу логических связок в формуле (включая кванторы общности и существования).

Если формула не имеет логических связок, т.е. является атомарной, то она сама имеет приведенную форму. Предположим, что всякая формула, содержащая не больше $k-1$ логических связок, обладает приведенной формой. Покажем теперь, что приведенной

формой обладает также и всякая формула, содержащая k логических связок. Пусть F — такая формула. Тогда, на основании определения 21.1, она имеет один из следующих видов: $\neg F_1$, $(F_1 \wedge F_2)$, $(F_1 \vee F_2)$, $(F_1 \rightarrow F_2)$, $(F_1 \leftrightarrow F_2)$, $(\forall \xi)(F_1)$, $(\exists \xi)(F_1)$. Каждая из формул F_1 , F_2 содержит логических связок не более $k-1$, а поэтому, по предположению индукции, обладает приведенной формой. Пусть F_1^* и F_2^* — приведенные формы для формул F_1 и F_2 соответственно. Отсюда формулы $(F_1^* \wedge F_2^*)$, $(F_1^* \vee F_2^*)$, $(\forall \xi)(F_1^*)$, $(\exists \xi)(F_1^*)$ являются приведенными формами для формул $(F_1 \wedge F_2)$, $(F_1 \vee F_2)$, $(\forall \xi)(F_1)$, $(\exists \xi)(F_1)$ соответственно.

Остается рассмотреть случаи, когда F имеет один из следующих видов: $\neg F_1$, $(F_1 \rightarrow F_2)$ или $(F_1 \leftrightarrow F_2)$.

Пусть F есть $\neg F_1$. Тогда формула $\neg F_1^*$ может не быть приведенной формой для формулы $\neg F_1$. Строго говоря, для этого случая следует провести доказательство также методом математической индукции по числу логических связок формулы F_1^* . Если F_1^* атомарна, т.е. F_1^* — предикатная переменная P , то $(\neg F_1)^*$ есть $\neg P$ — приведенная форма. Если же F_1^* — составная формула, то задача сводится к пронесению знака $\neg$ через кванторы и операции $\wedge$ и $\vee$ (другие логические операции не входят в приведенную форму F_1^*). Это пронесение осуществляется на основании равносильностей из логики предикатов и алгебры высказываний, называемых законами де Моргана (см. теоремы 21.9 и 4.4, p , c). Итак, если F есть $\neg F_1$ и F_1 обладает приведенной формой F_1^* , то мы сможем найти приведенную форму и для F .

Далее, пусть F есть $(F_1 \rightarrow F_2)$. Тогда на основании теоремы 4.4, у формула F равносильна формуле $(\neg F_1 \vee F_2)$. Заменив формулы F_1 и F_2 на равносильные им приведенные формы F_1^* и F_2^* соответственно, получим равносильную формулу $(\neg F_1^* \vee F_2^*)$, которая, вообще говоря, не является приведенной. Но, на основании предыдущего абзаца, можно найти для формулы $\neg F_1^*$ приведенную форму F_1^{**} . Тогда ясно, что формула $(F_1^{**} \vee F_2^*)$ имеет приведенный вид и равносильна исходной формуле F .

Наконец, если F есть $(F_1 \leftrightarrow F_2)$, то на основании равносильности теоремы 4.4, F равносильна формуле $((F_1 \rightarrow F_2) \wedge (F_2 \rightarrow F_1))$. В предыдущем абзаце было показано, как найти приведенные формы $(F_1^{**} \vee F_2^*)$ и $(F_2^{**} \vee F_1^*)$ для формул $(F_1 \rightarrow F_2)$ и $(F_2 \rightarrow F_1)$ соответственно. Тогда ясно, что формула $(F_1^{**} \vee F_2^*) \wedge (F_2^{**} \vee F_1^*)$ имеет приведенный вид и равносильна исходной формуле F .

Итак, в любом случае формула F обладает приведенной формой. Теорема доказана. $\square$

Разберите пример № 9.51, $л$ из Задачника.

Предваренная нормальная форма для формул логики предикатов. Еще одним удобным видом формулы, к которому ее можно привести равносильными преобразованиями, является предваренная нормальная форма.

Определение 22.4. Предваренной нормальной формой для формулы логики предикатов называется такая ее приведенная форма, в которой все кванторы стоят в ее начале, а область действия каждого из них распространяется до конца формулы, т.е. это формула вида $(K_1x_1) \dots (K_mx_m) (F(x_1, \dots, x_n))$, где K_i есть один из кванторов $\forall$ или $\exists$ ($i = 1, \dots, m$), $m \leq n$, причем формула F не содержит кванторов и является приведенной формулой. (Заметим, что кванторы в формуле могут отсутствовать вовсе.)

Теорема 22.5. Для каждой формулы логики предикатов существует предваренная нормальная форма.

Доказательство. Проведем доказательство по индукции, следуя правилу построения формул логики предикатов (определение 21.1).

Если формула атомарна, то она сама представляет собой предваренную нормальную форму. Поскольку каждая формула F равносильна формуле, полученной из более простых формул F_1 и F_2 с помощью операций $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$ (операции $\rightarrow$ и $\leftrightarrow$ выражаются через $\neg$, $\wedge$ и $\vee$), то теперь остается научиться находить предваренные нормальные формы для формул $\neg F_1$, $(F_1 \wedge F_2)$, $(F_1 \vee F_2)$, $(\forall x)(F_1)$, $(\exists x)(F_1)$, если известны предваренные нормальные формы F_1^* и F_2^* формул F_1 и F_2 соответственно. Пусть, например, F_1^* имеет вид $(\forall x_1)(\forall x_2)(\exists x_3) \dots (\exists x_n)(G_1(x_1, \dots, x_n))$, а F_2^* имеет вид $(\exists y_1)(\forall y_2) \dots (\forall y_m)(G_2(y_1, \dots, y_m))$.

Рассмотрим формулу $\neg F_1$. Поскольку $F_1 \equiv F_1^*$, то $\neg F_1 \equiv \neg F_1^*$. Но формула $\neg F_1^*$, в свою очередь, равносильна, на основании законов де Моргана для кванторов (теорема 21.9), формуле

$$(\exists x_1)(\exists x_2)(\forall x_3) \dots (\forall x_n)(\neg G_1(x_1, \dots, x_n)).$$

Остается по законам де Моргана для конъюнкции и дизъюнкции (теорема 4.4, p , c) пронести знак отрицания до предикатных переменных: $\neg G_1 \equiv G_1^*$. Тогда $\neg F_1$ будет иметь предваренную нормальную форму

$$(\exists x_1)(\exists x_2)(\forall x_3) \dots (\forall x_n)(G_1^*(x_1, \dots, x_n)).$$

Далее, покажем, как отыскивается предваренная нормальная форма для F , если F есть $(F_1 \wedge F_2)$. Поскольку при переименовании связанной переменной формула, очевидно, переходит в равносильную, то можно считать, что переменные $x_1, \dots, x_n$ не входят в формулу F_2^* , а переменные $y_1, \dots, y_m$ не входят в F_1^* . Ясно, что $F_1 \wedge F_2 \equiv F_1^* \wedge F_2^*$, но последняя формула еще не представляет собой предваренной нормальной формы. Покажем, как ее можно преобразовать к такой форме. На основании равносильности (получаемой из тавтологии) теоремы 21.11, а формула $(F_1^* \wedge F_2^*)$ равносильна формуле

$$(\forall x_1)[(\forall x_2)(\exists x_3) \dots (\exists x_n)(G_1(x_1, \dots, x_n)) \wedge (\exists y_1)(\forall y_2) \dots (\forall y_m)(G_2(y_1, \dots, y_m))].$$

Теперь можно производить равносильные преобразования под знаком квантора $\forall x_1$ в квадратных скобках, потому что в результате связывания квантором по одной и той же переменной x_1 двух равносильных формул мы снова получим равносильные формулы. Тогда, на основании той же равносильности, последняя формула равносильна формуле

$$(\forall x_1)(\forall x_2)[(\exists x_3) \dots (\exists x_n)(G_1(x_1, \dots, x_n)) \wedge \wedge (\exists y_1)(\forall y_2) \dots (\forall y_m)(G_2(y_1, \dots, y_m))].$$

И так далее. Наконец, на основании равносильности (получаемой из тавтологии) теоремы 21.11, ε последняя формула равносильна формуле

$$(\forall x_1)(\forall x_2)(\exists x_3) \dots (\exists x_n)[(G_1(x_1, \dots, x_n)) \wedge \wedge (\exists y_1)(\forall y_2) \dots (\forall y_m)(G_2(y_1, \dots, y_m))].$$

Таким же образом кванторы, стоящие перед формулой G_2 , выносятся за квадратные скобки. В результате получим формулу

$$(\forall x_1)(\forall x_2)(\exists x_3) \dots (\exists x_n) (\exists y_1)(\forall y_2) \dots \dots (\forall y_m) [G_1(x_1, \dots, x_n) \wedge G_2(y_1, \dots, y_m)],$$

равносильную формуле $(F_1 \wedge F_2)$ и являющуюся предваренной нормальной формой этой формулы.

Аналогичным образом при помощи равносильностей (получаемых из тавтологий) теоремы 21.11, δ можно построить предваренную нормальную форму для формулы $(F_1 \vee F_2)$, исходя из предваренных нормальных форм F_1^* и F_2^* формул F_1 и F_2 соответственно.

Наконец, нетрудно понять, что формула $(\forall \xi)(F_1^*)$ равносильна формуле $(\forall \xi)(F_1)$ и является ее предваренной нормальной формой. Аналогично, $(\exists \xi)(F_1^*)$ — предваренная нормальная форма для формулы $(\exists \xi)(F_1)$.

Итак, в каждом случае F обладает предваренной нормальной формой. Теорема доказана. $\square$

Разберите пример № 9.52, m из Задачника.

Логическое следование формул логики предикатов. Понятие логического следования для формул логики предикатов соответствует понятию логического следования для формул алгебры высказываний. Формула G логики предикатов называется *логическим следствием* формулы F , если при всякой интерпретации, при которой F превращается в тождественно истинный предикат, формула G также превращается в тождественно истинный предикат. Запись: $F \models G$. Как и в алгебре высказываний, $F \models G \Leftrightarrow \models F \rightarrow G$. Также две формулы равносильны тогда и только тогда, когда каждая из них является логическим следствием другой. Поэтому здесь целесооб-

ажно еще раз обратить внимание на такие тавтологии, имеющие форму импликации, для которых обратные импликации тавтологиями не являются. Так, закон о перестановке разноименных кванторов (теорема 21.14, в) приводит к логическому следованию: $(\exists y)(\forall x)(F(x, y)) \models (\forall x)(\exists y)(F(x, y))$, причем обратное следование не выполняется.

Аналогичные примеры логических следований дают тавтологии, связанные с пронесением кванторов через знаки логических пераций, которые мы обсуждали в предыдущем параграфе:

$$\begin{aligned}(\exists x)(P(x) \wedge Q(x)) &\models (\exists x)(P(x)) \wedge (\exists x)(Q(x)); \\(\forall x)(P(x)) \vee (\forall x)(Q(x)) &\models (\forall x)(P(x) \vee Q(x)); \\(\exists x)(P(x)) \rightarrow (\forall x)(Q(x)) &\models (\forall x)(P(x) \rightarrow Q(x)); \\(\forall x)(P(x) \rightarrow Q(x)) &\models (\forall x)(P(x)) \rightarrow (\forall x)(Q(x)); \\(\forall x)(P(x) \rightarrow Q(x)) &\models (\exists x)(P(x)) \rightarrow (\exists x)(Q(x)).\end{aligned}$$

Наконец обратим внимание на тавтологии теоремы 21.13, выражающие законы удаления квантора общности и введения квантора существования

$$\models (\forall x)(F(x)) \rightarrow F(y), \quad \models F(y) \rightarrow (\exists x)(F(x))$$

при условии, что предметная переменная y не входит свободно в формулу $F(x)$. Из этих тавтологий получаются следующие логические следования:

$(\forall x)(F(x)) \models F(y)$ — правило удаления квантора общности или *правило универсальной конкретизации*;

$F(y) \models (\exists x)(F(x))$ — правило введения квантора существования (или *правило экзистенциального обобщения*).

Эти правила можно представить также в следующих видах:

$$\frac{\Gamma \models F(x)}{\Gamma \models (\forall x)(F(x))}, \quad \frac{\Gamma, F(x) \models G}{\Gamma, (\exists x)(F(x)) \models G},$$

при условии, что ни в одну формулу из совокупности Γ и в формулу G предметная переменная x не входит свободно.

Обоснуем, например, первое из этих правил (второе обоснуем самостоятельно). По условию $\Gamma \models F(x)$, т.е. формула $F(x)$ превращается в тождественно истинный предикат при всякой такой интерпретации, при которой в тождественно истинные предикаты превращаются все формулы из совокупности Γ . Пусть мы имеем такую интерпретацию и при ней формула $F(x)$ превращается в тождественно истинный предикат $F_0(x, y_1, \dots, y_n)$ от переменных $x, y_1, \dots, y_n$. Тогда, по определению квантора общности, предикат $(\forall x)(F_0(x, y_1, \dots, y_n))$ от переменных $y_1, \dots, y_n$ также будет тождественно истинным. Это и означает, что $\Gamma \models (\forall x)(F(x))$.

§ 23. Проблемы разрешения для общезначимости и выполнимости формул

Постановка проблемы и ее неразрешимость в общем виде. В алгебре высказываний было установлено, что существует четкий алгоритм, позволяющий для каждой формулы алгебры высказываний ответить на вопрос, будет ли данная формула выполнима, тождественно истинна или тождественно ложна. Для этого нужно составить таблицу истинности формулы и посмотреть на распределение нулей и единиц в ее последнем столбце. Аналогичная проблема возникает и для формул логики предикатов: существует ли единый алгоритм, позволяющий для каждой формулы логики предикатов определить, будет ли она выполнимой или общезначимой? Ответ отрицательный: *общего такого алгоритма не существует*. Это было доказано в 1936 г. американским математиком А. Чёрчем. Тем не менее для некоторых частных видов формул данная проблема допускает решение. В настоящем параграфе покажем, как решается проблема разрешения для некоторых типов формул.

Решение проблемы для формул на конечных множествах. Если формула логики предикатов рассматривается на конечном множестве, то вместо ее предикатных переменных могут подставляться конкретные предикаты, определенные на этом конечном множестве. Ввиду того что операции квантификации на конечном множестве сводятся к конъюнкции и дизъюнкции (см. § 20), задача о выполнимости и общезначимости формулы логики предикатов на конечном множестве сводится к задаче о выполнимости или общезначимости некоторой формулы алгебры высказываний. Последняя задача, как мы знаем, эффективно разрешима.

Продemonстрируем идею действия этого алгоритма на конкретном примере. Рассмотрим формулу логики предикатов $(\forall y)(\exists x)(\neg P(x, y) \wedge P(y, y))$ и выясним, будет ли она выполнима или общезначима на двухэлементном множестве $\{a, b\}$. Напомним (см. § 20), что поскольку на этом множестве высказывание $(\forall x)(R(x))$ эквивалентно конъюнкции $R(a) \wedge R(b)$, а высказывание $(\exists x)(R(x))$ — дизъюнкции $R(a) \vee R(b)$, то данная формула равносильна формуле $(\exists x)(\neg P(x, a) \wedge P(a, a)) \wedge (\exists x)(\neg P(x, b) \wedge P(b, b))$, которая, в свою очередь, равносильна формуле

$$[(\neg P(a, a) \wedge P(a, a)) \vee (\neg P(b, a) \wedge P(a, a))] \wedge \\ \wedge [(\neg P(a, b) \wedge P(b, b)) \vee (\neg P(b, b) \wedge P(b, b))].$$

Одна двухместная предикатная переменная $P(x, y)$ исходной формулы как бы распалась на четыре пропозициональных переменных $P(a, a)$, $P(a, b)$, $P(b, a)$, $P(b, b)$ последней формулы, потому что при подстановке в исходную формулу вместо $P(x, y)$

двухместного предиката, определенного на $\{a, b\}$, указанные четыре переменные превратятся в конкретные высказывания (вообще говоря, различные). Так что последняя формула есть по сути дела формула алгебры высказываний. Чтобы это увидеть совсем отчетливо, обозначим указанные четыре пропозициональные переменные буквами P, R, Q, S соответственно. Тогда полученная формула примет вид: $[(\neg P \wedge P) \vee (\neg Q \wedge P)] \wedge [(\neg R \wedge S) \vee (\neg S \wedge S)]$. Составив таблицу истинности данной формулы алгебры высказываний (или каким-либо другим способом, как это делалось в алгебре высказываний), легко установить, что формула не является тавтологией, но выполнима: она превратится в истинное высказывание, если вместо P и S подставить истинные высказывания, а вместо Q и R — ложные. Применительно к исходной формуле логики предикатов это означает, что она не общезначима на двухэлементном множестве, но выполнима в нем: она превратится в выполнимый предикат, если вместо предикатной переменной $P(x, y)$ подставить в формулу такой конкретный двухместный предикат, который при одинаковых значениях его предметных переменных x и y превращается в истинные высказывания, а при разных — в ложные.

Пример формулы, выполнимой на бесконечном множестве и невыполнимой ни на каком конечном множестве. Наличие такой формулы позволит сделать, в частности, следующий вывод относительно проблемы разрешения для выполнимости формул логики предикатов: по выполнимости формулы на некотором множестве нельзя судить о выполнимости этой формулы на его подмножествах.

Вот п р и м е р такой формулы:

$$(\forall x)(\exists y)(P(x, y)) \wedge (\forall x)(\neg P(x, x)) \wedge (\forall x)(\forall y)(\forall z)[(P(x, y) \wedge P(y, z)) \rightarrow P(x, z)].$$

Можно сказать, что она характеризует неререфлексивность (второй член конъюнкции) и транзитивность (третий член конъюнкции) некоего двухместного предиката $P(x, y)$. Эта замкнутая формула превращается в истинное высказывание, если в нее вместо предикатной переменной $P(x, y)$ подставить, например, двухместный предикат « $x < y$ », определенный на $N \times N$, где N — множество всех натуральных чисел, т. е.

$$(\forall x)(\exists y)(x < y) \wedge (\forall x)(\neg(x < x)) \wedge (\forall x)(\forall y)(\forall z)[(x < y \wedge y < z) \rightarrow x < z].$$

Покажем, что эта формула не выполнима ни на каком конечном множестве. Допустим противное, т. е. предположим, что существует конкретный предикат $A(x, y)$, определенный на конечном множестве M , такой, что высказывание

$$(\forall x)(\exists y)(A(x, y)) \wedge (\forall x)(\neg A(x, x)) \wedge (\forall x)(\forall y)(\forall z)[(A(x, y) \wedge A(y, z)) \rightarrow A(x, z)] \quad (1)$$

истинно. Тогда истинным высказыванием будет и каждый член конъюнкции (1). В частности, истинно высказывание $(\forall x)(\exists y)(A(x, y))$. Возьмем элемент $a_1 \in M$. Тогда из истинности последнего высказывания следует вывод: существует такой элемент $a_2 \in M$, что высказывание $A(a_1, a_2)$ истинно. Далее, аналогично существует такой $a_3 \in M$, что истинно высказывание $A(a_2, a_3)$, и т.д. Поскольку множество M конечно, то не все элементы $a_1, a_2, a_3, \dots$ попарно различны. Пусть $a_p = a_{p+q}$ ($q > 0$). Тогда из истинности высказываний $A(a_p, a_{p+1}), A(a_{p+1}, a_{p+2}), \dots, A(a_{p+q-1}, a_{p+q})$ в силу истинности высказывания (третий член истинной конъюнкции (1))

$$(\forall x)(\forall y)(\forall z)[(A(x, y) \wedge A(y, z)) \rightarrow A(x, z)]$$

заключаем, что истинно высказывание $A(a_p, a_{p+q})$, т.е. высказывание $A(a_p, a_p)$. Но это противоречит истинности высказывания (второй член истинной конъюнкции (1)) $(\forall x)(\neg A(x, x))$. Полученное противоречие доказывает, что никакой конкретный предикат, определенный на конечном множестве, не может превратить данную формулу в истинное высказывание, т.е. данная формула невыполнима ни на каком конечном множестве.

Проблема разрешения выполнимости: влияние мощности множества и структуры формулы. Во-первых, нетрудно понять, что если некоторая формула выполнима или тождественно истинна на некотором множестве, то то же самое будет иметь место и на любом другом множестве с тем же самым числом элементов, т.е. на любом другом множестве, равномоном с исходным (это следует из наличия взаимно-однозначного отображения этих множеств одного на другое). Поэтому проблема разрешимости выполнимости и общезначимости формул логики предикатов состоит фактически в том, чтобы ответить на вопрос, для каких множеств данная формула выполнима (соответственно общезначима), а для каких — нет.

В дополнение к уже установленным результатам укажем еще ряд результатов в этом направлении. Так, теорема Лёвенгейма утверждает, что если формула выполнима на каком-нибудь бесконечном множестве, то она выполнима и на счетно-бесконечном множестве (доказательство можно найти, например, в книге П. С. Новикова [5.18]). Дальнейшее сведение проблемы разрешимости со счетно-бесконечных множеств на конечные, для которых проблемы разрешимости решаются, невозможно. Примером формулы, выполнимой на бесконечном множестве и не выполнимой ни на каком конечном множестве, может служить формула (1), рассмотренная в предыдущем пункте (см. также Задачник, формулы в задаче № 9.56).

Далее, примеры формул из задач № 9.54 и 9.55 Задачника показывают, что положительное решение проблемы выполнимости формулы на некотором конечном множестве не влечет ее положительного решения для этой формулы на множествах с меньшим числом элементов. Так, в задаче № 9.54 Задачника подробно анализируется формула

$$(\exists x, y, z)[R(x, y) \wedge R(x, z) \wedge R(y, z) \wedge (\forall t)(\neg R(t, t))],$$

относительно которой доказывается, что она будет выполнима на множестве из трех элементов (выполняющий предикат « $x \neq y$ ») и не выполнима на множестве из двух элементов.

В задаче № 9.55 Задачника предлагается привести пример формулы, выполнимой на множестве из четырех элементов и не выполнимой ни на каком множестве из трех элементов. Ясно, что она строится по образу и подобию предыдущей формулы:

$$(\exists x, y, z, u)[R(x, y) \wedge R(x, z) \wedge R(x, u) \wedge R(y, z) \wedge \\ \wedge R(y, u) \wedge R(z, u) \wedge (\forall t)(\neg R(t, t))].$$

Тем не менее проблема выполнимости обладает одним общим свойством.

Теорема 23.1. *Если некоторая формула логики предикатов выполнима в каком-нибудь множестве, то она выполнима также и в каждом множестве с большим числом элементов.*

Доказательство. Не нарушая общности, можно считать, что множество M' с числом элементов большим, чем число элементов в M , содержит M в качестве подмножества: достаточно установить взаимно-однозначное соответствие между элементами множества M и элементами подмножества M_0 множества M' , равномощного M . Пусть теперь формула $F(P_1, \dots, P_m)$ выполнима в множестве M и $M \subset M'$. Это означает, что некоторые конкретные предикаты $A_1, \dots, A_m$, заданные над множеством M , превращают формулу $F(P_1, \dots, P_m)$ в выполнимый предикат $F(A_1, \dots, A_m)$ над M . Увидим, что определения этих предикатов можно так расширить до предикатов $A'_1, \dots, A'_m$, заданных уже на M' , что они также будут превращать формулу $F(P_1, \dots, P_m)$ в выполнимый предикат $F(A'_1, \dots, A'_m)$ над M' . Для этого выбирается элемент $a \in M$, и предикат $A'_i(x_1, \dots, x_n)$ задается так. Логические значения высказывания $A'_i(a_1, \dots, a_n)$ на кортеже $a_1, \dots, a_n$ элементов из M' вычисляются по следующему правилу: $\lambda[A'_i(a_1, \dots, a_n)] = \lambda[A_i(\bar{a}_1, \dots, \bar{a}_n)]$, где $\bar{a}_k = a_k$, если $a_k \in M$, и $\bar{a}_k = a$, если $a_k \in M' \setminus M$. Тогда ясно, что предикат $F(A'_1, \dots, A'_m)$ будет превращаться в истинное высказывание на тех же самых предметах из $M \subset M'$, что и предикат $F(A_1, \dots, A_m)$. $\square$

В заключение укажем ряд результатов, которые сводят (редуцируют) проблему разрешимости для произвольных формул ло-

гики предикатов к проблеме разрешимости формул некоторых специальных видов. Будем считать, не нарушая общности, что все формулы, о которых идет речь, не имеют свободных предметных переменных, т. е. являются замкнутыми.

Во-первых, мы уже отмечали (см. теорему 21.5), что для всякой формулы логики предикатов существует равносильная ей формула в предваренной нормальной форме. Более того, еще в 1930-е гг. Сколем доказал, что для каждой формулы логики предикатов можно указать формулу в предваренной нормальной форме, кванторная приставка которой имеет вид $(\forall x_1) \dots (\forall x_m)(\exists y_1) \dots (\exists y_n)$ (так называемая *нормальная форма Сколема*), которая относительно выполнимости равнозначна первой. Это означает, что при решении проблемы выполнимости, не уменьшая общности, можно ограничиться рассмотрением лишь формул, имеющих кванторные приставки указанного вида.

Далее, для каждой формулы можно указать равнозначную ей в отношении выполнимости формулу, в которой имеются только одноместные и двухместные предикатные переменные (Лёвенгейм, 1915). Можно, далее, ограничиться даже такими формулами, в которых встречается только один-единственный двухместный предикатный символ и, кроме того, приставка имеет вид: $(\exists x_1) \dots (\exists x_m)(\forall y_1)(\forall y_2) (\exists z)(\forall u_1) \dots (\forall u_n)$ (Кальмар, 1936). При решении проблемы выполнимости можно также ограничиться формулами, приставки которых имеют форму $(\forall x_1)(\forall x_2)(\forall x_3)(\exists y_1) \dots (\exists y_n)$ (Гёдель, 1933) или же форму $(\exists x)(\forall y)(\exists z)(\forall u_1) \dots (\forall u_n)$ (Аккерман, 1936).

Имеются и другие предложения редукции рассматриваемой проблемы либо к формулам с кванторными приставками специальных видов, либо к формулам, содержащим предикатные переменные от определенного числа переменных.

Решение проблемы для формул, содержащих только одноместные предикатные переменные. В этом случае проблема сводится к проблеме разрешения выполнимости и общезначимости формулы на некотором конечном множестве, которая, как установлено выше, имеет эффективное решение. Такое сведение осуществляется на основе следующей теоремы и следствия из нее.

Теорема 23.2. *Если формула логики предикатов, содержащая только одноместные предикатные переменные, выполнима, то она выполнима на конечном множестве, содержащем не более 2^n элементов, где n — число различных предикатных переменных, входящих в рассматриваемую формулу.*

Доказательство. Заметим сначала, что если $G(x_1, \dots, x_k)$ — открытая формула логики предикатов, в которой $x_1, \dots, x_k$ — все ее свободные предметные переменные, то выполнимость такой формулы равносильна выполнимости следующей замкнутой формулы: $(\exists x_1) \dots (\exists x_k) (G(x_1, \dots, x_k))$. (Продумайте это утверждение.) По-

этому доказательство теоремы достаточно провести для замкнутой формулы в предваренной нормальной форме.

Пусть

$$F \equiv (K_1 x_1) \dots (K_n x_n) (H(P_1(x_1), \dots, P_n(x_n))) \quad (1)$$

такая формула, где каждый K_i есть один из кванторов $\forall$ или $\exists$ ($i = 1, \dots, n$), $P_i(x_i)$ — одноместные предикатные переменные ($i = 1, \dots, n$), а формула H не содержит кванторов. Предположим, что формула F выполняется на некотором множестве M . Это означает, что существуют конкретные одноместные предикаты $A_1(x_1), \dots, A_n(x_n)$, определенные на M , такие, что высказывание

$$F(A_1(x_1), \dots, A_n(x_n)) = (K_1 x_1) \dots (K_n x_n) (H(A_1(x_1), \dots, A_n(x_n))) \quad (2)$$

истинно.

Рассмотрим конечную последовательность $\xi_1, \xi_2, \dots, \xi_n$, в которой каждое ξ_i есть 0 или 1, и выберем все такие элементы a из множества M , для которых $\lambda(A_1(a)) = \xi_1, \lambda(A_2(a)) = \xi_2, \dots, \lambda(A_n(a)) = \xi_n$. Подмножество множества M , составленное из всех таких элементов, обозначим M_α (где α — десятичная запись двоичного числа $\overline{\xi_1 \xi_2 \dots \xi_n}$). Итак,

$$M_\alpha = \{a \in M : \lambda(A_1(a)) = \xi_1, \lambda(A_2(a)) = \xi_2, \dots, \lambda(A_n(a)) = \xi_n\}.$$

В частности, для некоторой последовательности $\xi_1, \xi_2, \dots, \xi_n$ требуемых элементов a в множестве M может не найтись. Тогда такое $M_\alpha = \emptyset$. Но ясно, что $M_\alpha \neq M_\beta = \emptyset$, если $\alpha \neq \beta$. Сколько же всего образуется подмножеств M_α ? Ровно столько, сколько существует конечных последовательностей длины n , составленных из нулей и единиц, т.е. 2^n (см. доказательство теоремы 10.3). Но некоторые подмножества, как было отмечено, могут быть пустыми. Поэтому число m непустых подмножеств M_α не превосходит числа 2^n . Другими словами, набор непустых подмножеств M_α образует разбиение множества M на непересекающиеся подмножества. Обозначим через $\mathbf{M}$ множество, элементами которого являются все непустые подмножества M_α :

$$\mathbf{M} = \{M_\alpha : M_\alpha \neq \emptyset, \alpha = 1, \dots, m; m \leq 2^n\}$$

(число элементов в $\mathbf{M}$ равно $m \leq 2^n$).

Определим на множестве $\mathbf{M}$ n одноместных предикатов $A'_1(x_1), \dots, A'_n(x_n)$ по следующему правилу: каждый предикат $A'_i(x_i)$ таков, что логическое значение $\lambda(A'_i(M_\alpha))$ высказывания $A'_i(M_\alpha)$, получающегося из этого предиката в результате подстановки вместо предметной переменной x_i элемента M_α множества $\mathbf{M}$, совпадает с логическим значением $\lambda(A_i(a))$ высказывания $A_i(a)$,

получающегося из предиката $A_i(x_i)$ подстановкой элемента a вместо переменной x_i , где $a \in M_\alpha$. (Отметим, что определение корректно, т.е. не зависит от выбора a в множестве M_α , потому что для всех a из M_α $\lambda(A_i(a)) = \xi_i$.) Итак, по определению имеем

$$\lambda(A'_i(M_\alpha)) = \lambda(A_i(a)) \quad (i = 1, \dots, n) \quad (3)$$

для $a \in M_\alpha$.

Докажем теперь, что формула $F(P_1, \dots, P_n)$ выполнима на m -элементном множестве $\mathbf{M}$, а именно, что она превращается при подстановке в нее вместо предикатных переменных $P_1(x_1), \dots, P_n(x_n)$ конкретных предикатов $A'_1(x_1), \dots, A'_n(x_n)$ соответственно в выполнимый предикат $F(A'_1(x_1), \dots, A'_n(x_n))$ (фактически истинное высказывание). Доказательство этого утверждения проведем индукцией по числу кванторов в предваренной нормальной форме формулы F . Сформулируем еще раз полностью то утверждение, которое будем доказывать по индукции: если некоторая формула $F(P_1, \dots, P_n)$ выполняется на множестве M для предикатов $A_1(x_1), \dots, A_n(x_n)$ и предметов $a_1, \dots, a_n \in M$, то она выполняется и на m -элементном множестве $\mathbf{M}$ для предикатов $A'_1(x_1), \dots, A'_n(x_n)$ и предметов $M_{\alpha_1}, \dots, M_{\alpha_n}$, таких, что $a_1 \in M_{\alpha_1}, \dots, a_n \in M_{\alpha_n}$ (эти предикаты определены в предыдущем абзаце). Причем некоторые (или все) предметы могут отсутствовать, если соответствующие переменные связаны.

Пусть сначала формула $F(P_1, \dots, P_n)$ не имеет кванторов вовсе, т.е.

$$F(P_1, \dots, P_n) \equiv H(P_1(x_1), \dots, P_n(x_n)).$$

Тогда выполнимость ее на множестве M для предикатов $A_1(x_1), \dots, A_n(x_n)$ и предметов $a_1, \dots, a_n \in M$ означает, что предикат $H(A_1(x_1), \dots, A_n(x_n))$ выполним, причем

$$\lambda[H(A_1(a_1), \dots, A_n(a_n))] = 1.$$

Формула H не содержит кванторов и, следовательно, является формулой алгебры высказываний. Поэтому логическое значение составного высказывания $H(A_1(a_1), \dots, A_n(a_n))$ может быть найдено на основании теоремы 2.2, в результате чего последнее равенство примет вид

$$H(\lambda(A_1(a_1)), \dots, \lambda(A_n(a_n))) = 1. \quad (4)$$

Для элементов $a_1, \dots, a_n$ множества M выберем такие подмножества $M_{\alpha_1}, \dots, M_{\alpha_n}$ этого множества, что $a_1 \in M_{\alpha_1}, \dots, a_n \in M_{\alpha_n}$. Тогда, по определению предикатов $A'_i(x_i)$ (см. (3)), $\lambda(A'_i(a_i)) = \lambda(A'_i(M_{\alpha_i}))$, $i = 1, \dots, n$.

Подставим эти значения в (4). Получим

$$H(\lambda(A'_1(M_{\alpha_1})), \dots, \lambda(A'_n(M_{\alpha_n}))) = 1,$$

откуда, на основании теоремы 2.2, заключаем, что

$$\lambda[H(A_1'(M_{\alpha_1}), \dots, A_n'(M_{\alpha_n}))] = 1.$$

Последнее означает выполнимость предиката $H(A_1'(x_1), \dots, A_n'(x_n))$ на m -элементном множестве $\mathbf{M}$ для предметов $M_{\alpha_1}, \dots, M_{\alpha_n}$ и, значит, выполнимость формулы $H(P_1(x_1), \dots, P_n(x_n))$, т.е. формулы $F(P_1, \dots, P_n)$ на этом же множестве для тех же предметов.

Предположим теперь, что для всякой формулы $F(P_1, \dots, P_n)$ с числом кванторов $< k$ из выполнимости ее на множестве M для предикатов $A_1(x_1), \dots, A_n(x_n)$ и предметов $a_1, \dots, a_n \in M$ следует выполнимость ее на множестве $\mathbf{M}$ для предикатов $A_1'(x_1), \dots, A_n'(x_n)$ и предметов $M_{\alpha_1}, \dots, M_{\alpha_n}$, таких, что $a_1 \in M_{\alpha_1}, \dots, a_n \in M_{\alpha_n}$.

Наконец рассмотрим произвольную формулу $F(P_1, \dots, P_n)$ с числом кванторов $k \leq n$, т.е.

$$F(P_1, \dots, P_n) \equiv (K_1 x_1) \dots (K_k x_k) (H(P_1, \dots, P_n)). \quad (5)$$

Допустим, что формула (5) выполняется на множестве M для предикатов $A_1(x_1), \dots, A_n(x_n)$ и предметов $a_{k+1}, \dots, a_n \in M$. Учитывая предположение индукции, покажем, что она выполняется на m -элементном множестве $\mathbf{M}$ для предикатов $A_1'(x_1), \dots, A_n'(x_n)$ и предметов $M_{\alpha_1}, \dots, M_{\alpha_n}$ таких, что $a_1 \in M_{\alpha_1}, \dots, a_n \in M_{\alpha_n}$. Здесь нужно рассмотреть две возможности для квантора $K_1 x_1$.

а) Квантор $K_1 x_1$ есть $\forall x_1$. Тогда выполнимость формулы (5) для предикатов $A_1(x_1), \dots, A_n(x_n)$ и предметов $a_{k+1}, \dots, a_n \in M$ означает, что при соответствующей подстановке она превращается в выполнимый предикат $(\forall x_1)(K_2 x_2) \dots (K_k x_k) (H(A_1(x_1), A_2(x_2), \dots, A_n(x_n)))$, причем $\lambda[(\forall x_1)(K_2 x_2) \dots (K_k x_k) (H(A_1(x_1), \dots, A_k(x_k), A_{k+1}(a_{k+1}), \dots, A_n(a_n)))] = 1$. Далее, по определению 20.1 квантора общности, из последнего соотношения следует, что для любого $a \in M$

$$\lambda[(K_2 x_2) \dots (K_k x_k) (H(A_1(a), A_2(x_2), \dots, A_k(x_k), A_{k+1}(a_{k+1}), \dots, A_n(a_n)))] = 1. \quad (6)$$

Равенство (6) означает, что формула

$$(K_2 x_2) \dots (K_k x_k) (H(P_1, P_2, \dots, P_n)) \quad (7)$$

выполнима на множестве M для предикатов $A_1(x_1), A_2(x_2), \dots, A_n(x_n)$ и предметов $a, a_{k+1}, \dots, a_n \in M$. Но формула (7) имеет $k-1$ кванторов. Поэтому на основании предположения индукции заключаем, что она выполняется на множестве $\mathbf{M}$ для предикатов $A_1'(x_1), A_2'(x_2), \dots, A_n'(x_n)$ и предметов $M_{\alpha}, M_{\alpha_{k+1}}, \dots, M_{\alpha_n}$, таких, что $a \in M_{\alpha}, a_{k+1} \in M_{\alpha_{k+1}}, \dots, a_n \in M_{\alpha_n}$, т.е.

$$\lambda[(K_2 x_2) \dots (K_k x_k) (H(A_1'(M_{\alpha}), A_2'(x_2), \dots, A_k'(x_k), A_{k+1}'(M_{\alpha_{k+1}}), \dots, A_n(M_{\alpha_n})))] = 1. \quad (8)$$

Соотношение (6) выполняется для любого $a \in M$, поэтому соотношение (8) будет выполняться для любого $M_\alpha \in \mathbf{M}$. Последнее означает, по определению квантора общности, что $\lambda[(\forall x_1)(K_2x_2) \dots (K_kx_k)(H(A_1'(x_1), A_2'(x_2), \dots, A_k'(x_k), A_{k+1}'(M_{\alpha_{k+1}}), \dots, A_n'(M_{\alpha_n})))] = 1$. Это равенство говорит о том, что формула $(\forall x_1)(K_2x_2) \dots (K_kx_k)(H(P_1, P_2, \dots, P_n))$ выполнима на множестве $\mathbf{M}$ для предикатов $A_1'(x_1), \dots, A_n'(x_n)$ и предметов $M_{\alpha_{k+1}}, \dots, M_{\alpha_n} \in \mathbf{M}$.

б) Квантор K_1x_1 есть $\exists x_1$. Тогда выполнимость формулы (5) для предикатов $A_1(x_1), \dots, A_n(x_n)$ и предметов $a_{k+1}, \dots, a_n \in M$ означает, что при соответствующей подстановке она превращается в выполнимый предикат

$$(\exists x_1)(K_2x_2) \dots (K_kx_k)(H(A_1(x_1), A_2(x_2), \dots, A_n(x_n))), \text{ причем} \\ \lambda[(\exists x_1)(K_2x_2) \dots (K_kx_k)(H(A_1(x_1), \dots, A_k(x_k), A_{k+1}(a_{k+1}), \dots, A_n(a_n))))] = 1.$$

Далее, по определению 20.3 квантора существования, из последнего соотношения получим, что

$$\lambda[(K_2x_2) \dots (K_kx_k)(H(A_1(a), A_2(x_2), \dots, A_k(x_k), \\ A_{k+1}(a_{k+1}), \dots, A_n(a_n))))] = 1$$

для некоторого $a \in M$. Полученное равенство означает, что формула (7) выполнима на множестве M для предикатов $A_1(x_1), A_2(x_2), \dots, A_n(x_n)$ и предметов $a, a_{k+1}, \dots, a_n \in M$. Но формула (7) имеет $k-1$ кванторов, поэтому на основании предположения индукции заключаем, что она выполняется на множестве $\mathbf{M}$ для предикатов $A_1'(x_1), A_2'(x_2), \dots, A_n'(x_n)$ и предметов $M_\alpha, M_{\alpha_{k+1}}, \dots, M_{\alpha_n} \in \mathbf{M}$, таких, что $a \in M_\alpha, a_{k+1} \in M_{\alpha_{k+1}}, \dots, a_n \in M_{\alpha_n}$, т.е. справедливо соотношение (8). По определению квантора существования, оно приводит к равенству $\lambda[(\exists x_1)(K_2x_2) \dots (K_kx_k)(H(A_1'(x_1), A_2'(x_2), \dots, A_k'(x_k), A_{k+1}'(M_{\alpha_{k+1}}), \dots, A_n'(M_{\alpha_n}))))] = 1$, показывающему, что формула $(\exists x_1)(K_2x_2) \dots (K_kx_k)(H(P_1, P_2, \dots, P_n))$ выполнима на множестве $\mathbf{M}$ для предикатов $A_1'(x_1), A_2'(x_2), \dots, A_n'(x_n)$ и предметов $M_\alpha, M_{\alpha_{k+1}}, \dots, M_{\alpha_n} \in \mathbf{M}$, таких, что $a \in M_\alpha, a_{k+1} \in M_{\alpha_{k+1}}, \dots, a_n \in M_{\alpha_n}$.

Итак, какое бы количество кванторов ни имела формула $\bar{F}$, она будет выполняться на m -элементном множестве $\mathbf{M}$, где $m \leq 2^n$. Теорема доказана. $\square$

Следствие 23.3. Если замкнутая формула $F(P_1, P_2, \dots, P_n)$, в которую входят только одноместные предикатные переменные $P_1, P_2, \dots, P_n$, тождественно истинна на множестве из 2^n элементов, то она общезначима.

Доказательство. Допустим, что рассматриваемая формула $F(P_1, P_2, \dots, P_n)$ не общезначима. Тогда ее отрицание $\neg F(P_1, P_2, \dots, P_n)$ есть выполнимая формула. Следовательно, по доказанной теореме, эта формула выполнима на конечном множестве из m элементов, причем $m \leq 2^n$. Отсюда, на основании теоремы 23.1, заключаем, что она выполнима на множестве из 2^n элементов. Значит, на таком множестве исходная формула $F(P_1, P_2, \dots, P_n)$ не

тождественно истинна, что противоречит условию. Следствие доказано. $\square$

Таким образом, задача об общезначимости формулы, содержащей лишь одноместные предикатные переменные, сводится к задаче о тождественной истинности этой формулы на конечном множестве. В свою очередь, во втором пункте настоящего параграфа показано, как последняя задача решается путем сведения ее к задаче о тождественной истинности некоторой формулы алгебры высказываний, т.е. к задаче, имеющей алгоритмическое решение. Следовательно, и наша исходная проблема разрешения общезначимости для класса формул логики предикатов, содержащих только одноместные предикаты, разрешима.

Проблема разрешения общезначимости и мощность множества, на котором рассматривается формула. Обратимся к проблеме общезначимости. *Теорема Лёвенгейма*, отмеченная выше, применительно к проблеме разрешения общезначимости звучит так: *если формула тождественно истинна в счетно-бесконечной области, то она общезначима*. Но снова, как и для проблемы выполнимости формул, переход от (счетно) бесконечных множеств к конечным или обратно является качественным. Следующий пример показывает, что, в отличие от проблемы выполнимости, разрешимость проблемы общезначимости на некотором множестве не влечет ее разрешимости на множестве, объемлющем данное.

Пример 23.4. Докажем, что следующая формула тождественно истинна на любом конечном множестве, но не является таковой на бесконечном множестве:

$$(\forall x, y, z)[R(x, x) \wedge (R(x, z) \rightarrow (R(x, y) \vee R(y, z)))] \rightarrow \\ \rightarrow (\exists x)(\forall y)(R(x, y)).$$

Во-первых, отметим, что предикат « $x \leq y$ », заданный на бесконечном множестве Z , превращает данную формулу в ложное высказывание:

$$(\forall x, y, z)[x \leq x \wedge (x \leq z \rightarrow (x \leq y \vee y \leq z))] \rightarrow (\exists x)(\forall y)(x \leq y),$$

ибо посылка этой импликации истинна, а следствие ложно.

Во-вторых, докажем, что данная формула тождественно истинна на любом конечном множестве. Доказательство будем вести индукцией по числу элементов в множестве. Для $M = \{a_1\}$ это очевидно (убедитесь самостоятельно). Если $M = \{a_1, a_2\}$, то истинными будут утверждения $R(a_1, a_1)$, $R(a_2, a_2)$ и $R(a_1, a_1) \rightarrow (R(a_1, a_2) \vee R(a_2, a_1))$, а значит, и дизъюнкция $R(a_1, a_2) \vee R(a_2, a_1)$. Если при этом истинно $R(a_1, a_2)$, то истинно $(\forall y)(R(a_1, y))$, т.е. истинно заключение $(\exists x)(\forall y)(R(x, y))$ импликации данной формулы и вся данная формула. Аналогично, если истинно $R(a_2, a_1)$, то истинно $(\forall y)(R(a_2, y))$ и снова истинна вся данная формула.

Предположим теперь, что данная формула тождественно истинна на всяком конечном множестве, содержащем не больше, чем n элементов. Покажем тогда, что она будет тождественно истинна и на любом $(n + 1)$ -элементном множестве. Пусть $M = \{a_1, \dots, a_n, a_{n+1}\}$. В силу тождественной истинности данной формулы на n -элементном подмножестве $M' = \{a_1, \dots, a_n\}$ и предположения истинности на M' посылки данной формулы, имеем истинные высказывания: $(\forall x)(R(x, x))$ и $(\forall x)(R(x, x) \rightarrow (\forall y)(R(x, y) \vee R(y, x)))$. Тогда истинно заключение $(\exists x)(\forall y)(R(x, y))$. Не нарушая общности, можно считать, что таким x будет элемент a_1 , т.е. $(\forall y)(R(a_1, y))$, т.е. истинны все утверждения $R(a_1, a_2), \dots, R(a_1, a_n)$.

Мы хотим доказать, что данная формула истинна на $(n + 1)$ -элементном множестве $M = \{a_1, \dots, a_n, a_{n+1}\}$. Для этого нужно показать, что на нем в предположении истинности посылки данной формулы верно ее заключение $(\exists x)(\forall y)(R(x, y))$. Если верно $R(a_1, a_{n+1})$, то утверждение доказано. Если же $R(a_1, a_{n+1})$ неверно, то, в силу истинности дизъюнкции $R(a_1, a_{n+1}) \vee R(a_{n+1}, a_1)$, заключаем, что истинно $R(a_{n+1}, a_1)$.

Далее, в силу истинности в M посылки $(\forall x, y, z)(R(x, z) \rightarrow \rightarrow (R(x, y) \vee R(y, z)))$ и утверждений $R(a_1, a_2), \dots, R(a_1, a_n)$, приходим к истинности всех следующих дизъюнкций: $R(a_1, a_{n+1}) \vee \vee R(a_{n+1}, a_2), \dots, R(a_1, a_{n+1}) \vee R(a_{n+1}, a_n)$. Поскольку первый член каждой дизъюнкции ложен, то истинны все вторые члены $R(a_{n+1}, a_2), \dots, R(a_{n+1}, a_n)$. Учитывая еще и истинность $R(a_{n+1}, a_1)$ и, кроме того, $R(a_{n+1}, a_{n+1})$, приходим к истинности утверждения $(\forall y)(R(a_{n+1}, y))$ на M . Это означает истинность на M заключения данной формулы $(\exists x)(\forall y)(R(x, y))$ и всей данной формулы.

Ситуация с проблемой разрешимости общезначимости, отмеченная в рассмотренном примере, имеет место не только при переходе от конечного множества к бесконечному, но и при переходе от одного конечного к другому конечному, содержащему большее количество элементов. Соответствующий пример формулы, тождественно истинной в области из трех элементов и не являющейся таковой в области из четырех элементов, приведен в Задачнике, № 9.57.

Решение проблемы для $\forall$ -формул и $\exists$ -формул. В заключение покажем, как решается проблема разрешения общезначимости еще для двух классов формул логики предикатов — $\forall$ -формул и $\exists$ -формул: и в этих случаях она сводится к тождественной истинности формул на конечных множествах. Под $\forall$ -формулой понимается формула $(\forall x_1)(\forall x_2) \dots (\forall x_n)(F(P_1, P_2, \dots, P_k))$, у которой в предваренной нормальной форме кванторная часть содержит только кванторы общности, а под $\exists$ -формулой понимается формула $(\exists x_1)(\exists x_2) \dots (\exists x_n)(F(P_1, P_2, \dots, P_k))$, у которой в предваренной нормальной форме кванторная часть содержит только кванторы существования, причем $P_i = P_i(x_1, x_2, \dots, x_n)$, $i = 1, 2, \dots, k$.

Теорема 23.5. $\forall$ -формула $(\forall x_1) \dots (\forall x_n)(F(P_1, \dots, P_k))$ общезначима тогда и только тогда, когда она тождественно истинна на n -элементном множестве.

Доказательство. В самом деле, пусть данная формула тождественно истинна на некотором n -элементном множестве. Тогда ясно, что она тождественно истинна на любом n -элементном множестве (это следует из наличия взаимно-однозначного отображения этих множеств друг на друга). Тогда на всяком n -элементном множестве будет тождественно истинна и формула $F(P_1, \dots, P_k)$. Рассмотрим теперь интерпретацию на произвольном множестве: $P_1 = A_1, \dots, P_k = A_k$. Получим конкретный предикат $F(A_1, \dots, A_k)$, зависящий от n переменных. Подставляя вместо них конкретные предметы, мы фактически имеем дело с n -элементным множеством, на котором этот предикат тождественно истинен. Значит, он будет тождественно истинен и на всем данном множестве. Значит, формула $F(P_1, \dots, P_k)$ тождественно истинна на любом множестве, а вместе с ней тождественно истинна на любом множестве, т. е. общезначима, и формула $(\forall x_1) \dots (\forall x_n)(F(P_1, \dots, P_k))$. $\square$

Теорема 23.6. $\exists$ -формула $(\exists x_1) \dots (\exists x_n)(F(P_1, \dots, P_k))$ общезначима тогда и только тогда, когда она тождественно истинна на одноэлементном множестве.

Доказательство этой теоремы аналогично доказательству предыдущей теоремы. Проведите его самостоятельно.

Итак, рассмотрения настоящего параграфа красноречиво демонстрируют, что в то время как в алгебре высказываний проблемы разрешимости выполнимости и общезначимости формул решались сравнительно легко, в логике предикатов они представляют собой весьма трудные и, в целом, отнюдь не решенные до конца проблемы.

§ 24. Применение логики предикатов к логико-математической практике

Некоторые современные математики и методисты склонны относить математику как науку и как учебный предмет к разряду гуманитарных дисциплин, поскольку она изучает язык, на котором, по образному выражению Галилея, написана грандиозная книга — Вселенная. Конечно, здесь речь идет о специфическом языке — языке математическом. Но математика, развиваясь, довела свой язык до такого совершенства и такой выразительной силы, что он вплотную приблизился по своим информационно-выразительным свойствам к общечеловеческому языку. Такого совершенства математический язык достиг, когда математикой был разработан язык математической логики и прежде всего язык логики предикатов. Язык логики предикатов — это, по существу, открытое вторжение математики в общечеловеческий язык,

математизация общечеловеческого языка с целью более точного, более адекватного его использования в первую очередь в самой математике. В языке логики предикатов соединились логика мышления, без которой немислим общечеловеческий язык, и математика. В человеческий язык вошла математика, а математический язык стал почти неотличим от общечеловеческого, слился с ним.

Поэтому умение грамотно оперировать языком логики предикатов (читай — языком математической логики) является основой современной логической культуры вообще. В связи с этим в настоящем параграфе мы уделим немало внимания записи на языке логики предикатов различных математических предложений, что будет способствовать более глубокому пониманию их структуры.

Практически важнейшей сферой применения логики предикатов к логико-математической практике является сфера построения доказательств различных теорем, основывающаяся на теории логического следования. Более сложное строение формул логики предикатов, по сравнению с формулами логики высказываний, дает возможность проводить более сложные доказательства и в результате получать более тонкие заключения. В настоящем параграфе мы попытаемся на простейших примерах проиллюстрировать суть теории логического вывода и ее применение.

Будут рассмотрены также приложения логики предикатов к теории множеств, к анализу аристотелевой силлогистики.

Запись на языке логики предикатов различных предложений. С помощью кванторной символики удобно записывать формулировки различных определений и теорем. В процессе такой записи приходится осмысливать данное предложение, отчетливо выделять в нем посылки и следствие (если это теорема), очерчивать более широкий круг понятий и четко выделять ограничивающее условие (если это определение). Одним словом, перевод расплывчатой словесной формулировки на строгий, не допускающий противоречивых толкований язык логики предикатов способствует четкости и ясности мышления. Рассмотрим некоторые примеры.

Пример 24.1. Определение предела последовательности «Число a называется пределом последовательности $\{a_n\}$, если для всякого положительного числа $\varepsilon > 0$ существует такое натуральное число n_0 , что для всякого натурального n , большего n_0 , $|a_n - a| < \varepsilon$ » на языке логики предикатов записывается так:

$$a = \lim a_n \stackrel{\text{опр.}}{\Leftrightarrow} (\forall \varepsilon)[\varepsilon > 0 \rightarrow (\exists n_0)(n_0 \in N \wedge (\forall n)(n > n_0 \rightarrow |a_n - a| < \varepsilon))].$$

Используя символику ограниченных кванторов (см. § 20), это определение можно записать компактнее:

$$a = \lim a_n \stackrel{\text{опр.}}{\Leftrightarrow} (\forall \varepsilon > 0)(\exists n_0 \in N)(\forall n > n_0)(|a_n - a| < \varepsilon).$$

Нередко требуется доказать, что некоторое число a не является пределом последовательности $\{a_n\}$, т. е. $a \neq \lim a_n$. Для доказательства нужно построить утверждение, являющееся отрицанием сформулированного определения. Поможет в этом логика предикатов. Используя равносильности логики предикатов, преобразуем отрицание исходной формулы к приведенному виду:

$$\begin{aligned} & \neg(\forall \varepsilon)[\varepsilon > 0 \rightarrow (\exists n_0)(n_0 \in N \wedge (\forall n)(n > n_0 \rightarrow |a_n - a| < \varepsilon))] \equiv \\ & \equiv (\exists \varepsilon) \neg[\neg(\varepsilon > 0) \vee (\exists n_0)(n_0 \in N \wedge (\forall n)(n > n_0 \rightarrow |a_n - a| < \varepsilon))] \equiv \\ & \equiv (\exists \varepsilon)[(\varepsilon > 0) \wedge (\forall n_0)(\neg(n_0 \in N) \vee \neg(\forall n)(\neg(n > n_0) \vee |a_n - a| < \varepsilon))] \equiv \\ & \equiv (\exists \varepsilon)[(\varepsilon > 0) \wedge (\forall n_0)(\neg(n_0 \in N) \vee (\exists n)(n > n_0 \wedge \neg(|a_n - a| < \varepsilon))] \equiv \\ & \equiv (\exists \varepsilon)[(\varepsilon > 0) \wedge (\forall n_0)(n_0 \in N \rightarrow (\exists n)(n > n_0 \wedge |a_n - a| \geq \varepsilon))]. \end{aligned}$$

Полученное утверждение можно записать компактнее, используя символику ограниченных кванторов:

$$(\exists \varepsilon > 0)(\forall n_0 \in N)(\exists n > n_0)(|a_n - a| \geq \varepsilon).$$

Таким образом, утверждение «Число a не является пределом последовательности $\{a_n\}$ » раскрывается так: «Существует такое положительное число ε , что для всякого натурального числа n_0 найдется такое натуральное $n > n_0$, что $|a_n - a| \geq \varepsilon$ ».

Несходимость последовательности $\{a_n\}$ означает, что никакое число не является ее пределом, т. е. $(\forall a)(a \neq \lim a_n)$. Это вместе с полученным утверждением дает

$$(\forall a)(\exists \varepsilon > 0)(\forall n_0 \in N)(\exists n > n_0)(|a_n - a| \geq \varepsilon).$$

Пример 24.2. Запишем на языке логики предикатов определение простого числа: «Натуральное число x называется простым, если оно не равно 1 и при всяком разложении его в произведение двух натуральных чисел одно из них оказывается равным 1 или x »:

$$\neg(x = 1) \wedge (\forall u)(\forall v)(x = u \cdot v \rightarrow (u = 1) \vee (u = x)).$$

Отрицание этого утверждения — утверждение того, что число x составное, записывается следующим образом:

$$(x = 1) \vee (\exists u)(\exists v)(x = u \cdot v \wedge u \neq 1 \wedge u \neq x).$$

Предлагается самостоятельно разобраться в его составлении.

Пример 24.3. Определение «Точка x_0 из области определения функции f называется точкой локального максимума функции f , если существует такая δ -окрестность данной точки, что для всех x из этой окрестности $f(x) < f(x_0)$ » на языке логики предикатов запишется так:

$$x_0 \in D_f \wedge (\exists \delta > 0)(\forall x)(|x - x_0| < \delta \rightarrow f(x) < f(x_0)).$$

Запишите самостоятельно отрицание данного утверждения.

Сравнение логики предикатов и логики высказываний. В начале § 21 уже отмечалось, что язык и логика алгебры предикатов тоньше и точнее отражают процессы мышления, нежели язык и логика алгебры высказываний. Приведем два примера, подтверждающих эту мысль.

Пример 24.4. Рассмотрим высказывание «Каждый человек имеет мать». Если на языке алгебры высказываний формулировка данного высказывания сведется лишь к обозначению его некоторой буквой, скажем A , то на языке логики предикатов возможна формализация, учитывающая внутреннюю (субъектно-предикатную) структуру этого высказывания. Действительно, пусть $P(x, y)$ — двухместный предикат « x есть мать y », определенный на множестве всех людей. Тогда данному высказыванию отвечает формула логики предикатов $(\forall y)(\exists x)(P(x, y))$. Рассматриваемое высказывание можно перевести на язык логики предикатов и иначе. Если ввести еще одноместный предикат $Q(x)$: « x есть человек», определенный на произвольном множестве, то высказывание запишется так: $(\forall y)(Q(y) \rightarrow (\exists x)(Q(x) \wedge P(x, y)))$.

Пример 24.5. Этот пример еще более наглядно демонстрирует выразительные возможности языка логики предикатов по сравнению с языком логики высказываний. Рассмотрим два высказывания: «В Москве живет женщина, имеющая брата в Петербурге» и «В Петербурге живет мужчина, имеющий сестру в Москве». Каждое из данных утверждений следует из другого, т.е. они равносильны. Спрашивается, можно ли выразить эту равносильность на языке алгебры высказываний, на языке логики предикатов? Оказывается второе возможно, а первое нет.

В самом деле, как мы могли бы формализовать данные высказывания на языке алгебры высказываний? Можно обозначить первое высказывание через A , второе — через B . Ясно, что ни о какой равносильности формул A и B говорить не приходится. Можно расчленить данные высказывания на более простые: A_1 — «Женщина живет в Москве»; A_2 — «Женщина имеет брата в Петербурге»; B_1 — «Мужчина живет в Петербурге»; B_2 — «Мужчина имеет сестру в Москве». Тогда первое исходное высказывание есть конъюнкция $A_1 \wedge A_2$, а второе — $B_1 \wedge B_2$. Но и эти две формулы алгебры высказываний не следуют одна из другой.

В отличие от алгебры высказываний, формализация на языке логики предикатов позволяет обнаружить равносильность двух данных высказываний. Действительно, введем предикаты, определенные на множестве людей: $P_1(x)$ — « x — женщина»; $P_2(x)$ — « x живет в Москве»; $Q_1(y)$ — « y — мужчина»; $Q_2(y)$ — « y живет в Петербурге»; $S(x, y)$ — « x есть сестра y ». Тогда высказыванию «В Москве живет женщина, имеющая брата в Петербурге» соответствует формула логики предикатов

$$(\exists x)[P_1(x) \wedge P_2(x) \wedge (\exists y)(Q_1(y) \wedge Q_2(y) \wedge S(x, y))],$$

а высказыванию «В Петербурге живет мужчина, имеющий сестру в Москве» — формула

$$(\exists y)[Q_1(y) \wedge Q_2(y) \wedge (\exists x)(P_1(x) \wedge P_2(x) \wedge S(x, y))].$$

Покажем, что полученные формулы равносильны, для чего первую из них равносильными преобразованиями сведем ко второй (предлагается обнаружить те равносильности логики предикатов, которые используются на каждом шаге преобразований):

$$\begin{aligned} & (\exists x)[P_1(x) \wedge P_2(x) \wedge (\exists y)(Q_1(y) \wedge Q_2(y) \wedge S(x, y))] \equiv \\ & \equiv (\exists x)(\exists y)[P_1(x) \wedge P_2(x) \wedge Q_1(y) \wedge Q_2(y) \wedge S(x, y)] \equiv \\ & \equiv (\exists y)(\exists x)[Q_1(y) \wedge Q_2(y) \wedge P_1(x) \wedge P_2(x) \wedge S(x, y)] \equiv \\ & \equiv (\exists y)[Q_1(y) \wedge Q_2(y) \wedge (\exists x)(P_1(x) \wedge P_2(x) \wedge S(x, y))]. \end{aligned}$$

Строение математических теорем. Остановимся на формах теорем четырех видов, выделенных еще в аристотелевской логике, основоположником которой был один из наиболее разносторонних мыслителей Древней Греции Аристотель (384 — 322 гг. до н. э.), и названных категорическими суждениями. Многие математические теоремы имеют именно такой вид. Логика предикатов позволит проанализировать их строение, сравнить между собой, и этот анализ будет более тонким, нежели анализ строения теорем, проведенный в алгебре высказываний. (Впрочем можно заметить, что в алгебре высказываний этот анализ проходил несколько в ином аспекте, и оба анализа скорее дополняют друг друга.)

Величайшая заслуга Аристотеля в области логики состоит в том, что он впервые систематизировал и подверг анализу с некоторой формальной точки зрения приемы рассуждений, уже практически широко применявшиеся его современниками, но до него оставшиеся еще теоретически неосознанными, несформулированными. Он показал, что правильное рассуждение можно свести к систематическому применению небольшого числа неизменных правил, независимых от частной природы объектов, относительно которых происходит рассуждение. Тем самым Аристотель применил такие подходы к исследованию рассуждений, которые сделали логику наукой. С точки зрения современной формальной (математической) логики этот особый вид логических рассуждений, который подробно исследовал Аристотель и который получил название «силлогического», представляет собой небольшую и довольно элементарную часть, относящуюся к логике предикатов, причем — к логике одноместных предикатов. В своем учении о силлогизме Аристотель выясняет общие закономерности, при которых из двух высказываний-посылок, имеющих вполне определенную логическую структуру (выражаемую специальными формулами логики предикатов, содержащими лишь одноместные предикатные переменные), определенное заключение с необходимостью либо следует, либо не следует. Современная форма силлогистики в ее

окончательном виде конечно же еще не содержится в трудах самого Аристотеля, она является результатом работы его многочисленных комментаторов и последователей — древнегреческих, древнеримских, арабских и средневековых логиков.

Аристотель, проанализировав строение простых высказываний (или, как он говорил, «категорических суждений»), пришел к выводу, что содержание любого из них может быть сведено к утверждению о наличии или отсутствии у предметов определенных свойств. При этом такие утверждения могут относиться не только к отдельным предметам, но и к классам предметов. Высказывание, в котором утверждается, что конкретный предмет обладает или не обладает определенным свойством, называется *единичным* (соответственно *единичноутвердительным* или *единичноотрицательным*). Например, высказывание «Число 10 четное» является единичноутвердительным. Его содержание сводится к утверждению о наличии у конкретного числа 10 свойства делимости на 2.

Высказывание, в котором утверждается, что все предметы класса обладают или не обладают определенным свойством, называется *общим* (соответственно *общеутвердительным* или *общеотрицательным*). Например, высказывание «Все металлы тонут в воде» общеутвердительное, а высказывание «Все простые числа не являются четными» общеотрицательное.

Высказывание, в котором утверждается, что некоторые предметы класса обладают или не обладают определенным свойством, называется *частным* (соответственно *частноутвердительным* или *частноотрицательным*). Например, высказывание «Некоторые реки впадают в озеро Байкал» является частноутвердительным, а высказывание «Некоторые прямоугольные треугольники не являются равнобедренными» — частноотрицательным.

Таким образом, по Аристотелю, все простые высказывания делятся на следующие шесть типов: единичноутвердительные, единичноотрицательные, общеутвердительные, общеотрицательные, частноутвердительные, частноотрицательные. Первые два типа высказываний есть высказывания о конкретных предметах, последние четыре — о классах предметов.

По традиции, также восходящей к Аристотелю, типы простых высказываний, относящихся к классам предметов, обозначаются гласными буквами латинского алфавита: *A* — общеутвердительные, *E* — общеотрицательные, *I* — частноутвердительные, *O* — частноотрицательные. (Эти буквы соответствуют латинским словам: *affirmo* — «утверждаю», *nego* — «отрицаю».) Далее класс предметов обозначается буквой *S*, свойство — буквой *P*. При этом *S* называется субъектом, а *P* — предикатом.

Таким образом, указанные выше четыре типа простых высказываний, относящихся к классам предметов, имеют следующую общелогическую форму:

А (общеутвердительное суждение): «Все предметы класса S обладают свойством P ». («Все S суть P ».) Символически: SaP ;

Е (общеотрицательное суждение): «Ни один предмет класса S не обладает свойством P ». («Ни один S не есть P ».) Символически: SeP ;

И (частноутвердительное суждение): «Некоторые предметы класса S обладают свойством P ». («Некоторые S суть P ».) Символически: SiP ;

О (частноотрицательное суждение): «Некоторые предметы класса S не обладают свойством P ». («Некоторые S не суть P ».) Символически: SoP .

Исходя из описанного подхода к простым высказываниям анализ их строения состоит в выявлении их субъектно-предикатной структуры, т.е. в выявлении в высказывании субъекта и предиката и фиксировании способа связи между ними (по типу A , E , I , O).

Рассмотрим более подробно эти виды суждений.

Общеутвердительное суждение: «Все S суть P ». Примерами математических теорем, имеющих такое строение, являются следующие: «Все прямоугольники — параллелограммы», «Все гомотетии суть преобразования подобия», «Все дифференцируемые функции непрерывны», «Все поля суть кольца», «Все сферы — тела вращения». Можно указать немало суждений нематематического характера, имеющих такое строение: «Все люди смертны», «Все змеи — пресмыкающиеся», «Все планеты — спутники Солнца».

Суждение «Все S суть P » в терминах логики предикатов понимается так: каков бы ни был объект x , если он обладает свойством S (т.е. $S(x)$ истинно), то он обладает также свойством P (т.е. $P(x)$ истинно). Это утверждение на языке логики предикатов выглядит следующим образом:

$$A: \quad (\forall x)(S(x) \rightarrow P(x)). \quad (1)$$

(Напомним, что утверждения такого типа рассматривались в § 20, в материале об ограниченных кванторах: утверждение представляло собой развернутую запись ограниченного квантора общности.)

Логика предикатов дает возможность представить суждение A в несколько ином виде с использованием квантора существования. Для этого преобразуем формулу (1) равносильным образом, используя равносильности (получающиеся на основе тавтологий) теоремы 21.9, б и теоремы 4.4 а, с, у:

$$(\forall x)(S(x) \rightarrow P(x)) \equiv (\forall x)(\neg \neg (\neg S(x) \vee P(x))) \equiv \neg (\exists x)(\neg (\neg S(x) \vee P(x))) \equiv \neg (\exists x)(\neg \neg S(x) \wedge \neg P(x)) \equiv \neg (\exists x)(S(x) \wedge \neg P(x)).$$

В этом виде суждение A можно сформулировать так: «Неверно, что некоторые S не суть P ».

Отметим, что, как правило, не говорят: «Все S суть P », если известно, что объектов, удовлетворяющих свойству S , не существует. Обычно под этим суждением мы понимаем следующее: «Существует объект, удовлетворяющий S , и все S суть P », или в переводе на язык логики предикатов оно выглядит так:

$$(\exists x)(S(x)) \wedge (\forall x)(S(x) \rightarrow P(x)). \quad (1')$$

При этом возможно и иное понимание исходного суждения, а именно: «Если существует объект, удовлетворяющий свойству S , то все S суть P », переводимое на язык логики предикатов следующим образом:

$$(\exists x)(S(x) \rightarrow (\forall x)(S(x) \rightarrow P(x))). \quad (1'')$$

(Проверьте самостоятельно, что формула $(1'')$ равносильна формуле (1) , и поэтому данное толкование общеутвердительного суждения совпадает с первоначальным его пониманием.)

Всем этим вариантам предпочтем (1) по той главной причине, что данный перевод, во-первых, проще, чем $(1')$ и $(1'')$, а во-вторых, при теоретико-множественном толковании суждения «Все S суть P » он позволяет заключить, что множество S всех объектов x , удовлетворяющих свойству $S(x)$, является подмножеством множества P объектов, удовлетворяющих свойству $P(x)$, т.е. $S \subseteq P$.

Отметим также, что в повседневной речи слово «все» в общеутвердительных суждениях порой опускают, так что, например, эквивалентом фразы «Все люди смертны» является вариант «Люди смертны».

Общеотрицательное суждение: «Никакое S не есть P ». Вот примеры математических теорем, имеющих такое строение: «Никакой эллипс не есть алгебраическая линия первого порядка», «Никакая осевая симметрия на плоскости не есть движение первого рода», «Никакой треугольник не является окружностью», «Никакой числовой ряд, у которого предел общего члена не равен нулю, не сходится». Вот примеры нематематических суждений такого типа: «Никакие змеи не есть птицы», «Никакие камни не разговаривают».

Смысл общеотрицательного суждения: каков бы ни был объект x , если он обладает свойством S (т.е. $S(x)$ истинно), он не обладает свойством P (т.е. $P(x)$ ложно). На языке логики предикатов это выражается так:

$$E: \quad (\forall x)(S(x) \rightarrow \neg P(x)). \quad (2)$$

Другими словами, общеотрицательное утверждение читается: «Все S суть не P ». Можно записать выражение (2) и в виде ограниченного квантора общности: $(\forall x)(S(x) \rightarrow (\neg P(x)))$.

Логика предикатов дает возможность представить суждение E в несколько ином виде, с использованием квантора существования. Для этого формулу E необходимо преобразовать равносильным образом, используя те же равносильности, что и в случае преобразования общеутвердительного суждения:

$$(\forall x)(S(x) \rightarrow \neg P(x)) \equiv (\forall x)(\neg(\neg S(x) \vee \neg P(x))) \equiv \\ \equiv \neg(\exists x)(\neg(\neg S(x) \vee \neg P(x))) \equiv \neg(\exists x)(S(x) \wedge P(x)).$$

В этом виде суждение E формулируется так: «Неверно, что некоторые S суть P ».

Отметим, что при теоретико-множественном толковании общеотрицательного суждения «Все S суть не P » запись (2) позволяет заключить, что множество S всех объектов x , удовлетворяющих свойству $S(x)$, включается в множество $\bar{P}$ всех объектов, не удовлетворяющих свойству $P(x)$, являющееся дополнением множества P , т.е. $S \subseteq \bar{P}$.

Частноутвердительное суждение: «Некоторые S суть P ». Примерами математических утверждений с такими строениями служат следующие: «Некоторые гомотетии суть движения», «Некоторые функции — периодические», «Некоторые параллелограммы могут быть вписаны в окружность», «Некоторые простые числа четны». Приведем примеры нематематических суждений, имеющих такое строение: «Некоторые люди взошли на Эверест», «Некоторые змеи ядовиты» и т.д.

Частноутвердительному суждению придается следующий смысл: существует такой объект x , обладающий свойством $S(x)$, который также обладает и свойством $P(x)$. Тогда ему соответствует следующая формула логики предикатов:

$$I: (\exists x)(S(x) \wedge P(x)). \quad (3)$$

(Напомним, что это утверждение представляет собой развернутую запись ограниченного квантора существования, см. § 20.)

Снова, используя технику логики предикатов, можем представить данное суждение в несколько ином виде с использованием квантора общности:

$$(\exists x)(S(x) \wedge P(x)) \equiv (\exists x)(\neg(\neg S(x) \vee \neg P(x))) \equiv \\ \equiv (\exists x)(\neg(S(x) \rightarrow \neg P(x))) \equiv \neg(\forall x)((S(x) \rightarrow \neg P(x))).$$

Сравнив теперь общеотрицательное суждение E и частноутвердительное суждение I , видим, что каждое из них является отрицанием другого.

Частноутвердительное суждение можно выразить на теоретико-множественном языке следующим образом: $S \cap P \neq \emptyset$, где S и P — множества таких объектов x , которые удовлетворяют предикатам $S(x)$ и $P(x)$ соответственно.

Отметим, что в повседневной речи слово «некоторые» в частноутвердительных суждениях порой опускают, так что, например, фраза «Люди взойшли на Эверест» обозначает «Некоторые люди взойшли на Эверест».

Частноотрицательное суждение: «Некоторые S не суть P ». Укажем примеры математических утверждений такого вида: «Некоторые треугольники — неравносторонние», «Некоторые функции — непериодические», «Некоторые преобразования подобия не являются движениями», «Некоторые ромбы нельзя вписать в окружность», «Некоторые группы не абелевы». Вот примеры нематематических суждений, имеющих частноотрицательный характер: «Некоторые грибы не съедобны», «Некоторые реки не впадают в моря» и т.д.

Частноотрицательное суждение «Некоторые S не суть P » понимается так: существует такой объект x , который обладает свойством S ($S(x)$ истинно) и не обладает свойством P ($P(x)$ ложно, т.е. истинно $\neg P(x)$). На языке логики предикатов это записывается следующим образом:

$$O: \quad (\exists x)(S(x) \wedge \neg P(x)). \quad (4)$$

Выражение (4) можно записать в виде ограниченного квантора существования $(\exists S(x))(\neg P(x))$.

Преобразовав его равносильным образом (проделайте самостоятельно), получаем $(\exists x)(S(x) \wedge \neg P(x)) \equiv \neg(\forall x)(S(x) \rightarrow P(x))$. Эта равносильность показывает, что общеутвердительное суждение A и частноотрицательное суждение O являются взаимными отрицаниями.

Частноотрицательное суждение O следующим образом выражается на теоретико-множественном языке: $S \cap \bar{P} \neq \emptyset$, где S — множество объектов x , удовлетворяющих предикату (свойству) $S(x)$, а $\bar{P}$ — дополнение множества P , состоящего из всех объектов x , удовлетворяющих предикату $P(x)$.

В заключение отметим, что общеотрицательное суждение E и частноутвердительное суждение I допускают обращение. Такой вывод можно сделать, если вспомнить выражения для этих суждений на языке логики предикатов с использованием квантора общности и закона коммутативности конъюнкции:

$$\begin{aligned} E: \quad & \neg(\exists x)(S(x) \wedge P(x)) \equiv \neg(\exists x)(P(x) \wedge S(x)); \\ I: \quad & (\exists x)(S(x) \wedge P(x)) \equiv (\exists x)(P(x) \wedge S(x)). \end{aligned}$$

Это означает, что «Никакое S не есть P » тогда и только тогда, когда «Никакое P не есть S » и соответственно «Некоторые S суть P » истинно тогда и только тогда, когда истинно суждение «Некоторые P суть S ». Соответствующая запись с кванторами существования для суждений A и O показывает, что в них буквы S и P переставить нельзя, эти суждения обращения не допускают.

И еще одно важное замечание. Необходимо отчетливо осознавать, что значит доказать теорему того или иного типа. Так, доказательство общеутвердительных (A) и общеотрицательных (E) теорем должно состоять в построении строгой цепочки логических умозаключений, начинающейся с условий теоремы и заканчивающейся ее заключением. Например, при доказательстве теоремы «Все дифференцируемые функции непрерывны» нужно исходя из определения дифференцируемой (в точке) функции построить строгую цепочку логических заключений, завершающуюся определением непрерывной (в точке) функции. При доказательстве общеотрицательной теоремы «Никакая осевая симметрия плоскости не является движением первого рода» нужно исходя из определения осевой симметрии построить неопровержимую цепь рассуждений, завершающуюся отрицанием определения движения первого рода. При этом, конечно, нужно знать последнее определение и уметь сформулировать его отрицание (возможно, и на языке логики предикатов). Напротив, при доказательстве утверждений частноутвердительных (I) и частноотрицательных (O) цепочек логических рассуждений строить не требуется. Здесь нужно находить или строить примеры. Так, для доказательства частноутвердительного суждения «Некоторые параллелограммы могут быть вписаны в окружность» следует указать конкретный пример такого параллелограмма, который можно вписать в окружность (например, прямоугольник). Аналогично, для доказательства частноотрицательного суждения «Некоторые функции не являются периодическими» достаточно привести пример хотя бы одной непериодической функции.

Методы рассуждений: аристотелева силлогистика. Наиболее часто употребляемые приемы логических рассуждений были впервые охарактеризованы еще аристотелевой логикой и получили название аристотелевых силлогизмов. Создатели известной методической концепции укрупнения дидактических единиц в обучении математике П. М. Эрдниев и Б. П. Эрдниев так характеризуют роль аристотелевской силлогистики в школьном математическом образовании: «В настоящее время образом логической строгости в школе выступает аристотелева силлогистика: незывлемым считается порядок, когда из двух посылок (большой и малой) выводится одно заключение»¹.

Итак, расклассифицировав описанным в предыдущем пункте образом простые высказывания на типы A , E , I , O , Аристотель приступает к анализу умозаключений, которые можно осуществить на их основе. Он выделяет важнейший вид дедуктивных умозаключений — так называемые силлогистические умозаключения, или силлогизмы. Аристотелев силлогизм представляет

¹ Эрдниев П. М., Эрдниев Б. П. Укрупнение дидактических единиц в обучении математике. М., 1986. С. 176.

собой схему логического вывода (умозаключения), состоящую из трех простых высказываний одного из четырех указанных видов *A, E, I, O*: два первых высказывания — посылки, третье — заключение.

Более точно, умозаключения аристотелевой силлогистики имеют следующее строение. В них рассматриваются три свойства (Аристотель называет их терминами): *S, M, P*. Первая посылка (называемая *большая*) представляет собой простое высказывание, связывающее *M* и *P*; вторая посылка (называемая *малая*) связывает *M* и *S*; следствие связывает *S* и *P*, причем в следствии всегда *S* выступает в качестве субъекта, а *P* — в качестве предиката. Фактически аристотелевский силлогизм есть установление соотношения между двумя свойствами *S* и *P* посредством «связующего» свойства *M*. В зависимости от расположения «связующего» свойства *M* может быть четыре вида силлогизмов (по Аристотелю — четыре фигуры модусов силлогизмов), которые схематически представляются следующим образом (запись в столбец означает, что суждение, записанное под чертой, является следствием суждений, записанных над чертой):

Фигура I	Фигура II	Фигура III	Фигура IV
MxP	PxM	MxP	PxM
SyM	SyM	MyS	MyS
SzP	SzP	SzP	SzP

Здесь $x, y, z \in \{a, e, i, o\}$ и запись SzP (как и MxP и SyM и т. п.) обозначает в зависимости от значения z одно из четырех суждений видов *A, E, I, O*, включающих соответствующие предикаты *S* и *P*. Поскольку каждое из трех суждений фигуры независимо одно от другого может иметь один из четырех видов, то каждая фигура составляет следующее количество силлогизмов (схем): $4 \cdot 4 \cdot 4 = 64$. Поскольку фигур 4, то получаем $4 \cdot 64 = 256$ силлогизмов. (Выпишите самостоятельно все силлогизмы каждой из четырех фигур.)

Задача аристотелевой силлогистики, блестяще решенная самим Аристотелем, состоит в том, чтобы обнаружить все те силлогизмы (схемы умозаключений), которые справедливы, т.е. представляют собой логические следования. Таких силлогизмов, как установил Аристотель, имеется ровно 19, остальные — неверны. При этом 4 из 19 правильных силлогизмов оказываются условно правильными.

Для облегчения запоминания всех правильных силлогизмов (или модусов, как их называют) в XIII в. было составлено особое mnemonicское латинское стихотворение. При этом название силлогизма само по себе непереводимо, но дано так, чтобы из гласных букв в него входили лишь те три буквы из *a, e, i, o*, которые указы-

вают на характер посылок и следствия данного силлогизма. Выпишем все верные модусы с их латинскими названиями:

Фигура I

Barbara	Darii	Celarent	Ferio
<i>MaP</i>	<i>MaP</i>	<i>MeP</i>	<i>MeP</i>
<i>SaM</i>	<i>SiM</i>	<i>SaM</i>	<i>SiM</i>
<i>SaP</i>	<i>SiP</i>	<i>SeP</i>	<i>SoP</i>

Фигура II

Baroco	Camestres	Cesare	Festino
<i>PaM</i>	<i>PaM</i>	<i>PeM</i>	<i>PeM</i>
<i>SoM</i>	<i>SeM</i>	<i>SaM</i>	<i>SiM</i>
<i>SoP</i>	<i>SeP</i>	<i>SeP</i>	<i>SoP</i>

Фигура III

Darapti	Datisi	Disamis	Bocardo	Felapton	Ferison
<i>MaP</i>	<i>MaP</i>	<i>MiP</i>	<i>MoP</i>	<i>MeP</i>	<i>MeP</i>
<i>MaS</i>	<i>MiS</i>	<i>MaS</i>	<i>MaS</i>	<i>MaS</i>	<i>MiS</i>
<i>SiP</i>	<i>SiP</i>	<i>SiP</i>	<i>SoP</i>	<i>SoP</i>	<i>SoP</i>

Фигура IV

Bramantip	Dimaris	Camenes	Fesapo	Fresison
<i>PaM</i>	<i>PiM</i>	<i>PaM</i>	<i>PeM</i>	<i>PeM</i>
<i>MaS</i>	<i>MaS</i>	<i>MeS</i>	<i>MaS</i>	<i>MiS</i>
<i>SiP</i>	<i>SiP</i>	<i>SeP</i>	<i>SoP</i>	<i>SoP</i>

В предыдущем пункте было показано, как на языке логики предикатов каждое из категорических суждений *A*, *E*, *I*, *O* может быть представлено формулой логики предикатов (см. записи (1), (2), (3), (4)). Тогда каждый из 19 правильных аристотелевых силлогизмов также может быть представлен некоторой формулой логики предикатов. Рассмотрим примеры некоторых силлогизмов и дадим их обоснование методами логики предикатов.

Пример 24.6. Самый распространенный и простой силлогизм *Barbara*:

$$\begin{array}{c}
 \text{«Все } M \text{ суть } P\text{»}, \\
 \text{«Все } S \text{ суть } M\text{»} \\
 \hline
 \text{«Все } S \text{ суть } P\text{»}.
 \end{array}$$

Здесь как обе посылки, так и заключение являются общеутвердительными суждениями. Вот пример такого рассуждения. «Все квадраты суть ромбы», «Все ромбы суть параллелограммы». Следовательно, «Все квадраты суть параллелограммы».

Обоснуем справедливость такого рассуждения, для чего представим данный силлогизм на языке логики предикатов:

$$\frac{(\forall x)(M(x) \rightarrow P(x)), \quad (\forall x)(S(x) \rightarrow M(x))}{(\forall x)(S(x) \rightarrow P(x))}.$$

Нужно проверить, что третья (нижняя) формула является логическим следствием первых двух, т.е. нужно показать, что она превращается в истинное высказывание при всякой такой подстановке вместо ее предикатных переменных $S(x)$ и $P(x)$ таких конкретных предикатов, при которой обе первые формулы превращаются в истинные высказывания. В самом деле, на основании равносильности (получаемой из тавтологии) теоремы 21.11, а, для конъюнкции посылки имеем

$$\begin{aligned} &(\forall x)(S(x) \rightarrow M(x)) \wedge (\forall x)(M(x) \rightarrow P(x)) \equiv \\ &\equiv (\forall x)[(S(x) \rightarrow M(x)) \wedge (M(x) \rightarrow P(x))]. \end{aligned}$$

Истинность обеих посылок означает истинность их конъюнкции и, следовательно, ввиду приведенной равносильности — тождественную истинность предиката $(S(x) \rightarrow M(x)) \wedge (M(x) \rightarrow P(x))$, т.е. истинность высказывания $(S(a) \rightarrow M(a)) \wedge (M(a) \rightarrow P(a))$ для любого a . Но тогда, на основании закона силлогизма (тавтология теоремы 3.1, е), для любого a будет истинно высказывание $S(a) \rightarrow P(a)$, т.е. будет тождественно истинным предикат $S(x) \rightarrow P(x)$. Последнее означает, что будет истинно высказывание $(\forall x)(S(x) \rightarrow P(x))$, являющееся заключением рассматриваемого силлогизма.

Пример 24.7. Совершенно аналогично обосновывается (предлагается проделать самостоятельно) справедливость силлогизма *Celarent*:

$$\frac{\begin{array}{l} \text{«Все } M \text{ суть не } P\text{»,} \\ \text{«Все } S \text{ суть } M\text{»} \end{array}}{\text{«Все } S \text{ суть не } P\text{»}.$$

Пример 24.8. Рассмотрим еще один силлогизм *Festino*:

$$\frac{\begin{array}{l} \text{«Никакое } P \text{ не есть } M\text{»,} \\ \text{«Некоторые } S \text{ суть } M\text{»} \end{array}}{\text{«Некоторые } S \text{ не суть } P\text{»}.$$

Приведем пример рассуждения, основанного на этой схеме. «Никакая окружность не является квадратом», «Некоторые параллелограммы являются квадратами». Следовательно, «Некоторые параллелограммы не являются окружностями».

Запишем данный силлогизм на языке логики предикатов:

$$\frac{(\forall x)(P(x) \rightarrow \neg M(x)), \quad (\exists x)(S(x) \wedge M(x))}{(\exists x)(S(x) \wedge \neg P(x))}.$$

Покажем, что третья формула является логическим следствием первых двух. Из истинности первого высказывания вытекает истинность высказывания $P(a) \rightarrow \neg M(a)$ для любого предмета a . Следовательно, на основе равносильностей теоремы 4.4, a , b , истинно высказывание $M(a) \rightarrow \neg P(a)$ для любого a .

Докажем, далее, истинность следующего высказывания:

$$(\exists x)(S(x) \wedge M(x)) \rightarrow (\exists x)(S(x) \wedge \neg P(x)). \quad (1)$$

Допустим, что посылка $(\exists x)(S(x) \wedge M(x))$ истинна. Это означает, что существует такой объект a , что высказывание $S(a) \wedge M(a)$ истинно. Следовательно, истинны оба высказывания $S(a)$ и $M(a)$. Из истинности высказываний $M(a)$ и $M(a) \rightarrow \neg P(a)$ вытекает истинность высказывания $\neg P(a)$, что вместе с истинностью $S(a)$ дает истинность конъюнкции $S(a) \wedge \neg P(a)$ для некоторого объекта a . Последнее означает истинность высказывания $(\exists x)(S(x) \wedge \neg P(x))$. Таким образом, истинность импликации (1) установлена.

Итак, показано, что из первой посылки рассматриваемого силлогизма следует формула (1). Символически это можно выразить так: $F \models G \rightarrow H$, где F , G — посылки, а H — следствие рассматриваемого силлогизма. Тогда, на основании теоремы 6.3, заключаем, что $F, G \models H$, т.е. формула H является логическим следствием формул F и G . Рассматриваемый силлогизм действительно справедлив.

Пример 24.9. Приведем пример неверного силлогизма. «Некоторые B суть C », «Некоторые A суть B », следовательно, «Некоторые A суть C ». Действительно, эта схема умозаключения неверна, потому что на основании ее, например, из истинных утверждений «Некоторые выпуклые фигуры — круги» и «Некоторые многоугольники — выпуклые фигуры» приходим к ложному выводу «Некоторые многоугольники являются кругами». Этому силлогизму соответствует формула логики предикатов:

$$((\exists x)(B(x) \wedge C(x)) \wedge (\exists x)(A(x) \wedge B(x))) \rightarrow (\exists x)(A(x) \wedge C(x)),$$

не являющаяся общезначимой (примеры соответствующих предикатов только что указаны).

Аристотелева силлогистика и логика предикатов. В предыдущем пункте показано как аристотелевы силлогизмы переводятся на язык логики предикатов: каждому силлогизму сопоставляется формула логики предикатов, при этом правильным силлогизмам соответствуют тавтологии (общезначимые формулы) логики предикатов, а неправильным силлогизмам — формулы, не являющиеся тавтологиями.

Тем не менее при более пристальном рассмотрении этих формул выясняется, что так происходит не для всех правильных аристотелевых силлогизмов: тавтологии соответствуют лишь пятнадцати из них. Остальным четырем правильным силлогизмам *Darapti*, *Felapton*, *Bramantip* и *Fesapo* соответствуют формулы логики предикатов, не являющиеся общезначимыми, т.е. тавтологиями.

Пример 24.10. Рассмотрим формулу, отвечающую силлогизму *Darapti*:

$$((\forall x)(M(x) \rightarrow P(x)) \wedge (\forall x)(M(x) \rightarrow S(x))) \rightarrow (\exists x)(S(x) \wedge P(x)).$$

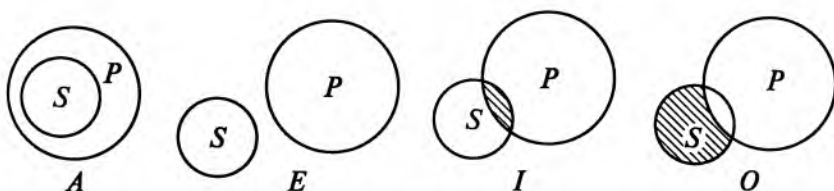
Покажем, что эта формула не является общезначимой. Для этого нужно указать такие конкретные предикаты $A(x)$, $B(x)$, $C(x)$, заданные над некоторым множеством M , что посылка силлогизма превратится в истинное высказывание $(\forall x)(B(x) \rightarrow C(x) \wedge (\forall x)(B(x) \rightarrow A(x)))$, а следствие — в ложное $(\exists x)(A(x) \wedge C(x))$. Для этого достаточно, чтобы предикат $B(x)$ был тождественно ложен, а предикаты $A(x)$ и $C(x)$ обладали бы тем свойством, что для любого предмета $a \in M$ одно из высказываний $A(a)$ или $C(a)$ было бы ложным. Последнее возможно, если, например, один из предикатов $A(x)$ или $C(x)$ является отрицанием другого. Укажите самостоятельно примеры таких предикатов, например, на множестве натуральных чисел N .

Выпишите самостоятельно формулы логики предикатов для оставшихся трех «плохих» силлогизмов и докажите, что они не общезначимы. Выпишите также формулы логики предикатов для пятнадцати «хороших» аристотелевых силлогизмов и докажите их общезначимость. (См. также Задачник, № 9.68 — 9.71.)

Какой же вывод можно сделать после анализа результатов перевода аристотелевых силлогизмов на язык логики предикатов? Вывод таков, что логика предикатов, как и алгебра высказываний, далеко не является совершенной математической теорией, отражающей (описывающей) процесс человеческого мышления. И эта теория допускает изъяны, приводит к выводам, не сопоставимым с результатами реальных процессов, которые теория призвана описать. Это же обстоятельство приводит, с одной стороны, к задаче создания аксиоматической теории аристотелевых силлогизмов, в которой каждый верный силлогизм по каким-то

правилам выводился бы из аксиом, а с другой — к задаче построения такой логической системы, которая все же вписывала бы всю традиционную силлогистику в общий ансамбль современной формальной логики. Эти вопросы будут рассмотрены в § 30.

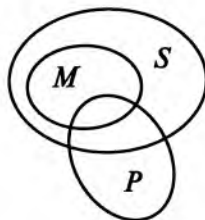
Теоретико-множественная интерпретация аристотелевой силлогистики. Данная интерпретация, в частности, поможет лучше понять причину того, что не все верные силлогизмы выражаются на языке логики предикатов общезначимой формулой. Обозначим множества истинности предикатов $S(x)$, $M(x)$, $P(x)$ через S , M , P соответственно. Тогда утверждения об истинности категорических суждений A , E , I , O могут быть следующим образом выражены на теоретико-множественном языке (учитывайте запись этих утверждений на языке логики предикатов, мы говорили уже об этом выше): A : $S \subseteq P$ ($S \cap P = S$), E : $S \cap P = \emptyset$, I : $S \cap P \neq \emptyset$, O : $S \not\subseteq P$ ($S \setminus P \neq \emptyset$). Нетрудно изобразить с помощью диаграмм Эйлера — Венна взаимоотношения между множествами S и P в каждом случае:



Теперь каждый аристотелев силлогизм будет представлять собой утверждение о том, что из каких-то двух соотношений между множествами S , M , P непременно следует третье соотношение между множествами S и P .

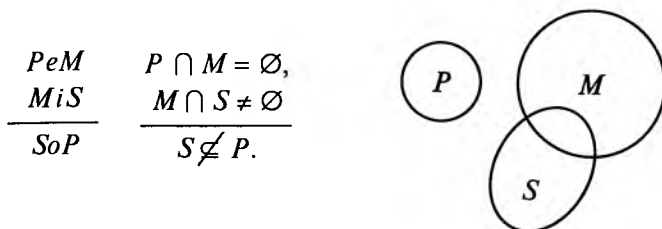
Пример 24.11. Например, силлогизм *Bocardo* на теоретико-множественном языке запишется так:

MoP	$M \not\subseteq P$,
MaS	$M \subseteq S$
SoP	$S \not\subseteq P$.



Используя свойства отношения включения $\subseteq$, нетрудно установить справедливость данного силлогизма. В самом деле, допустим, что он несправедлив, т. е. $M \not\subseteq P$, $M \subseteq S$, но $S \subseteq P$. Тогда из второго и третьего условий, в силу транзитивности отношения $\subseteq$, заключаем, что $M \subseteq P$, а это противоречит первому условию.

Пример 24.12. Пример верного силлогизма *Fresison*. Его запись:



Предположим, что $S \subseteq P$. Тогда $S \cap P = S$. Учитывая это, находим: $S \cap (P \cap M) = (S \cap P) \cap M = S \cap M \neq \emptyset$ (неравенство на основании второго условия). Следовательно, $P \cap M \neq \emptyset$, что противоречит первому условию.

Пример 24.13. Приведем пример неправильного силлогизма:

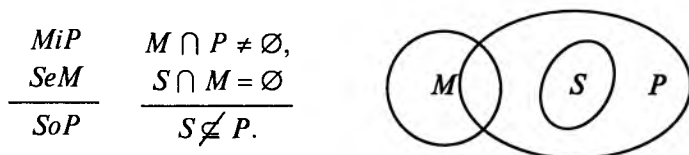
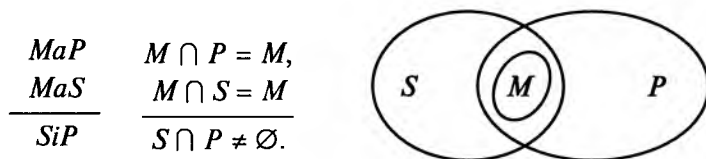


Диаграмма показывает, что для трех множеств S, M, P возможна ситуация, когда условия выполнены: $M \cap P \neq \emptyset$, $S \cap M = \emptyset$, а заключение — нет: $S \subseteq P$. Следовательно, данный силлогизм неверен, т.е. рассуждения по данной схеме неправильны.

Наконец обратимся к четырем «плохим» с точки зрения логики предикатов правильным силлогизмам *Darapti*, *Felapton*, *Bramantip* и *Fesapo* и постараемся понять, почему выражающие их формулы логики предикатов оказались необщезначимыми.

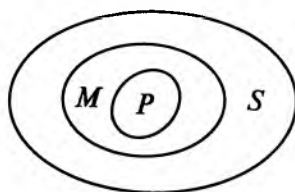
Пример 24.14. Силлогизм *Darapti* имеет вид:



Из условий вытекает, что $M \cap (S \cap P) = M$, т.е. $M \subseteq S \cap P$. Если $M \neq \emptyset$, то $S \cap P \neq \emptyset$, и заключение силлогизма выполняется. Если же $M = \emptyset$, то при выполнении условий силлогизма заключение может и не выполниться: $S \cap P = \emptyset$. (Вспомните здесь, что соответствующая формула логики предикатов превращалась в ложное высказывание, если вместо предикатной переменной $M(x)$ подставить тождественно ложный предикат.)

Пример 24.15. Силлогизм *Bramantip* имеет вид:

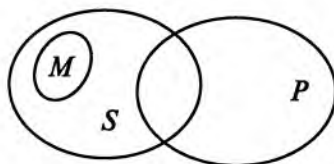
$$\frac{PaM \quad MaS}{SiP} \quad \frac{P \subseteq M \quad (P \cap M = P), \quad M \subseteq S \quad (M \cap S = M)}{S \cap P \neq \emptyset}.$$



Из условий получаем $(P \cap M) \cap (M \cap S) = P \cap M$, т.е. $S \cap (P \cap M) = P$, откуда $S \cap P = P$. Это означает, что если $P \neq \emptyset$, то $S \cap P \neq \emptyset$, и заключение силлогизма выполняется. Если же $P = \emptyset$, то при выполнении условий силлогизма его заключение может и не выполняться: $S \cap P = \emptyset$.

Пример 24.16. Силлогизм *Felapton* имеет вид:

$$\frac{MeP \quad MaS}{SoP} \quad \frac{M \cap P = \emptyset, \quad M \subseteq S}{S \not\subseteq P}.$$



Допустим, что условия верны, но $S \subseteq P$. Тогда $M \subseteq P$, т.е. $M \cap P = M$, а значит, $M = \emptyset$. Таким образом, при $M = \emptyset$ из выполнимости условий силлогизма может не следовать выполнимость его заключения. Аналогична теоретико-множественная ситуация с силлогизмом *Fesapo*.

Итак, четыре рассмотренных силлогизма с теоретико-множественной точки зрения не выполняются в тех случаях, когда в них участвуют пустые множества. С точки зрения логики предикатов это означает, что мы не исключаем тождественно ложных предикатов. Это означает, что в теоретико-множественной теории силлогизмов, находящейся в рамках логики предикатов, имеется лишь 15 верных силлогизмов. Если же мы исключим из рассмотрения в логике предикатов тождественно ложные предикаты, то мы будем иметь 19 верных силлогизмов.

Что же касается классической аристотелевской силлогистики, то в ней изначально не предполагались пустые термины, т.е. предикаты с пустым множеством субъектов, или, в нашей терминологии, тождественно ложные предикаты. Поэтому классическая аристотелевская силлогистика включает 19 верных силлогизмов.

Отметим, что М. В. Ломоносов (1711 — 1765), осуществляя нововведения в традиционную логику, не признавал правильными «плохие» силлогизмы *Darapti*, *Felapton*, *Bramantip* и *Fesapo*. Это

красноречиво говорит о том, насколько глубоко этот гениальный ученый проник и в эту область научного знания.

О других методах рассуждений. Аристотелевская силлогистика охватывает далеко не все типы умозаключений так называемой логики свойств, к которой эту силлогистику принято относить. Полная формализация таких умозаключений осуществляется в логике (одноместных) предикатов. Рассмотрим еще ряд некоторых типов умозаключений.

Пример 24.17. Вот один такой широко распространенный способ рассуждений. Приведем сначала примеры таких рассуждений. «Все люди смертны. Сократ — человек. Следовательно, Сократ смертен». «Всякое нечетное натуральное число является разностью двух квадратов. 7 есть нечетное натуральное число. Следовательно, 7 является разностью двух квадратов». Приведенные рассуждения основаны на следующей схеме:

$$\frac{(\forall x)(H(x) \rightarrow P(x)), \quad H(a)}{P(a)},$$

означающей, что третья формула является логическим следствием первых двух. Проверим, что это действительно так. Пусть первые две формулы превратились в истинные высказывания $(\forall x)(A(x) \rightarrow B(x))$ и $A(a)$ при подстановке вместо предикатных переменных H и P некоторых конкретных предикатов $A(x)$ и $B(x)$ соответственно, определенных на некотором множестве M . Истинность высказывания $(\forall x)(A(x) \rightarrow B(x))$ означает тождественную истинность предиката $A(x) \rightarrow B(x)$, откуда, в частности, вытекает истинность высказывания $A(a) \rightarrow B(a)$. Наконец, из истинности высказываний $A(a)$ и $A(a) \rightarrow B(a)$ следует истинность высказывания $B(a)$, полученного из заключительной формулы $P(a)$ в результате подстановки конкретного предиката B на место предикатной переменной P . Тем самым справедливость приведенной схемы рассуждений доказана.

И аристотелевские силлогизмы, и приведенная схема рассуждений обосновываются с привлечением лишь одноместных предикатов. Приведем пример рассуждения, для обоснования которого уже нельзя обойтись только одноместными предикатами.

Пример 24.18. «Бинарное отношение $<$ на множестве натуральных чисел транзитивно и антирефлексивно. Следовательно, оно несимметрично». Символически:

$$\frac{(\forall x)(\forall y)(\forall z)(x < y \wedge y < z \rightarrow x < z), \quad (\forall x)(\neg(x < x))}{(\forall x)(\forall y)(x < y \rightarrow \neg(y < x))}.$$

Это рассуждение основано на следующей схеме с двухместным предикатом $P(x, y)$:

$$\frac{(\forall x)(\forall y)(\forall z)(P(x, y) \wedge P(y, z) \rightarrow P(x, z)), \quad (\forall x)(\neg P(x, x))}{(\forall x)(\forall y)(P(x, y) \rightarrow \neg P(y, x)).}$$

Проверим справедливость этой схемы. Отметим вначале, что тавтологию закона удаления квантора общности (теорема 21.13, а) в терминах логического следования можно трактовать так: формула $P(y)$ является логическим следствием формулы $(\forall x)(P(x))$. На основании данного закона из первой формулы рассматриваемой схемы следует формула

$$P(x, y) \wedge P(y, x) \rightarrow P(x, x) \quad (1)$$

(переменную z переименовали в x). Далее, из второй формулы рассматриваемой схемы по тому же закону удаления квантора общности следует формула

$$\neg P(x, x). \quad (2)$$

При фиксированных x и y две последние формулы превращаются в формулы алгебры высказываний: $(A \wedge B) \rightarrow C, \neg C$. Используя методы алгебры высказываний (см. § 6), нетрудно проверить, что

$$(A \wedge B) \rightarrow C, \neg C = A \rightarrow \neg B. \quad (3)$$

Переводя полученную формулу $A \rightarrow \neg B$ на первоначальный язык, получим формулу $P(x, y) \rightarrow \neg P(y, x)$. Таким образом, выводимость (3) показывает, что формула $P(x, y) \rightarrow \neg P(y, x)$ является логическим следствием формул (1) и (2) для каждого значения x и y . Следовательно, и формула $(\forall x)(\forall y)(P(x, y) \rightarrow \neg P(y, x))$ будет превращаться в истинное высказывание при всякой такой подстановке вместо предикатной переменной P конкретного предиката, а вместо предметных переменных x и y — конкретных предметов, при которой в истинные высказывания превращаются формулы (1) и (2). Этим завершается проверка справедливости схемы умозаключения.

В заключение приведем пример доказательства математической теоремы, целиком основанного на одной тавтологии логики предикатов. По существу здесь мы имеем пример теоремы из конкретного раздела математики, доказательство которой носит не математический, а чисто логический характер.

Пример 24.19. Рассмотрим следующую тавтологию логики предикатов (см. Задачник, № 9.43, *м*):

$$(\forall x)(P(x)) \rightarrow (\forall x)(P(x) \vee Q(x)). \quad (1)$$

Покажем, как она может быть применена к доказательству следующего утверждения: «Наименьший элемент (если он существует) упорядоченного множества минимален.»

Напомним определения. *Отношением порядка* на множестве A называется бинарное отношение $<$ на A , удовлетворяющее условиям:

- 1) рефлексивность: $(\forall x)(x < x)$;
- 2) антисимметричность: $(\forall x, y, z)((x < y \wedge y < x) \rightarrow x = y)$;
- 3) транзитивность: $(\forall x, y, z)((x < y \wedge y < z) \rightarrow x < z)$.

Множество A вместе с заданным на нем отношением порядка $<$ называется *упорядоченным* и обозначается $<A; <>$. Элемент a упорядоченного множества $<A; <>$ называется *наименьшим*, если он меньше всех элементов этого множества: $(\forall x)(a < x)$, и называется *минимальным*, если меньше его нет элемента в этом множестве: $\neg(\exists x)(x < a)$. Таким образом, утверждение, которое мы хотим доказать, на языке логики предикатов записывается так:

$$(\forall x)(a < x) \rightarrow \neg(\exists x)(x < a). \quad (2)$$

С помощью равносильных преобразований преобразуем сначала заключение этой импликации:

$$\neg(\exists x)(x < a) \equiv (\forall x)[\neg(x < a)] \equiv (\forall x)[a < x \vee (\neg(a < x) \wedge \neg(x < a))] \equiv (\forall x)[(a < x \vee \neg(a < x)) \wedge (a < x \vee \neg(x < a))] \equiv (\forall x)(a < x \vee \neg(x < a)).$$

Тогда утверждение (2) имеет вид

$$(\forall x)(a < x) \rightarrow (\forall x)(a < x \vee \neg(x < a)). \quad (3)$$

Именно в это высказывание и превращается формула (1) при подстановке в нее вместо переменной $P(x)$ предиката « $a < x$ », а вместо переменной $Q(x)$ — предиката « $\neg(x < a)$ ». Поскольку формула (1), как мы доказали, общезначима, то высказывание (3), а вместе с ним и высказывание (2) истинны.

Принцип полной дизъюнкции в предикатной форме. Теореме 7.18 об обратимости системы импликаций можно придать следующий предикатный вид.

Теорема 24.20. Пусть справедливы все следующие прямые теоремы ($m \geq 2$):

$$(\forall x)(P_1(x) \rightarrow Q_1(x)), (\forall x)(P_2(x) \rightarrow Q_2(x)), \dots, (\forall x)(P_m(x) \rightarrow Q_m(x)).$$

Причем для посылок известно, что истинно утверждение $(\forall x)(P_1(x) \vee P_2(x) \vee \dots \vee P_m(x))$, а следствия попарно исключают друг друга, т.е. истинны все высказывания $\neg(\exists x)(Q_i(x) \wedge Q_j(x))$ ($i, j = 1, \dots, m, i \neq j$). Тогда справедливы и все обратные импликации:

$$(\forall x)(Q_1(x) \rightarrow P_1(x)), (\forall x)(Q_2(x) \rightarrow P_2(x)), \dots, (\forall x)(Q_m(x) \rightarrow P_m(x)).$$

(Предполагается, конечно, что все предикаты заданы над одним и тем же множеством M .)

Доказательство. Покажем сначала, что истинна первая обратная импликация: $(\forall x)(Q_1(x) \rightarrow P_1(x))$. Пусть $a \in M$. Если высказывание $Q_1(a)$ ложно, то импликация $Q_1(a) \rightarrow P_1(a)$ истинна. Предположим, что высказывание $Q_1(a)$ истинно. Покажем, что тогда все высказывания $P_2(a), \dots, P_m(a)$ ложны. Допустим противное: например, пусть $P_2(a)$ истинно. В силу истинности (по условию) универсального высказывания $(\forall x)(P_2(x) \rightarrow Q_2(x))$ будет истинна и импликация $P_2(a) \rightarrow Q_2(a)$, что вместе с истинностью ее посылки $P_2(a)$ приводит к истинности следствия $Q_2(a)$. Итак, высказывания $Q_1(a)$ и $Q_2(a)$ истинны. Значит, истинна конъюнкция $Q_1(a) \wedge Q_2(a)$, а вместе с ней истинно экзистенциальное высказывание $(\exists x)(Q_1(x) \wedge Q_2(x))$, что противоречит условию, согласно которому истинно отрицание этого высказывания. Таким образом, все высказывания $P_2(a), \dots, P_m(a)$ ложны. Тогда высказывание $P_1(a)$ должно быть истинно, ибо если и оно будет ложным, то ложной будет и дизъюнкция $P_1(a) \vee P_2(a) \vee \dots \vee P_m(a)$, а вместе с ней и универсальное высказывание $(\forall x)(P_1(x) \vee \dots \vee P_m(x))$, что противоречит условию. Итак, высказывания $Q_1(a)$ и $P_1(a)$ истинны. Следовательно, истинна импликация $Q_1(a) \rightarrow P_1(a)$.

Итак, мы доказали, что, каким бы ни был элемент $a \in M$ (превращающим предикат $Q_1(x)$ в ложное высказывание или превращающим его в истинное высказывание), импликация $Q_1(a) \rightarrow P_1(a)$ будет истинной. Следовательно, будет истинно и высказывание $(\forall x)(Q_1(x) \rightarrow P_1(x))$.

Совершенно аналогично устанавливается истинность и остальных обратных импликаций: $(\forall x)(Q_2(x) \rightarrow P_2(x)), \dots, (\forall x)(Q_m(x) \rightarrow P_m(x))$. $\square$

Частным видом рассмотренной теоремы об обратимости системы импликаций при $m = 2$ является следующая теорема.

Теорема 24.21. Пусть справедливы следующие две прямые теоремы: $(\forall x)(P(x) \rightarrow Q_1(x))$ и $(\forall x)(\neg P(x) \rightarrow Q_2(x))$, причем следствия $Q_1(x)$ и $Q_2(x)$ взаимно исключают друг друга, т. е. истинно высказывание $\neg(\exists x)(Q_1(x) \wedge Q_2(x))$. Тогда справедливы обратные теоремы: $(\forall x)(Q_1(x) \rightarrow P(x))$ и $(\forall x)(Q_2(x) \rightarrow \neg P(x))$.

Для того чтобы доказать, что данная теорема действительно является частным видом теоремы предыдущего пункта, заметим, что ее условие удовлетворяет требованиям условия предыдущей теоремы. Следствия здесь действительно исключают одно другое, а для посылок $P(x)$ и $\neg P(x)$ ясно, что верно утверждение $(\forall x)(P(x) \vee \neg P(x))$, чего и требует условие предыдущей теоремы. $\square$

Приведем пример двух теорем из геометрии, истинность обратных утверждений для которых может быть установлена с помощью рассмотренного частного случая теоремы об обратимости системы импликаций.

Пример 24.22. Рассмотрим теоремы: 1) «Если две плоскости параллельны, то всякая плоскость при пересечении с ними дает две

прямые линии, которые также параллельны. Символически: $(\forall \pi_1, \pi_2)[\pi_1 \parallel \pi_2 \rightarrow (\forall \pi)(\pi_1 \cap \pi \parallel \pi_2 \cap \pi)]$ »;

2) «Если две плоскости не параллельны, то существует плоскость, которая при пересечении с ними дает две пересекающиеся прямые линии. Символически: $(\forall \pi_1, \pi_2)[\pi_1 \nparallel \pi_2 \rightarrow (\exists \pi)((\pi_1 \cap \pi) \cap (\pi_2 \cap \pi) \neq \emptyset)]$ ».

Ясно, что следствия этих утверждений $(\forall \pi)(\pi_1 \cap \pi \parallel \pi_2 \cap \pi)$ и $(\exists \pi)((\pi_1 \cap \pi) \cap (\pi_2 \cap \pi) \neq \emptyset)$ взаимно исключают друг друга. Тогда можно сделать вывод о справедливости двух обратных утверждений:

1') «Если при пересечении любых двух данных плоскостей всякой третьей плоскостью получаются две параллельные прямые, то и сами данные плоскости также параллельны»;

2') «Если при пересечении любых двух данных плоскостей некоторой третьей плоскостью получаются две пересекающиеся прямые, то и сами данные плоскости также пересекаются».

Метод (полной) математической индукции — специальный метод доказательства, применяемый для доказательства истинности утверждений типа $(\forall x \in N)(P(x))$, т.е. $(\forall x)(x \in N \rightarrow P(x))$. Такие утверждения выражают тот факт, что некоторое свойство P присуще каждому натуральному числу. Аксиоматическое обоснование этого метода будет дано в § 29. Сейчас изложим суть этого метода. Формальной основой метода математической индукции служит одна из аксиом, называемая аксиомой индукции (или математической индукции) и выражающая свойство естественного отношения порядка, имеющегося на множестве всех натуральных чисел. Эта аксиома такова. Если свойством P обладает число 1 и для всякого натурального числа из того, что оно обладает этим свойством, следует, что и непосредственно следующее за ним натуральное число также обладает им, то и всякое натуральное число обладает свойством P . Символически, на языке логики предикатов, эта аксиома записывается так: $(P(1) \wedge (\forall x)(P(x) \rightarrow P(x+1))) \rightarrow (\forall y)(P(y))$.

Эта аксиома дает следующий метод доказательства утверждений, выражающих некоторые свойства всех натуральных чисел. Если нужно доказать утверждение $(\forall y)(P(y))$, где $y \in N$ («Всякое натуральное число обладает свойством P »), достаточно установить истинность высказывания $P(1)$ («Число 1 обладает свойством P ») и доказать, что $(\forall x)(P(x) \rightarrow P(x+1))$, т.е. «Если x обладает свойством P , то этим свойством обладает и число $x+1$, непосредственно следующее за x ».

Таким образом, логическая схема доказательства методом математической индукции может быть представлена следующим образом:

(1): $P(1)$ — устанавливается проверкой;

(2): $(\forall x)(P(x) \rightarrow P(x+1))$ — доказывается;

(3): $P(1) \wedge (\forall x)(P(x) \rightarrow P(x+1))$ — из (1), (2) по правилу введения конъюнкции;

(4): $(P(1) \wedge (\forall x)(P(x) \rightarrow P(x+1))) \rightarrow (\forall y)(P(y))$ — аксиома индукции;

(5): $(\forall y)(P(y))$ — из (3), (4) по правилу МР.

При этом установление истинности утверждения $P(1)$ называется основанием или базой индукции; предположение об истинности утверждения $P(x)$ — предположением индукции; последующее доказательство истинности утверждения $P(x+1)$ — шагом индукции.

Методом математической индукции доказано утверждение о том, что число двоичных наборов длины n (упорядоченных n -ок), составленных из нулей и единиц, равно 2^n (теорема 10.3), о представлении булевых функций (теорема 10.5), теорема 15.4 о дедукции. Неоднократно применялась индукция по числу логических связок, входящих в формулу логики высказываний или предикатов (см. теоремы 2.2, 22.3, 22.5).

Необходимые и достаточные условия. Отношение следования предикатов и соответствующее ему отношение включения соответствующих множеств истинности этих предикатов могут придать дополнительные штрихи к методике обучения понятиям необходимых и достаточных условий, усвоение которых вызывает значительные затруднения не только у школьников, но и у студентов.

Предположим, что некоторая математическая теорема имеет вид: $(\forall x)(P(x) \rightarrow Q(x))$. Это означает, что предикат $P(x) \rightarrow Q(x)$ тождественно истинен, т.е. его множество истинности $(P \rightarrow Q)^+ = U$. Используя теоремы 19.2, 19.6, 19.9, находим: $U = (P \rightarrow Q)^+ = (\neg P \vee Q)^+ = (\neg P)^+ \cup Q^+ = \overline{P}^+ \cup Q^+$. Следовательно, $P^+ \subseteq Q^+$, а значит, предикат $Q(x)$ является следствием предиката $P(x)$.

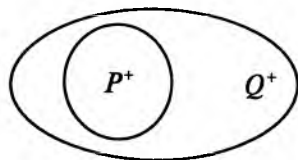
Исходная теорема $(\forall x)(P(x) \rightarrow Q(x))$ означает, что условие $P(x)$ является достаточным для условия $Q(x)$, а $Q(x)$ — необходимым для $P(x)$. Проведенное только что рассуждение показывает, что это будет тогда и только тогда, когда имеет место включение $P^+ \subseteq Q^+$ соответствующих множеств истинности.

Если теперь изобразить эти множества и отношение включения между ними кругами Эйлера, то, используя обычные житейские представления о терминах «необходимо» и «достаточно», можно заключить:

1) чтобы элемент x принадлежал множеству Q^+ (т.е. удовлетворял условию $Q(x)$), (вполне) достаточно, чтобы он принадлежал множеству P^+ (т.е. удовлетворял условию $P(x)$);

2) чтобы элемент x принадлежал множеству P^+ , необходимо, чтобы он принадлежал множеству Q^+ (ибо в противном случае, если он не принадлежит Q^+ , то он и подавно не принадлежит множеству P^+).

Полезно научиться оперировать этими понятиями на наглядном языке эйлеров-



ских диаграмм. Эта своего рода материализованная форма умственной деятельности будет способствовать формированию чисто умственных действий, связанных с понятиями необходимых и достаточных условий. Здесь необходимо освоить два вида деятельности.

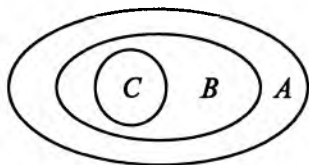
Во-первых, научиться рисовать диаграмму Эйлера, описывающую ту или иную словесную формулировку.

Пример 24.23. Формулировки могут быть, например, такими:

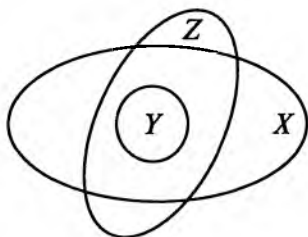
- 1) P необходимо для Q ;
- 2) B необходимо для A ;
- 3) M достаточно для N , N достаточно для K ;
- 4) A необходимо для B , B необходимо для C ;
- 5) X необходимо для Y , Y достаточно для Z ;
- 6) X достаточно для Y , Y необходимо для Z .

Диаграммы Эйлера выглядят так:

(в случае 4)

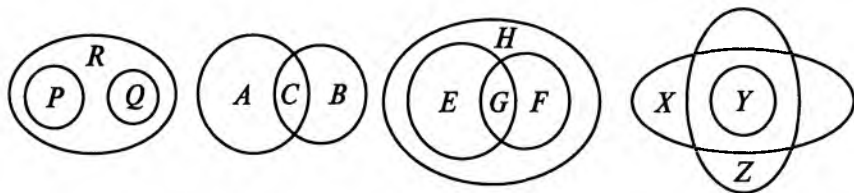


(в случае 5)



Во-вторых, наоборот, в ответ на предложенную диаграмму Эйлера дать соответствующую ей словесную формулировку.

Пример 24.24. Вот примеры диаграмм:



Соответствующие словесные формулировки таковы: Y достаточно для X , Y достаточно для Z ; R необходимо и для P , и для Q .

Логика предикатов и алгебра множеств. В § 8 была показана связь алгебры высказываний с теорией множеств. Логика предикатов усиливает эти связи, так как позволяет дать четкое толкование и обоснование известным теоретико-множественным понятиям и концепциям, а также ввести ряд новых. Например, понятие равенства двух множеств (принцип равнообъемности) на языке логики предикатов выражается так:

$$M_1 = M_2 \stackrel{\text{опр.}}{\Leftrightarrow} (\forall x)(x \in M_1 \leftrightarrow x \in M_2),$$

а понятие включения множеств следующим образом:

$$M_1 \subseteq M_2 \stackrel{\text{опр.}}{\Leftrightarrow} (\forall x)(x \in M_1 \rightarrow x \in M_2).$$

Тогда законы логики предикатов позволяют строго обосновать утверждение.

Пример 24.25. $M_1 = M_2 \Leftrightarrow M_1 \subseteq M_2 \wedge M_2 \subseteq M_1$.

Действительно, доказательство представляет собой цепочку равносильностей:

$$\begin{aligned} M_1 = M_2 &\Leftrightarrow (\forall x)(x \in M_1 \leftrightarrow x \in M_2) \Leftrightarrow \\ &\Leftrightarrow (\forall x)[(x \in M_1 \rightarrow x \in M_2) \wedge (x \in M_2 \rightarrow x \in M_1)] \Leftrightarrow \\ &\Leftrightarrow (\forall x)(x \in M_1 \rightarrow x \in M_2) \wedge (\forall x)(x \in M_2 \rightarrow x \in M_1) \Leftrightarrow \\ &\Leftrightarrow M_1 \subseteq M_2 \wedge M_2 \subseteq M_1. \end{aligned}$$

Далее, тавтологии логики высказываний позволяют обосновывать свойства теоретико-множественных операций: дополнения, пересечения, объединения множеств. При этом каждое множество M мыслится как множество истинности одноместного предиката « $x \in M$ » (см. § 8).

Логика предикатов позволяет ввести новые теоретико-множественные понятия. Покажем, в частности, как обобщаются теоретико-множественные операции объединения и пересечения множеств на случай бесконечного числа множеств. Пусть имеется некоторое семейство $(M_i)_{i \in I}$ подмножеств множества M . (Это означает, что каждому элементу $i \in I$ взаимно-однозначно сопоставлено подмножество M_i множества M . Множество I называется множеством индексов семейства $(M_i)_{i \in I}$, а само семейство называется индексированным.) *Объединением данного семейства* называется

множество, обозначаемое $\bigcup_{i \in I} M_i$, состоящее из всех таких элементов множества M , которые принадлежат по меньшей мере одному из подмножеств семейства:

$$\bigcup_{i \in I} M_i = \{x \in M : (\exists i \in I)(x \in M_i)\}.$$

Пересечением данного семейства называется множество, обозначаемое $\bigcap_{i \in I} M_i$, состоящее из всех таких элементов множества M , которые принадлежат каждому из подмножеств семейства:

$$\bigcap_{i \in I} M_i = \{x \in M : (\forall i \in I)(x \in M_i)\}.$$

Логика предикатов позволяет установить свойства этих теоретико-множественных операций: они в некотором смысле аналогичны соответствующим свойствам объединения и пересечения.

Пример 24.26. Проверим, например, один из законов де Моргана:

$$\overline{\bigcup_{i \in I} M_i} = \bigcap_{i \in I} \overline{M_i}.$$

Используя закон де Моргана для кванторов (теорема 21.9, б), получаем

$$\begin{aligned} \overline{\bigcup_{i \in I} M_i} &= \{x : \neg(x \in \bigcup_{i \in I} M_i)\} = \{x : \neg(\exists i \in I)(x \in M_i)\} = \\ &= \{x : (\forall i \in I)(\neg(x \in M_i))\} = \{x : (\forall i \in I)(x \in \overline{M_i})\} = \bigcap_{i \in I} \overline{M_i}. \end{aligned}$$

Аналогично можно установить второй закон де Моргана для этих операций, законы дистрибутивности одной операции относительно другой и ряд других свойств.

Большими возможностями располагает логика предикатов в теории бинарных отношений, где на языке предикатов выражаются фактически все понятия этой теории: проекции, срезы, функциональность, однозначность, взаимная однозначность, сюръективность, обращение и произведение бинарных отношений, их рефлексивность, симметричность, транзитивность, антисимметричность, асимметричность, связность и т.д.

§ 25. Формализованное исчисление предикатов

Задача формализованного исчисления предикатов (ФИП) та же, что и формализованного исчисления высказываний (ФИБ), — дать аксиоматическую теорию совокупности всех общезначимых формул (тавтологий) логики предикатов, т.е. научиться выводить (доказывать) все такие формулы и только их, исходя из выбранной системы аксиом и с использованием выбранных правил вывода.

Первоначальные понятия (язык формализованного исчисления предикатов). Алфавит исчисления предикатов состоит из предметных переменных $x_1, x_2, \dots$, предметных констант (символы выделенных элементов) $c_1, c_2, \dots$, предикатных букв $P'_1, P'_2, \dots, P'_k, \dots$, функциональных букв $f'_1, f'_2, \dots, f'_n, \dots$, а также знаков логических связей $\neg$ и $\wedge$, кванторов $\forall$ и $\exists$ и скобок $(,)$. При этом верхние индексы предикатных и функциональных букв указывают число аргументов соответственно предиката или функции, которые могут быть подставлены вместо этих букв.

Понятие *формулы* определяется в два этапа. Сначала определяются *термы*. Ими являются отдельно взятые предметные переменные и константы, а также выражения вида $f^n(t_1, \dots, t_n)$, где f^n — n -местный функциональный символ; $t_1, \dots, t_n$ — термы. Наконец, определяются формулы:

а) если P_n — предикатная буква, $t_1, \dots, t_n$ — термы, то $P_n(t_1, \dots, t_n)$ — формула; при этом все вхождения переменных в эту формулу называются *свободными*;

б) если F_1, F_2 — формулы, то формулами являются $\neg F_1, (F_1 \rightarrow F_2)$; причем все вхождения переменных, свободные в F_1, F_2 , являются свободными и в формулах указанных видов; кроме того, можно считать, что в F_1 и F_2 нет предметных переменных, которые связаны в одной формуле и свободны в другой;

в) если $F(x)$ — формула, содержащая свободные вхождения переменной x , то $(\forall x)(F(x))$ и $(\exists x)(F(x))$ — формулы; при этом вхождения переменной x в них называются *связанными*; вхождения же всех остальных предметных переменных в эти формулы остаются свободными (связанными), если они были свободными (связанными) в формуле $F(x)$ (формула $F(x)$ называется *областью действия квантора*);

г) никаких других формул, кроме тех, которые строятся по правилам а, б, в, нет.

Из этого определения ясно, что вхождения переменных в формулу обладают следующими свойствами: свободные и связанные переменные обозначены разными буквами (если это не так, то ясно, что, не нарушая смысла формулы, можно переобозначить в ней связанные переменные); если какой-либо квантор находится в области действия другого квантора, то переменные, связанные этими кванторами, обозначены разными буквами (если это не так, то ясно, что, не нарушая смысла формулы, можно переобозначить в ней соответствующие переменные). Нарушения этих свойств называются *коллизией переменных*. Определенные формулы называются *формулами первой степени*, так как в них разрешается навешивать кванторы только по предметным переменным, а по функциональным и предикатным — не разрешается. Возникающее исчисление предикатов называют *исчислением предикатов первой степени* или *узким исчислением предикатов* (в отличие от расширенного исчисления предикатов), сокращенно — УИП.

Совокупность $G = \{c_1, c_2, \dots; f_1, f_2, \dots; P_1, P_2, \dots\}$ называется *сигнатурой* рассматриваемого исчисления предикатов. Если в сигнатуре отсутствуют функциональные символы, (а значит, функциональные термы), то возникающее исчисление предикатов называется *чистым исчислением предикатов*. Оно строится для произвольной предметной области и не зависит от взаимосвязи между предметами в этой области. Это чисто логическая теория. Именно о таком чистом исчислении предикатов и пойдет речь. Если же такие связи имеются и они описываются функциями на этой предметной области, то логика проникает в эту область и в эти связи и возникает логическая теория соответствующей математической дисциплины, или, как говорят, некая *формальная математическая теория*. О таких теориях речь пойдет в § 30.

Система аксиом исчисления предикатов. Указанная система состоит из двух групп из которых первая — это аксиомы формализованного исчисления высказываний:

- (A1): $F \rightarrow (G \rightarrow F)$;
 (A2): $(F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$;
 (A3): $(\neg G \rightarrow \neg F) \rightarrow ((\neg G \rightarrow F) \rightarrow G)$,

где под F, G, H понимаются уже любые формулы исчисления предикатов.

Вторая группа аксиом (схем аксиом) — это собственно предикатные аксиомы (схемы аксиом), т. е. аксиомы с кванторами. Выберем в качестве них следующие (называемые *аксиомами Бернайса*):

(PA1): $(\forall x)(F(x)) \rightarrow F(y)$;

(PA2): $F(y) \rightarrow (\exists x)(F(x))$,

где $F(x)$ — любая формула, содержащая свободные вхождения x , причем ни одно из них не находится в области действия квантора по y (если таковой имеется); формула $F(y)$ получена из $F(x)$ заменой всех свободных вхождений x на y .

Существенность последнего требования можно пояснить следующим примером. Рассмотрим в качестве формулы $F(x)$ формулу $(\exists y)(P(x, y))$, где это требование нарушено: свободное вхождение x находится в области действия квантора $\exists y$. Подставив эту формулу в аксиому (PA1), получим формулу $(\forall x)(\exists y)(P(x, y)) \rightarrow (\exists y)(P(y, y))$, которая не будет общезначимой. В самом деле, предикат $A(x, y) : x < y$ на множестве вещественных чисел превращает ее в ложное высказывание: $(\forall x)(\exists y)(x < y) \rightarrow (\exists y)(y < y)$.

Правила вывода. К правилу вывода МР из исчисления высказываний добавляются еще два правила вывода:

$\forall$ -правило, или правило обобщения:
$$\frac{F \rightarrow G(x)}{F \rightarrow (\forall x)(G(x))};$$

$\exists$ -правило, или правило конкретизации:
$$\frac{G(x) \rightarrow F}{(\exists x)(G(x)) \rightarrow F}$$

при условии, что $G(x)$ содержит свободное вхождение x , а F не содержит.

Последнее требование также весьма существенно. Его нарушение может привести по этим правилам к ложным выводам из истинных посылок. Так, например, взяв предикаты $A(x) : 6|x$ и $B(x) : 3|x$ над N , получим тождественно истинный предикат $A(x) \rightarrow B(x) : 6|x \rightarrow 3|x$. Но применив к нему правило обобщения, получим уже опровержимый предикат: $6|x \rightarrow (\forall x)(3|x)$ (он превращается в ложное высказывание при тех x , которые делятся на 6). Если к предикату $6|x \rightarrow 3|x$ применить (в нарушение условия) $\exists$ -правило, то получим также опровержимый предикат $(\exists x)(6|x \rightarrow 3|x)$. Применив же к последнему предикату уже на корректных основаниях $\forall$ -правило, придем к ложному высказыванию $(\exists x)(6|x) \rightarrow (\forall x)(3|x)$.

Теория формального вывода. Определения формального доказательства (формального вывода из аксиом и из гипотез) доказуемой формулы (теоремы) в формализованном исчислении пре-

дикатов даются так же, как и в формализованном исчислении высказываний (см. определение 15.1), с точностью до добавления двух новых аксиомных схем (РА1) и (РА2) и двух новых правил вывода: $\forall$ -правила и $\exists$ -правила.

Уточним все же понятие формальной выводимости формулы из гипотез в исчислении предикатов. Формула G называется *выводимой из гипотез* $F_1, \dots, F_m$ с фиксированными вхождениями (в гипотезы) свободных переменных, если существует такая конечная последовательность формул $B_1, B_2, \dots, B_k, \dots, B_s \equiv G$, каждая формула которой является либо аксиомой, либо гипотезой, либо получена из предыдущих формул последовательности по одному из правил вывода. (Сама эта последовательность называется *выводом* G из гипотез $F_1, \dots, F_m$). При этом, если B_k есть первая гипотеза, встречающаяся в выводе, то дальше в этом выводе не могут быть использованы $\forall$ - и $\exists$ -правила вывода по любой переменной x , которая входит свободно хотя бы в одну из гипотез. Обозначение используется то же, что и в исчислении высказываний: $F_1, \dots, F_m \vdash G$. Если гипотезы отсутствуют, то говорят, что G *выводима из аксиом* (или просто *выводима*), и называют G *теоремой* формализованного исчисления предикатов и пишут $\vdash G$.

Отметим сначала, что так как все формулы, выводимые в исчислении высказываний, являются также выводимыми в исчислении предикатов, то, совершая подстановки в выводимые формулы исчисления высказываний, мы будем получать выводимые формулы исчисления предикатов. (Тем не менее всякую выводимую формулу исчисления предикатов таким способом получить нельзя.) Следовательно, все производные правила вывода, установленные для исчисления высказываний, остаются справедливыми и для исчисления предикатов, и мы будем в логике предикатов широко пользоваться этим.

Дальнейшее изучение формализованного исчисления предикатов происходит по Задачнику, § 11. Это исчисление строится там в форме систематизированной подборки задач на доказательство теорем ФИП. Подборка начинается с построения выводов из аксиом. Затем рассматривается построение выводов из гипотез. Наконец — теорема о дедукции и ее применение к доказательству теорем ФИП. Теорема о дедукции в ФИП формулируется так же, как и в ФИВ: если $F_1, \dots, F_{m-1}, F_m \vdash G$, то $F_1, \dots, F_{m-1} \vdash F_m \rightarrow G$ (в частности, если $F \vdash G$), то $\vdash F \rightarrow G$. Ничем особо не отличается и идея доказательства, с той лишь разницей, что появятся случаи, связанные с получением формулы в последовательности-выводе не только по правилу МР, но и по $\forall$ -правилу и по $\exists$ -правилу. Исчисление предикатов будет развито настолько, что все рассмотренные в § 21 тавтологии логики предикатов окажутся теоремами построенного формализованного исчисления предикатов. Что же касается свойств этого исчисления, то они будут рассмотрены в гл. 6 (§ 29).

Глава V

НЕФОРМАЛЬНЫЕ АКСИОМАТИЧЕСКИЕ ТЕОРИИ

Мы подошли к тому разделу курса математической логики, который должен убедительно продемонстрировать всю мощь воздействия методов этой науки на прочие математические науки, показать особую (цементирующую) роль математической логики в системе математических наук. Здесь необходимо увидеть отчетливую связь изученных понятий и методов со школьной математикой, с педагогической деятельностью учителя математики. Должна быть осознана всеобъемлющая, универсальная роль математической логики в вопросах обоснования математики вообще и школьного курса математики в особенности.

Можно сказать, что математическая наука достигает совершенства лишь тогда, когда ей удастся пользоваться аксиоматическим методом, т.е. когда наука принимает характер аксиоматической теории. Более того, развитие наук в XX в. показало, что математика выделяется в системе наук тем, что в ней чрезвычайно широко используется аксиоматический метод, который в значительной мере и обуславливает поразительную эффективность математики в процессе познания окружающего мира и преобразующего воздействия на него.

В настоящей главе рассматривается аксиоматический или дедуктивный метод построения математических теорий. Это рассмотрение проводится на неформальном (содержательном) уровне. В § 26 изложены основные сведения об аксиоматическом методе и аксиоматических теориях, приведены примеры таких теорий, возникших в разных областях математики. В § 27 дана характеристика свойств аксиоматических теорий — непротиворечивость, категоричность, полнота, независимость системы аксиом.

§ 26. Аксиоматический метод в математике и аксиоматические теории

Понятие аксиоматической теории. Аксиома (от греч. *axioma*) — положение, принимаемое без логического доказательства в силу непосредственной убедительности, является истинным исходным положением теории. Такой способ построения научной теории в

виде системы аксиом (постулатов) и правил вывода (аксиоматики) позволяет путем дедукции, т.е. по правилам логики, получать утверждения данной теории. Аксиоматический метод не является достижением только двадцатого столетия. В начале XX в. благодаря главным образом работам немецкого математика Д. Гильберта (1862—1943) окончательно сформировались принципиальные положения данного метода и было осознано его значение для математики. Первые идеи, связанные с этим методом, восходят к титанам античной мысли Платону и Аристотелю (IV в. до н. э.). Первый практический шаг на этом пути был сделан более двух тысяч лет назад древнегреческим математиком Евклидом (около 300 г. до н. э.). Его труд «Начала» (15 книг) как энциклопедия геометрических знаний служил образцом написания математических работ на протяжении более двадцати веков. Именно благодаря этому авторитетнейшему произведению сформировалось общечеловеческое представление об аксиоме как об утверждении, не требующем доказательства, обоснования, являющем собой некую абсолютную истину. Тем не менее внутри математической науки этот взгляд на аксиомы претерпевал самые решительные изменения. Такой процесс шел постепенно, но качественный скачок в нем произошел после того, как в 20—30-е гг. XIX в. великим русским математиком Н. И. Лобачевским (1792—1856) и независимо от него молодым венгром Яношем Бояи (1802—1860), а также великим немецким ученым К. Ф. Гауссом (1777—1855) были внесены изменения в представления о природе пространства, т.е. возникает неевклидова геометрия. Суть открытия состояла в том, что вместо пятого постулата Евклида о параллельных в систему аксиом было включено утверждение, являющееся его отрицанием, и затем на базе полученной системы аксиом была построена непротиворечивая геометрическая теория, названная Н. И. Лобачевским «воображаемой геометрией». Важным этапом в процессе эволюции взглядов на аксиомы явилось построение во второй половине XIX в. нескольких моделей геометрии Лобачевского. Оказалось, что терминам, входящим в аксиомы, и самим аксиомам можно придавать разный смысл, а не только тот наглядный, который имел в виду Евклид.

Такое развитие взглядов на природу аксиом и аксиоматический метод привело к следующей концепции *аксиоматической теории*. Выбирается ряд *первоначальных понятий*, которые не определяются и используются без объяснения их смысла. Вместе с тем все другие понятия, которые будут использоваться, должны быть строго определены через первоначальные неопределяемые понятия и через понятия, смысл которых был определен ранее. Высказывание, определяющее таким способом значение понятия, называется *определением*, а само понятие, смысл которого определен, носит название *определяемого понятия*. Евклид сделал попытку строго определить все первоначальные понятия геометрии: точки, прямые,

плоскости и т. д. Но эти понятия также должны определяться через свои понятия, которые, в свою очередь, опираются на следующие понятия, и так до бесконечности. Таким образом, первоначальные понятия аксиоматической теории не определяются.

Аналогична ситуация и с утверждениями о первоначальных и об определяемых понятиях. Невозможно доказать все истинные утверждения об этих понятиях, потому что при доказательстве нужно опираться на какие-то предыдущие утверждения, а при их доказательстве, в свою очередь, — на следующие, и так без конца. Поэтому и здесь необходимо выделить некоторые утверждения и объявить их истинными. Такие утверждения, принимаемые без доказательства, называются *аксиомами* аксиоматической теории. Совокупность аксиом обозначим буквой Σ . Вопрос о том, какие утверждения о первоначальных понятиях выбираются в качестве аксиом, заслуживает специального рассмотрения. Отметим только, что Евклид в качестве пяти своих аксиом (постулатов) выбрал наиболее, на его взгляд, очевидные утверждения о точках и прямых, т. е. такие утверждения, которые многократно подтверждались практическим опытом человечества.

Итак, после того как система аксиом аксиоматической теории выбрана, приступают к развитию самой аксиоматической теории. Для этого, исходя из выбранной системы аксиом и пользуясь правилами логического умозаключения, выводят новые утверждения о первоначальных понятиях, а также об определяемых понятиях. Получаемые утверждения называются *теоремами* данной аксиоматической теории.

Можно более точно сформулировать понятия теоремы аксиоматической теории и ее доказательства. *Доказательством* утверждения C , сформулированного в терминах данной теории, называется конечная последовательность $B_1, B_2, \dots, B_s$ высказываний теории, в которой каждое высказывание есть либо аксиома, либо оно получено из одного или большего числа предыдущих высказываний данной последовательности по логическим правилам вывода, а последнее высказывание B_s есть утверждение C . При этом C называется *теоремой* или *доказуемым утверждением* аксиоматической теории. Обозначение: $\vdash C$. Отметим, что каждая аксиома аксиоматической теории является ее теоремой: доказательство аксиомы есть одноэлементная последовательность, состоящая из нее самой.

Важным является следующее обобщение понятия теоремы. Пусть Γ — конечное множество высказываний некоторой аксиоматической теории. Утверждение C теории называется *выводимым* из Γ (обозначается: $\Gamma \vdash C$), если существует конечная последовательность высказываний $B_1, B_2, \dots, B_s$, называемая *выводом* C из Γ , каждое высказывание которой является либо аксиомой, либо высказыванием из Γ , либо получено из одного или большего числа предыдущих высказываний этой последовательности по какому-

либо из правил вывода рассматриваемой теории, а последнее высказывание B , есть утверждение C . Утверждения из множества Γ называются *гипотезами* (или посылками, или допущениями). В частном случае, когда $\Gamma = \emptyset$, вывод C из Γ превращается в доказательство утверждения C , а C становится теоремой аксиоматической теории.

Итак, под *аксиоматической теорией*, построенной на основе системы аксиом Σ , понимается совокупность всех теорем, доказываемых на основе этой системы аксиом. Такую совокупность теорем обозначают $Th(\Sigma)$.

Изложенный метод построения математической теории носит название *аксиоматического* или *дедуктивного метода*. Выбор системы аксиом есть дело условия: одно и то же утверждение теории может быть аксиомой, если оно так выбрано, а может выступать в качестве теоремы, если выбор аксиом осуществлен по-иному. Итак, если в обыденной жизни за термином «аксиома» утвердился его изначальный смысл (в переводе с греческого «аксиома» означает «достойный признания») — именно смысл самоочевидной, безусловной истины, то в математике при построении аксиоматических теорий аксиомы условны. Они «достойны признания» не сами по себе, не ввиду их самоочевидной истинности, а потому, что на их основе строится та или иная аксиоматическая теория. При новом выборе системы аксиом прежние аксиомы становятся теоремами. Иначе говоря, аксиомы — это то, из чего выводятся теоремы, а теоремы — то, что выводится из аксиом.

Как возникают аксиоматические теории. Можно проследить два пути, по которым происходило становление тех или иных аксиоматических теорий, известных в математике.

Первый путь можно охарактеризовать тем, что та или иная математическая теория, достигнув достаточно высокого уровня развития, принимает характер аксиоматической теории. Подобным образом произошла аксиоматизация таких математических теорий, как арифметика (на основе системы аксиом Дж. Пеано), геометрия (на основе систем аксиом Д. Гильберта, Г. Вейля, М. Пиери и др.), теория вероятностей (аксиоматика А. Н. Колмогорова) и т.д.

Второй путь возникновения аксиоматических теорий связан с процессом постепенного осознания глубокого внутреннего сходства основных черт, казалось бы, совершенно разных математических теорий, с попыткой выделить общие черты, с тем чтобы, руководствуясь ими, построить аксиоматическую теорию. (Может быть, именно поэтому Д. Гильберт считал математику искусством называть разные вещи одним и тем же именем.) На этом пути возникли, по-видимому, все алгебраические (аксиоматические) теории, прежде всего теории групп, колец, полей и других алгебраических систем, общая или универсальная алгебра и т.д.

Именно на этом пути появляется прекрасная возможность взаимопроникновения методов одних математических наук в другие, а также возможность свободно интерпретировать первоначальные понятия и аксиомы аксиоматической теории, что раскрывает широкие перспективы для приложений таких теорий и является одним из мощных источников действенной силы математики как науки вообще.

Примеры аксиоматических теорий. Приведем примеры аксиоматических теорий, возникших различными путями.

Пример 26.1. Теория групп — одна из теорий, возникших на втором пути. Было известно немало объектов, обладающих многими общими чертами. Среди них, в частности: множество $F_{1-1}(M)$ всех взаимно-однозначных отображений множества M на себя, рассматриваемое вместе с операцией суперпозиции отображений; множество Z всех целых чисел, рассматриваемое вместе с операцией сложения целых чисел; множество V_2 всех векторов плоскости, рассматриваемое вместе с операцией сложения векторов по правилу треугольника или параллелограмма. Обозначив каждое из этих множеств через G , а каждую из операций через $*$ (и называя ее композицией элементов из G), обнаруживаем, что все три указанных объекта обладают следующими свойствами:

(G_0): Для любых a и b из G композиция $a * b$ есть однозначно определенный элемент из G ;

(G_1): Для любых a, b и c из G $(a * b) * c = a * (b * c)$;

(G_2): В G имеется такой элемент e , что для любого a из G $a * e = e * a = a$;

(G_3): Для любого a из G имеется такой a' из G , что $a * a' = a' * a = e$.

Например, элемент e , существование которого утверждается в свойстве G_2 , в случае $F_{1-1}(M)$ есть тождественное отображение M на M , в случае Z — целое число 0, в случае V_2 — нуль-вектор $\vec{0}$. В свойстве G_3 элемент a' есть обратное преобразование f^{-1} (противоположное число $-m$, противоположный вектор $\overrightarrow{BA}$) для преобразования f (целого числа m и вектора $\overrightarrow{AB}$ соответственно). Утверждения $G_0 - G_3$ и составляют систему аксиом теории групп. Из этих аксиом можно выводить разнообразные теоремы и тем самым строить аксиоматическую теорию групп. Докажем несколько теорем этой теории.

(G_4): В группе имеется точно один единичный элемент.

Доказательство. Ввиду G_2 нужно доказать лишь единственность. Допустим, что в G имеются два единичных элемента: e_1 и e_2 , т.е. на основании G_2 для любого a справедливы равенства $e_1 * a = a$ и $a * e_2 = a$. Тогда, в частности, $e_1 * e_2 = e_2$ и $e_1 * e_2 = e_1$. Следовательно, в силу G_0 и свойств равенства $e_1 = e_2$. $\square$

(G_5): Для каждого элемента группы имеется точно один обратный.

Доказательство. Ввиду G_3 остается доказать лишь его единственность. Допустим, что в G для элемента a имеются два обратных a' и a'' , т. е. таких элементов, что $a'' * a = e$ и $a * a' = e$. Тогда в силу G_1 $(a'' * a) * a' = a''$, а следовательно, $e * a' = a'' * e$. Отсюда следует, согласно G_2 , что $a' = a''$. $\square$

В мультипликативной терминологии обратный элемент для a обозначается через a^{-1} , так что $a^{-1} * a = a * a^{-1} = e$, где e — единственный единичный элемент из G .

(G_6) : Для любых элементов a, b, c группы G из $a * b = a * c$ следует $b = c$, и из $b * a = c * a$ следует $b = c$.

Доказательство. Пусть $a * b = a * c$. Тогда $a^{-1} * (a * b) = (a^{-1} * a) * b = e * b = b$. С другой стороны, $a^{-1} * (a * b) = a^{-1} * (a * c) = (a^{-1} * a) * c = e * c = c$. Следовательно, $b = c$. Второе утверждение доказывается аналогично.

Следующие две теоремы докажите самостоятельно.

(G_7) : Для любых элементов a и b из G каждое из уравнений $a * x = b$ и $y * a = b$ имеет в G единственное решение.

(G_8) : Для любых элементов a и b из G $(a * b)^{-1} = b^{-1} * a^{-1}$.

Пример 26.2. Как отмечалось в предыдущем пункте, примером аксиоматической теории, возникшей на первом пути, является геометрия. Здесь рассматривается ее маленький фрагмент — теория конгруэнтности (равенства) отрезков. Условимся, что первичными терминами являются S — множество всех отрезков и $\equiv$ — отношение, называемое отношением конгруэнтности, так что выражение $x \equiv y$ означает так: отрезок x конгруэнтен отрезку y . Выберем в качестве аксиом следующие утверждения:

(K_1) : Для всякого x из S справедливо $x \equiv x$ (другими словами, каждый отрезок конгруэнтен самому себе).

(K_2) : Для любых элементов x, y, z из S , если $x \equiv z$ и $y \equiv z$, то $x \equiv y$ (другими словами, два отрезка, порознь конгруэнтные третьему, конгруэнтны между собой).

Докажем некоторые теоремы.

(K_3) : Для любых элементов y и z из S , если $y \equiv z$, то $z \equiv y$.

Доказательство. По аксиоме K_2 , подставив z вместо x , получим, что если $z \equiv z$ и $y \equiv z$, то $z \equiv y$. Поскольку член конъюнкции $z \equiv z$ истинен на основании аксиомы K_1 , то из конъюнкции его можно убрать. Получим, что если $y \equiv z$, то $z \equiv y$. $\square$

(K_4) : Для любых элементов x, y, z из S , если $x \equiv y$ и $y \equiv z$, то $x \equiv z$.

Докажите самостоятельно. (См. также Задачник, № 16.3 — 16.6.)

Пример 26.3. Аксиоматическая теория натуральных чисел построена итальянским математиком Дж. Пеано (1858—1932) на рубеже XIX — XX вв. Ее первоначальными понятиями являются: непустое множество N , бинарное отношение «'» (называемое отношением следования) и выделенный элемент 1. Аксиомы выбираются следующие:

$(P_1): (\forall x)(x' \neq 1);$

$(P_2): (\forall x, y)(x = y \rightarrow x' = y');$

$(P_3): (\forall x, y)(x' = y' \rightarrow x = y);$

$(P_4): (\text{Аксиома индукции}) (1 \in M \wedge (\forall x)(x \in M \rightarrow x' \in M)) \rightarrow M = N.$

Правилами вывода служат обычные логические правила МР и правило подстановки.

Приведем доказательства двух теорем, непосредственно вытекающих из этих аксиом.

$(P_5): (\forall x)(x' \neq x).$

Доказательство. Рассмотрим множество: $M = \{x \in N: x' \neq x\}.$

Покажем, используя аксиому индукции (P_4) , что $M = N.$

$1 \in M$, так как $1' \neq 1$ по аксиоме $P_1.$

Пусть $x \in M$, т.е. $x' \neq x$. Тогда, по аксиоме P_3 $(x')' \neq x'$. Следовательно, по определению $x' \in M.$

Условия аксиомы P_4 выполнены. Тогда, по аксиоме P_4 $M = N.$

Это и означает, что $(\forall x)(x' \neq x).$ $\square$

$(P_6): (\forall x)(x = 1 \vee (\exists y)(x = y')).$

Доказательство. Рассмотрим множество: $M = \{1\} \cup \{x \in N: (\exists y)(x = y')\}$ и покажем, используя аксиому индукции P_4 , что $M = N.$

$1 \in M$ по определению множества.

Пусть $x \in M$ и $x \neq 1$. Тогда $x \in \{x \in N: (\exists y)(x = y')\}$, т.е. $x = y'$ для некоторого $y \in N$. Отсюда, ввиду аксиомы P_2 , $x' = (y')'$, т.е. x' следует за элементом y' . Тогда, по определению M элемент $x' \in M.$

Условия аксиомы P_4 выполнены. Тогда, по аксиоме P_4 $M = N.$ $\square$

Аксиоматической теории натуральных чисел, построенной на основе приведенной системы аксиом, много времени уделяется в курсе «Числовые системы», изучаемом после курса математической логики.

Пример 26.4 (построение евклидовой геометрии на основе системы аксиом Гильберта). Эта система аксиом представлена Гильбертом в его книге «Основания геометрии», вышедшей в 1899 г. и ставшей с того момента вечным фундаментом этой науки. Гильберт так начинает свое сочинение: «Геометрия, так же как и арифметика, требует для своего построения только немногих простых основных положений. Эти основные положения называются «аксиомами геометрии». Установление аксиом геометрии и исследование их взаимоотношений — это задача, которая со времен Евклида являлась темой многочисленных прекрасных произведений математической литературы. Задача эта сводится к логическому анализу нашего пространственного представления.» [3.5, с. 55].

В системе Гильберта первоначальными (неопределяемыми) понятиями являются понятия трех объектов — «точки», «прямые» и «плоскости» и трех сортов отношений между ними, выражаемых словами «принадлежит» (точка принадлежит прямой или плоскости), «между» (точка лежит между двумя другими точками) и «конгруэнтен» (кон-

груэнтны два отрезка или два угла). При этом точки обозначаются $A, B, C, \dots$, прямые — $a, b, c, \dots$, плоскости — $\alpha, \beta, \gamma, \dots$. Эти объекты и эти отношения между ними удовлетворяют двадцати аксиомам, разделенным на пять групп: I. Аксиомы принадлежности (или инцидентности); II. Аксиомы порядка; III. Аксиомы конгруэнтности; IV. Аксиомы непрерывности; V. Аксиома параллельности Евклида.

Пример 26.5 (построение евклидовой геометрии на основе системы аксиом Вейля). Эта система предложена немецким математиком Германом Вейлем в 1916 г., и путь построения геометрии, основанный на этой системе аксиом, возможно, является самым коротким и динамичным путем аксиоматизации геометрии. К тому же на этом пути в элементарную геометрию входит одно из фундаментальнейших понятий современной математики — понятие векторного пространства, чрезвычайно важное и для многочисленных ее приложений (к физике, химии, экономике и т.д.). Идея Вейля состоит в том, чтобы принять в качестве первоначальных, неопределяемых понятий понятия «точка», «вектор» (в частности, понятия «прямая» и «плоскость» определяются), «сумма векторов», «произведение вектора на число», «скалярное произведение векторов», «откладывание вектора от точки», а в качестве аксиом — свойства этих операций над векторами и некоторые свойства, связывающие точки и векторы.

С логической точки зрения вейлевский путь аксиоматизации эквивалентен гильбертовскому: он позволяет доказать все те же самые теоремы. Но с методологической точки зрения вейлевский путь имеет ряд преимуществ. Вместо скрупулезных и утомительных рассуждений по гильбертовской схеме путь Вейля дает ясное и краткое изложение, насыщенное современными идеями и мощными методами решения геометрических задач.

Система аксиом Вейля включает 16 аксиом, которые отчетливо делятся на две части: аксиомы векторного (евклидова) пространства и аксиомы точечного пространства в его связи с векторным пространством. Здесь важно отметить, что понятие векторного пространства размерности n без преувеличения играет фундаментальную роль во всех областях современной математики и сопредельных с ней наук. Оно изучалось также в курсе алгебры и в курсе математического анализа. Исключительно важна его роль и в геометрии. Геометрия изучает точки и фигуры — множества точек (но не векторы, с которыми имеет дело *векторное* пространство). Понятие точки — следующее неопределяемое понятие. Точки и векторы — объекты разной природы, но они очень тесно связаны между собой. Эта связь выражена во второй части аксиом — *аксиомах Вейля точечного пространства*. Имеется отображение, сопоставляющее любым двум точкам A и B (в указанном порядке) вектор из векторного пространства V , обозначаемый $\overrightarrow{AB}$. Это отображение должно удовлетворять следующим аксиомам:

$$(V_1): (\forall A)(\forall \bar{a})(\exists B)(\overline{AB} = \bar{a});$$

$$(V_2): (\forall A, M, N)(\overline{AM} = \overline{AN} \rightarrow M = N);$$

$$(V_3): (\forall A, B, C)(\overline{AB} + \overline{BC} = \overline{AC}).$$

Первая из этих аксиом называется аксиомой откладывания векторов: от каждой точки любой вектор можно отложить. Вторая аксиома утверждает, что это отложение осуществляется единственным образом: заданные начальная точка и вектор однозначно определяют конечную точку. Наконец, третья аксиома называется аксиомой треугольника.

Итак, пространство векторов (векторное пространство) и пространство точек (точечное пространство) — разные объекты, но очень тесно связанные между собой. Говорят, что точечное пространство рассматривается (или задано) над векторным пространством и что векторное пространство является пространством переносов соответствующего точечного пространства. Если векторное пространство V_n не является евклидовым (т. е. в нем не задано скалярное произведение), то соответствующее точечное пространство обозначается A_n и называется *аффинным*. Если векторное пространство V_n является евклидовым (в нем задано скалярное произведение векторов), то соответствующее точечное пространство обозначается E_n и называется *евклидовым точечным пространством*.

Таким образом, система аксиом векторного пространства вместе с аксиомами (V_1) , (V_2) , (V_3) и есть *система аксиом евклидовой геометрии по Герману Вейлю*. Все дальнейшие понятия (как то: прямая, плоскость и т. д.) вводятся при помощи определений на основе уже введенных первоначальных понятий, т. е. являются определяемыми, вторичными. Все теоремы о первоначальных и вторичных понятиях доказываются на основе сформулированных аксиом (с использованием, конечно, уже доказанных теорем). При этом фундаментальным с точки зрения логики является тот факт, что всякая аксиома системы аксиом Гильберта оказывается теоремой при вейлевском подходе к обоснованию геометрии. Отсюда следует, что всякая теорема евклидовой геометрии, выводимая из системы аксиом Гильберта, может быть выведена и из системы аксиом Вейля (к выводу теоремы из системы аксиом Гильберта нужно добавить вначале выводы необходимых аксиом Гильберта из системы аксиом Вейля). Верно и обратное утверждение. Тот факт, что из системы аксиом Гильберта выводится каждое утверждение о векторах, которое Вейлем принято за аксиому, фактически и доказывается в разных курсах элементарной математики, в которых понятие вектора сделано вторичным. Отсюда и следует, что всякая теорема евклидовой геометрии, выводимая из системы аксиом Вейля, может быть выведена и из системы аксиом Гильберта. Таким образом, системы аксиом Гильберта и Вейля оказываются эквивалентными: на основе каждой из них могут быть доказаны одни и те же теоремы евклидовой геометрии.

Пример 26.6 Геометрия Лобачевского может быть построена, например, на базе системы аксиом Гильберта евклидовой геометрии, о которой говорилось в примере 26.4, если в этой системе аксиому параллельности Евклида заменить аксиомой параллельности Лобачевского, представляющей собой отрицание аксиомы параллельности Евклида.

Пример 26.7 (аксиоматическое построение канторовской («навивной») теории множеств на основе нескольких систем аксиом). Читатель, знакомый с основами современной алгебры, узнает в приводимых системах аксиом аксиоматики так называемой «булевой алгебры», так как совокупность всех подмножеств данного множества образует алгебраическую систему, называемую булевой алгеброй. Всего рассмотрим три системы аксиом.

Первоначальными понятиями теории T_1 являются бинарные операции $\cap$, $\cup$ (называемые соответственно пересечением и объединением), унарная операция $'$ (называемая дополнением) и нульарные операции 0 и 1 , фиксирующие два разных элемента — нулевой и единичный. Система аксиом Σ_1 этой теории симметрична относительно операций $\cap$, $\cup$, 0 , 1 (или, как говорят, самодвойственна):

(A1): $x \cap y = y \cap x$;	(A5): $x \cap 1 = x$;
(A2): $x \cup y = y \cup x$;	(A6): $x \cup 0 = x$;
(A3): $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$;	(A7): $x \cap x' = 0$;
(A4): $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$;	(A8): $x \cup x' = 1$.

Первоначальными понятиями второй теории T_2 являются бинарная операция $\cap$ и унарная операция $'$. Система аксиом Σ_2 этой теории, наоборот, асимметрична, «смещена» в сторону операции $\cap$:

(B1): $x \cap y = y \cap x$;	(B3): $x \cap y' = z \cap z' \Rightarrow x \cap y = x$;
(B2): $(x \cap y) \cap z = x \cap (y \cap z)$;	(B4): $x \cap y = x \Rightarrow x \cap y' = z \cap z'$.

Наконец, в третьей теории T_3 , в которой первоначальными понятиями являются бинарное отношение $\subset$, бинарные операции $\cap$ и $\cup$, унарная операция $'$ и нульарные операции 0 и 1 , система аксиом Σ_3 следующая:

(C1): $x \subset x$;	(C6): $x \subset 1$;
(C2): $x \subset y \wedge y \subset z \Rightarrow x \subset z$;	(C7): $0 \subset x$;
(C3): $x \cup y \subset z \Rightarrow x \subset z \wedge y \subset z$;	(C8): $1 \subset x \cup x'$;
(C4): $z \subset x \cap y \Rightarrow z \subset x \wedge z \subset y$;	(C9): $x \cap x' \subset 0$.
(C5): $x \cap (y \cup z) \subset (x \cap y) \cup (x \cap z)$;	

Можно доказать равносильность всех этих трех систем аксиом.

Интерпретации и модели аксиоматической теории. Формулируя аксиомы в примерах предыдущего пункта, мы не обращали никакого внимания на природу элементов тех множеств, которые там встречаются, а также на природу других первоначальных понятий этих аксиоматических теорий.

Определение 26.8. Приписывание значений (смысла) первоначальным понятиям аксиоматической теории называется *интерпретацией* теории. Если некоторая совокупность предметов и отношений между ними, выбранных в качестве значений первоначальных понятий аксиоматической теории, т. е. в качестве ее интерпретации, удовлетворяет всем аксиомам теории, то она называется *моделью* данной аксиоматической теории (или моделью системы аксиом теории).

Другими словами, интерпретация теории — просто функция f , областью определения которой является множество T первоначальных понятий этой теории. Если же образ $f[T]$ удовлетворяет всем аксиомам теории, то это есть модель данной теории.

Так, в примере 26.1 каждое из множеств $F_{1-1}(M)$, Z и V_2 , рассматриваемое вместе с соответствующей операцией, является моделью аксиоматической теории групп или, проще, группой. Существуют многочисленные другие модели данной теории. Вот в этой-то свободе интерпретаций аксиоматических теорий заключена одна из причин их обширных приложений в других науках и в практике. Но искусство интерпретации поистине одно из высочайших искусств математика-прикладника. Например, теория групп была с успехом применена в 1890 г. русским кристаллографом Е. С. Федоровым (1853 — 1919) для классификации и описания всевозможных форм кристаллов, существующих в природе, а в самое последнее время эта теория плодотворно работает в теории элементарных частиц.

Дадим аксиоматической теории, основанной на аксиомах K_1 и K_2 (пример 26.2), еще одну интерпретацию. В качестве первоначальных понятий возьмем множество R всех действительных чисел и отношение $\equiv$, определяемое так: $x \equiv y$ тогда и только тогда, когда разность $x - y$ есть целое число. Нетрудно убедиться в том, что при такой интерпретации аксиомы K_1 и K_2 превращаются в истинные утверждения (в теоремы теории действительных чисел). Следовательно, получаем модель аксиоматической теории $Th(K_1, K_2)$.

Наконец, укажем две модели теории $Th(P_1 - P_4)$ натуральных чисел. Если интерпретировать N как множество $\{1, 2, 3, \dots\}$ натуральных чисел, а отношение $'$ интерпретировать как функцию следования (т. е. $x' = x + 1$), то аксиомы $P_1 - P_4$ будут выражать общеизвестные свойства натуральных чисел, т. е. получим модель рассматриваемой аксиоматической теории.

Ранее уже отмечалась возможность взаимопроникновения методов одних математических наук в другие в процессе создания аксиоматической теории. Проиллюстрируем это на примерах. Так, доказав в аксиоматической теории групп теорему G_8 , можно интерпретировать ее для конкретных моделей данной теории. В частности, на модели $F_{1-1}(M)$ она превращается в утверждение $(g * f)^{-1} = f^{-1} * g^{-1}$, а на модели V_2 — в утверждение $-(\bar{a} + \bar{b}) = -(\bar{a}) + (-\bar{b})$. Таким образом, природа этих, казалось бы, разнородных свойств одна — теоретико-групповая. Аналогично, без како-

го бы то ни было специального рассуждения мы уверены в том, что теоремы K_3 и K_4 станут истинными утверждениями о действительных числах при интерпретации, рассмотренной в настоящем пункте.

Но не только аксиоматическая теория привносит что-то в свои модели. Имеется и обратная связь: порой модели аксиоматической теории могут сослужить ей определенную службу при решении некоторых внутренних проблем теории. Пусть, например, требуется выяснить, является или нет теоремой теории $Th(K_1, K_2)$ следующее высказывание:

А: «Существуют два элемента x и y множества S , для которых неверно, что $x \equiv y$ (другими словами, существуют два неконгруэнтных отрезка)».

То обстоятельство, что не удастся получить вывод данного утверждения из аксиом K_1, K_2 , приводит к догадке (гипотезе), что это сделать невозможно. Для ее подтверждения рассуждаем следующим образом. Если бы утверждение А было выводимо из аксиом K_1, K_2 , т.е. принадлежало бы аксиоматической теории $Th(K_1, K_2)$, то ему удовлетворяла бы каждая модель этой теории. Поэтому, если удастся построить такую модель системы аксиом $\{K_1, K_2\}$, в которой не выполняется утверждение А, то догадка (гипотеза) будет подтверждена, т.е. А невозможно вывести из K_1 и K_2 . В самом деле, рассмотрим, например, множество всех целых чисел и введенное выше отношение $\equiv$ между его элементами: $x \equiv y$ тогда и только тогда, когда $x - y \in \mathbb{Z}$. На этой структуре, как мы уже отмечали, аксиомы K_1 и K_2 выполняются. Но совершенно ясно, что утверждение А на данной модели не выполняется, потому что $x \equiv y$ для любых элементов x и y из $\mathbb{Z}$.

§ 27. Свойства аксиоматических теорий

В настоящем параграфе речь пойдет об изучении аксиоматической теории как таковой. Математическую теорию, изучающую данную аксиоматическую теорию как единое целое, устанавливающую свойства данной аксиоматической теории, называют *метатеорией* по отношению к изучаемой теории, и методы математической логики являются основными методами этой науки. Факты, устанавливаемые в ней относительно изучаемой аксиоматической теории, называют *метатеоремами*, чтобы отличить их от собственно теорем рассматриваемой теории. Вопросы, связанные с моделями данной аксиоматической теории, с ее непротиворечивостью, категоричностью, полнотой, со свойством независимости ее системы аксиом, — это и есть важнейшие вопросы, на которые должна дать ответ метатеория изучаемой аксиоматической теории. Эти понятия вкратце были изложены в гл. 3 при построении формализованного исчисления высказываний, а также при построении формализованного исчисления предикатов. Теперь же рассмотрим их более обстоятельно применительно к произвольной аксиоматической теории.

Непротиворечивость. Это важнейшее свойство аксиоматических теорий и важнейшее требование, предъявляемое к ним, поскольку, как увидим ниже, противоречивые теории никакой ценности не представляют.

Определение 27.1. Аксиоматическая теория называется *непротиворечивой*, если ни для какого утверждения A , сформулированного в терминах этой теории, само утверждение A и его отрицание $\neg A$ не могут быть одновременно теоремами этой теории. Если для некоторого утверждения A теории оба утверждения A и $\neg A$ являются ее теоремами, то аксиоматическая теория называется *противоречивой*.

Покажем, что *если аксиоматическая теория противоречива, а используемая в ней логическая система включает исчисление высказываний с правилом вывода modus ponens (MP), то любое предложение C этой теории является ее теоремой*.

Доказательство. В самом деле, ввиду противоречивости теории существует предложение A теории, такое, что A и $\neg A$ — ее теоремы. Рассмотрим следующую последовательность высказываний данной теории: ..., A , ..., $\neg A$, B_1 , B_2 , ..., B_s , $A \rightarrow (\neg A \rightarrow C)$, $\neg A \rightarrow C$, C . Многогочия перед A и $\neg A$ обозначают их выводы. Следующее $s + 1$ высказывание — вывод истинного высказывания $A \rightarrow (\neg A \rightarrow C)$ (эта формула есть тавтология, что легко проверить, и потому доказуема). Наконец, предпоследняя формула получена из A и $A \rightarrow (\neg A \rightarrow C)$ по правилу MP, а последняя — по тому же правилу из $\neg A$ и $\neg A \rightarrow C$. Таким образом, данная последовательность есть доказательство утверждения C в рассматриваемой аксиоматической теории. $\square$

Ясно, что обратное утверждение также справедливо: *если любое предложение аксиоматической теории является ее теоремой, то теория противоречива*.

Следовательно, определения противоречивой и непротиворечивой аксиоматической теорий можно сформулировать и следующим равносильным образом. Аксиоматическая теория называется *противоречивой*, если любое утверждение, сформулированное в терминах этой теории, является ее теоремой, и называется *непротиворечивой*, если существует утверждение, не являющееся ее теоремой. Значит, противоречивая теория никакой ценности не имеет, потому что в ней можно доказать что угодно.

В связи со сказанным приобретает первостепенную важность проблема установления непротиворечивости аксиоматической теории. Ясно, что эта проблема имеет две стороны: отсутствие заложенного как бы внутри системы аксиом противоречия (которое проявится при развитии теории) и истинность логических умозаключений, которые мы используем при построении доказательств. Таким образом, желая установить непротиворечивость той или иной аксиоматической теории, мы должны подвергнуть исследованию как ее математическое содержание (т.е. систему аксиом, лежащую в ее

основе), так и саму логику. Ко второму моменту мы еще вернемся в гл. 6, а сейчас посмотрим, как же решается вопрос о непротиворечивости системы аксиом, положенной в основу аксиоматической теории, об отсутствии противоречия внутри нее.

Во многих случаях этот вопрос удастся решить с помощью понятия модели. Развивая аксиоматическую теорию на базе той или иной системы аксиом Σ , мы не вкладываем в ее основные понятия и отношения между ними никакого содержания сверх того, что сказано о них в аксиомах; в них содержатся все сведения об этих понятиях, необходимые для построения теории путем чисто логических умозаключений. Изменим теперь нашу точку зрения на первоначальные понятия: будем понимать под ними некоторые вполне определенные объекты и соотношения между ними из какой-нибудь области математики (другой аксиоматической теории), которую мы считаем уже установленной и обоснованной (непротиворечивой). Это придание каждому первоначальному понятию и отношениям между ними конкретного содержания посредством каких-то конкретных предметов и конкретных отношений между ними, как мы говорили в предыдущем параграфе, называется *интерпретированием* данной системы аксиом Σ . Совокупность этих конкретных предметов и отношений между ними называется *интерпретацией* данной системы аксиом. В результате каждая аксиома из Σ превращается во вполне определенное предложение из той уже обоснованной области математики (непротиворечивой аксиоматической теории), которая используется для интерпретации. Каждое из этих предложений может быть как истинным (теоремой), так и ложным в непротиворечивой аксиоматической теории, использованной для интерпретации. Если все аксиомы из Σ превращаются в истинные утверждения, то построенная интерпретация называется *моделью* данной системы аксиом Σ . (Если же хотя бы одна аксиома превратилась в ложное утверждение, то можно считать, что интерпретирование не удалось: ведь цель интерпретирования — построить модель системы аксиом!)

Если модель системы аксиом Σ построена, то отсюда следует чрезвычайно важный вывод о непротиворечивости этой системы аксиом. В самом деле, все теоремы аксиоматической теории $Th(\Sigma)$, построенной на базе системы аксиом Σ , суть чисто логические следствия аксиом из Σ . В результате интерпретирования все аксиомы из Σ превратились в истинные предложения; значит, логически следующие из них теоремы также превратятся в истинные предложения (в смысле той аксиоматической теории, которая использована для построения модели). Поэтому, если предположить, что в исследуемой аксиоматической теории (построенной на базе системы аксиом Σ) могут быть выведены две теоремы A и $\neg A$, противоречащие друг другу, то в модели им соответствовали бы два истинных утверждения A^* и $\neg A^*$, также друг другу противоречащих (утверждение и его отрицание не могут быть одновременно

истинными). Но это невозможно, так как аксиоматическая теория, в которой мы рассматриваем модель нашей системы аксиом Σ , считается свободной от противоречий (непротиворечивой).

Итак, предъявляемая модель системы аксиом служит обоснованием непротиворечивости соответствующей аксиоматической теории. Но, поскольку модель исходной системы аксиом Σ построена в некоторой другой аксиоматической теории, такое обоснование имеет *относительный характер*: исходная теория непротиворечива, если непротиворечива аксиоматическая теория, в терминах которой построена ее модель. Таким образом, вопрос о непротиворечивости одной аксиоматической теории сводится к вопросу о непротиворечивости другой аксиоматической теории.

Именно такова ситуация с геометрией Н. И. Лобачевского. Хорошо известны различные модели геометрии Лобачевского, построенные в геометрии Евклида. Наличие такой модели доказывает относительную непротиворечивость геометрии Лобачевского: она непротиворечива, если непротиворечива геометрия Евклида. В свою очередь, непротиворечивость геометрии Евклида также требует обоснования. Далее в курсе геометрии строится модель евклидовой геометрии в теории действительных чисел, чем устанавливается непротиворечивость первой относительно второй. Наконец, вопрос о непротиворечивости теории действительных чисел может быть сведен путем построения соответствующих моделей к вопросу о непротиворечивости теории натуральных чисел, построенной на основе системы аксиом Пеано. Подробнее об этом речь пойдет в § 28.

К непротиворечивости арифметики аналогичным образом сводится непротиворечивость обширных областей классической математики. Тем не менее «абсолютная» непротиворечивость ни геометрии Лобачевского, ни евклидовой геометрии, ни арифметики натуральных чисел не установлена. Уверенность в непротиворечивости этих теорий, в их истинности есть своего рода акт веры.

В заключение отметим, что если удастся построить конечную модель аксиоматической теории, то этим устанавливается «абсолютная» непротиворечивость теории. Например, двухэлементное множество $\{e, a\}$ вместе с определенной на нем по следующим правилам операций: $e \cdot e = a \cdot a = e$, $e \cdot a = a \cdot e = a$ является, как нетрудно убедиться, моделью теории групп. Поэтому с полной уверенностью можно утверждать, что аксиоматическая теория групп непротиворечива.

Категоричность. Это свойство в значительной мере характеризует происхождение аксиоматической теории (см. § 26, п. «Как возникают аксиоматические теории»). В большинстве категоричные теории возникали на первом пути. По второму пути происходит формирование в основном некатегоричных теорий.

Проанализируем первый путь. Аксиоматика строится для одной конкретной содержательной теории, которая развита уже доста-

точно хорошо. Эта конкретная теория выступает в качестве модели аксиоматической теории. Никаких других моделей построенная аксиоматическая теория и не имеет, поскольку она строилась применительно к данной конкретной теории. Точнее, другие модели теории могут существовать, но они должны быть неотличимы (с точностью до терминологии и обозначений) от исходной модели. В этом случае можно сказать, что первоначальные понятия и аксиомы дают исчерпывающую совокупность главных принципов конкретной содержательной теории. Такая неотличимость двух моделей называется их *изоморфизмом*. (Из курса высшей алгебры известны понятия изоморфизма групп, колец, полей. Поэтому имеется представление о точном определении изоморфизма для конкретных моделей.) Аксиоматическая теория в этом случае и называется категоричной.

Определение 27.2. Аксиоматическая теория называется *категоричной*, если любые две ее модели изоморфны.

Примерами категоричных теорий служат аксиоматические теории евклидовой геометрии, различных систем чисел: натуральных, целых, рациональных, действительных, комплексных. Категоричность евклидовой геометрии доказывается в курсе геометрии. Категоричность теорий систем чисел устанавливается в курсе «Числовые системы».

Некатегоричная аксиоматическая теория имеет существенно различные (т.е. неизоморфные) модели. Такие теории возникают на втором пути, в процессе обобщения общих свойств нескольких различных конкретных теорий. Примером такой теории является теория групп. Многообразие моделей этой теории обуславливает многообразие ее приложений. Некатегоричны также теория колец, теория полей и теории некоторых других алгебраических систем.

Независимость системы аксиом. Мы уже имели дело с понятием независимости системы аксиом, когда устанавливалась независимость системы аксиом аксиоматической теории высказываний. Здесь обсудим его более подробно. Сформулируем сначала определения понятия независимости аксиомы от остальных аксиом данной системы в двух формах и докажем их равносильность.

Определение 27.3. Аксиома A из системы аксиом Σ называется *независящей* от остальных аксиом этой системы, если ее нельзя вывести (доказать) из множества $\Sigma \setminus \{A\}$ всех остальных аксиом системы Σ .

Определение 27.4. Аксиома A из системы аксиом Σ называется *независящей* от остальных аксиом этой системы, если ее исключение из системы Σ уменьшает запас теорем аксиоматической теории, т.е. $Th(\Sigma \setminus \{A\}) \subset Th(\Sigma)$, где $Th(\Sigma)$ — совокупность всех теорем, выводимых из системы аксиом Σ , т.е. аксиоматическая теория, построенная на базе системы аксиом Σ .

Определения 27.3, 27.4 равносильны.

Доказательство. В самом деле, из первого определения вытекает второе, так как если утверждение A нельзя вывести из мно-

жества $\Sigma \setminus \{A\}$, то его не будет среди теорем теории $Th(\Sigma \setminus \{A\})$ и оно будет среди теорем теории $Th(\Sigma)$, т.е. $Th(\Sigma \setminus \{A\}) \subset Th(\Sigma)$. Обратно, если $Th(\Sigma \setminus \{A\}) \subset Th(\Sigma)$, то A нельзя вывести из $\Sigma \setminus \{A\}$, ибо в противном случае, каждая теорема, выводимая из Σ , могла бы быть выведена и из $\Sigma \setminus \{A\}$, т.е. каждая теорема из $Th(\Sigma)$ принадлежала бы теории $Th(\Sigma \setminus \{A\})$, т.е. $Th(\Sigma) \subset Th(\Sigma \setminus \{A\})$, что противоречило бы условию. Равносильность двух определений установлена. $\square$

Таким образом, требование независимости непротиворечивой системы аксиом состоит в том, чтобы в эту систему не включалось такое утверждение, которое может быть доказано на основе остальных аксиом системы и, следовательно, являясь излишним в этой системе, должно быть отнесено к разряду теорем. Другими словами, система аксиом должна содержать минимальное число утверждений, необходимых для логического вывода всех остальных утверждений данной теории. Это важное требование, которому должна удовлетворять система аксиом, но вовсе не обязательное, в отличие, например, от рассмотренного ранее требования непротиворечивости. Свойство независимости системы аксиом характеризует некое изящество и лаконичность этой системы. Но не всегда для той или иной аксиоматической теории целесообразно выбирать независимую систему аксиом: изящество системы аксиом может привести к громоздкости доказательств теорем данной теории. Поэтому отступление от выполнения требования независимости вполне допустимо из методических или иных практических соображений. Именно так и делается в большинстве школьных курсов геометрии, где приходится учитывать психологические и возрастные особенности учащихся. Без доказательства допускается большое количество утверждений. Их истинность считается само собой разумеющейся, а некоторые из них даже не формулируются явно. Такой подход сильно упрощает изложение геометрии и облегчает ее усвоение учащимися, ибо доказательство самых простых и очевидных утверждений геометрии требует очень тонких и кропотливых рассуждений, цель которых будет непонятна, а усвоение недоступно для детей школьного возраста.

Интересно отметить, что проблема независимости систем аксиом является, по существу, самой первой проблемой в основаниях математики. Уже ближайшим последователям Евклида было известно, что если воспользоваться понятием движения, то его IV постулат, утверждающий, что все прямые углы равны между собой, может быть доказан как логическое следствие остальных аксиом и постулатов. Также было известно, что аксиомы «Если удвоим равные, то получим равные» и «Половины равных равны между собой» являются логическими следствиями остальных. С размышления над проблемой независимости менее тривиального V постулата Евклида, собственно, и началась наука об обосновании геометрии. Проблема непротиворечивости тогда не возникала, да и не могла воз-

никнуть вплоть до XIX в., пока Лобачевский не указал метод доказательства независимости аксиом — метод построения моделей.

В чем же состоит метод доказательства независимости аксиомы A от остальных аксиом непротиворечивой системы аксиом Σ ? Рассмотрим систему аксиом $(\Sigma \setminus \{A\}) \cup \{\neg A\}$, получающуюся из Σ заменой аксиомы A ее отрицанием $\neg A$. Если окажется, что полученная система аксиом, так же как и Σ , непротиворечива, то отсюда будет следовать независимость аксиомы A от аксиом из $\Sigma \setminus \{A\}$. В самом деле, если бы A можно было доказать исходя из системы $\Sigma \setminus \{A\}$, то A можно было бы доказать и исходя из системы $(\Sigma \setminus \{A\}) \cup \{\neg A\}$. Но это означало бы противоречивость системы аксиом $(\Sigma \setminus \{A\}) \cup \{\neg A\}$, так как из нее выводимы противоречащие одно другому утверждения A и $\neg A$, что не так.

В то же время известно, что непротиворечивость системы аксиом устанавливается путем построения модели этой системы аксиом в некоторой заведомо непротиворечивой теории. Таким образом, приходят к следующему *методу доказательства независимости аксиом*. Для доказательства независимости аксиомы A от остальных аксиом системы Σ нужно сконструировать (построить) модель, в которой выполнялись бы все аксиомы данной системы Σ , кроме аксиомы A , т. е. сконструировать такую интерпретацию, которая была бы моделью системы аксиом $\Sigma \setminus \{A\}$, но не была бы моделью системы аксиом Σ .

Именно на этой идее, принадлежащей Лобачевскому, и основывается доказательство независимости аксиомы о параллельных Евклида (аксиома V.1) от аксиом I — IV групп абсолютной геометрии: строится модель системы аксиом $\{I — IV, \neg(V.1)\}$, полученной из системы аксиом евклидовой геометрии заменой в ней аксиомы о параллельных Евклида ее отрицанием, которая и определяет геометрию Лобачевского. Наличие такой модели служит доказательством независимости аксиомы о параллельных от остальных аксиом евклидовой геометрии. В § 29 это будет рассматриваться подробнее.

Система аксиом Σ называется *независимой*, если каждая ее аксиома не зависит от остальных. Отсюда ясно, насколько кропотливо исследование системы аксиом на независимость. Если для доказательства непротиворечивости данной системы аксиом достаточно построить одну ее модель, то для доказательства ее независимости придется построить столько моделей, сколько аксиом содержит система, причем каждая модель должна реализовывать все аксиомы, кроме одной — исследуемой на независимость.

Полнота. Обобщенно можно сказать, что аксиоматическая теория называется *полной*, если она содержит достаточное для какой-нибудь цели количество теорем. В зависимости от целей выделяют различные виды полноты. Так, в теореме 16.6 была установлена полнота аксиоматической теории высказываний относительно алгебры высказываний: теория охватывала все тавтологии этой алгебры. Доказательство соответствующей теоремы для аксиома-

тической теории предикатов будет дано в § 29. Это понятие полноты — относительно, или внешнее, понятие полноты (полнота относительно внешнего фактора).

Выделяют понятие внутренней полноты. Здесь различают две его модификации: абсолютная полнота и полнота в узком смысле.

Определение 27.5. Аксиоматическая теория называется *абсолютно полной*, если для любого утверждения A , сформулированного в терминах этой теории, точно одно из утверждений A и $\neg A$ является ее теоремой (или, как говорят, средств аксиоматической теории достаточно для того, чтобы доказать или опровергнуть любое утверждение, сформулированное в терминах данной теории).

Определение 27.6. Аксиоматическая теория называется *полной в узком смысле* (или *в смысле Поста*), если добавление к ее аксиомам любого недоказуемого в ней утверждения с сохранением всех правил вывода приводит к противоречивой теории.

Всякая абсолютно полная теория будет полна и в узком смысле.
Доказательство. В самом деле, допустим, что некоторая абсолютно полная теория не полна в узком смысле. Значит, найдется такое утверждение A этой теории, недоказуемое в ней, что новая теория, построенная на основе прежних аксиом и утверждения A в качестве новой аксиомы, непротиворечива. Ясно, что A принадлежит новой теории. Кроме того, ввиду абсолютной полноты исходной теории и недоказуемости в ней утверждения A заключаем, что в ней доказуемо $\neg A$. Но все аксиомы, из которых выведено $\neg A$, вошли в состав системы аксиом новой теории. Поэтому $\neg A$ принадлежит и новой теории. Получаем противоречие с тем, что новая теория непротиворечива. $\square$

Смысл требования (абсолютной) полноты непротиворечивой системы аксиом заключается в том, чтобы она давала возможность без всяких добавочных предпосылок, без какого бы то ни было обращения к наглядным представлениям и опыту исключительно логическим путем доказать всякое предложение, сформулированное в терминах данной теории, либо его опровергнуть.

Классическим примером неполной системы аксиом является система аксиом и постулатов «Начал» Евклида. Уже при доказательстве первых теорем Евклид вынужден молчаливо прибегать к наглядности и очевидности. Так, для обоснования наличия точки пересечения у двух прямых, у двух окружностей, у прямой и окружности требуется аксиома непрерывности, что было осознано математиками лишь в XIX в. Понятие равенства фигур Евклид определяет через движение: «И совмещающиеся равны между собой». Но свойства движения, которые Евклид, несомненно, почерпнул из эмпирических представлений о механическом движении твердых тел и которыми он широко пользуется при доказательстве теорем, никак не выражены в его аксиомах. Нет среди евклидовых аксиом и аксиом порядка или расположения (поэтому тот факт, что прямая делит плоскость на две

части, очевиден для Евклида), как и аксиом, связанных с измерением длин, площадей и объемов. (Последнюю задачу блестяще решил великий геометр, механик и инженер древности Архимед, живший непосредственно после Евклида (287—212 гг. до н. э.), который в своем сочинении «О сфере и цилиндре» развил теорию измерения площадей и объемов, получив, в частности, формулы площади поверхности и объема шара, ввел аксиому, носящую и поныне его имя.)

Другим примером неполной системы аксиом может служить система аксиом абсолютной геометрии (аксиомы I—IV групп системы аксиом Гильберта). В этой системе не может быть ни доказано, ни опровергнуто ни одно предложение, опирающееся на аксиому параллельности Евклида (V.1) или аксиому параллельности Лобачевского — (V.1) (а также, конечно, и сами эти аксиомы).

Вернемся к анализу понятия полноты. Сопоставим его с понятием непротиворечивости. Если непротиворечивость гарантирует, что из данной системы аксиом Σ не могут быть выведены два противоречащих друг другу утверждения A и $\neg A$, то полнота гарантирует доказуемость одного из них. Так что оба требования вместе дают гарантию разрешимости всякого вопроса теории и притом только в одном смысле.

Обсуждая выше проблему независимости системы аксиом, мы доказали, что утверждение A (не входящее в Σ) не зависит от системы аксиом Σ , если существует модель системы аксиом $\Sigma \cup \{\neg A\}$ (в некоторой непротиворечивой аксиоматической теории). В то же время, как известно, утверждение A не противоречит системе аксиом Σ , т. е. система аксиом $\Sigma \cup \{A\}$ непротиворечива, если существует модель этой системы аксиом в непротиворечивой аксиоматической теории. Нетрудно понять, что как модель системы аксиом $\Sigma \cup \{\neg A\}$, так и модель системы аксиом $\Sigma \cup \{A\}$ являются моделями системы аксиом Σ . Причем эти модели конечно же неизоморфны, так как в одной из них выполняется утверждение A , а в другой выполняется его отрицание $\neg A$ (т. е. A не выполняется). Итак, соединим вместе эти два направления настоящего абзаца. (Мы имели два утверждения $P \rightarrow R$ и $Q \rightarrow R$; их конъюнкция равносильна утверждению $(P \wedge Q) \rightarrow R$.) Непротиворечащее системе аксиом Σ утверждение A не будет зависеть от этой системы аксиом, если существуют две такие неизоморфные модели системы аксиом Σ , в одной из которых A выполняется, а в другой — нет.

Снова вернемся к анализу понятия полноты системы аксиом и попытаемся связать его с понятием модели данной системы аксиом. Снова, как и в случае с требованием непротиворечивости, мы пытаемся уйти от выражения этого понятия на языке выводимости к выражению его на языке моделей, т. е. пытаемся уйти от синтаксиса к семантике, от формализма к содержанию. Но здесь эта попытка не окажется столь успешной, как в случае с непротиворечивостью. (Хотя и там ее успех был относителен.) Все это

свидетельствует о том, что к этим проблемам предстоит вернуться и именно на языке синтаксиса, на языке формализма, что и будет выполнено в гл. 6, и результаты окажутся поразительными.

Нетрудно уяснить тот факт, что чем меньшее количество аксиом содержит система аксиом Σ , т. е. чем меньше требований предъявляет система аксиом к первоначальным понятиям, тем большее количество объектов ей удовлетворяет, т. е. тем большее количество моделей имеет эта система аксиом. И наоборот, чем больше аксиом содержит система Σ , т. е. чем больше требований предъявляет она к первоначальным понятиям, тем меньше объектов ей удовлетворяют, т. е. тем меньше моделей имеет эта система аксиом. (Чем больше аксиом содержит система, тем богаче содержанием основанная на ней теория, но и тем уже область ее применения, т. е. тем меньшей общностью отличаются ее теоремы.) Но что же требует от системы аксиом Σ условие ее полноты? Относительно каждого утверждения A можно решить, выводимо A из Σ или нет, т. е. нет утверждений, сформулированных в терминах данной теории, которые не зависели бы от системы аксиом Σ . Но независимость некоторого утверждения от системы аксиом Σ , как было установлено ранее, вытекает из наличия у Σ двух неизоморфных моделей. Поэтому, если у системы Σ нет не зависящих от нее предложений, т. е. если Σ полна, у нее не существует двух неизоморфных моделей. Учитывая, что Σ конечно же непротиворечива, т. е. имеет хотя бы одну модель, в итоге заключаем, что все модели системы Σ изоморфны, т. е. Σ имеет единственную с точностью до изоморфизма модель. Такая система аксиом (и построенная на ее базе аксиоматическая теория) называется категоричной. Таким образом, мы установили, что *всякая полная и непротиворечивая аксиоматическая теория категорична*.

Руководствуясь этим соображением, в ряде учебников по основаниям геометрии понятие полноты аксиоматической теории отождествлено с ее категоричностью. Тем не менее это не так: *не всякая категоричная аксиоматическая теория полна*. Таковой является, например, аксиоматическая теория натуральных чисел, построенная на базе системы аксиом Пеано (см. гл. 6, § 30).

Тем не менее всестороннее решение проблем, связанных с полнотой аксиоматических теорий, удастся получить только в рамках формальных аксиоматических теорий, когда будут уточнены понятия выводимости, доказуемости, правил вывода, когда сама аксиоматическая теория станет точно определяемым математическим понятием (до сих пор она рассматривалась лишь в описательном плане), подвергаемым изучению методами математической логики. Это выполнено в § 30 гл. 6, а здесь ограничимся замечанием, что для многих важных математических теорий задача сочетания обоих рассмотренных качеств — непротиворечивости и полноты — оказывается невыполнимой.

ФОРМАЛЬНЫЕ АКСИОМАТИЧЕСКИЕ ТЕОРИИ

Вспоминая рассмотренные ранее аксиоматические теории (натуральных чисел, геометрии, множеств) и еще раз анализируя их, мы должны отметить, что при всей их строгости они все же не являются вполне абстрактными, или, как говорят, формальными. Все они абстрактны в том смысле, что предметами их изучения могут быть объекты абсолютно произвольной природы (числа, точки, прямые, множества и т.д.). И это несомненно значительный шаг на пути формализации математической теории. Но возможен и следующий шаг на пути абстрагирования от привычного нам неформального (или, как говорят, содержательного) понимания компонентов математической теории. Имея дело с формальными (произвольной природы) объектами, мы применяли к ним не формальную, а содержательную логику, рассуждали не формальным, а неким общечеловеческим образом, считая всем известным и понятным смысл слов: «из утверждения A следует утверждение B » или «утверждение A противоречит (несовместимо, исключает) утверждению B ». Так вот, следующий шаг на пути формализации математических теорий состоит в формализации мыслительных процессов, процессов построения умозаключений при построении математической теории, т.е. в слиянии математической теории и математической логики.

Этот шаг впервые был сделан в работах Д. Гильберта и его школы, когда был разработан так называемый метод формализма в основаниях математики. В рамках этого направления была достигнута следующая стадия уточнения понятия аксиоматической теории, а именно выработано понятие формальной аксиоматической теории или формальной системы. В результате этого уточнения оказалось возможным представлять сами математические теории как точные математические объекты и строить общую теорию, или метатеорию, таких теорий.

Программа формализации была выдвинута Д. Гильбертом с целью доказательства непротиворечивости математики точными математическими методами. Она предусматривала уточнение понятия доказательства, чтобы эти доказательства могли стать объектами точной математической теории — теории доказательств. Чтобы сделать

такое возможным, доказательствам придается единая, точная и вполне определенная форма в рамках формальной аксиоматической теории, или формальной системы. Процесс формализации доказательства состоит в том, что утверждения теории заменяются конечными последовательностями определенных знаков, а логические способы заключения — формальными правилами образования новых формально представленных высказываний из уже доказанных.

В § 28—30 рассмотрены вопросы, связанные с формальными аксиоматическими теориями, или формальными системами. Этот раздел будет центральным для понимания роли математической логики в математических теориях. Фундаментальная теорема Гёделя о существовании модели у всякого синтаксически непротиворечивого множества формул узкого исчисления предикатов, доказываемая во втором параграфе, устанавливает исключительно важную взаимосвязь между свойствами формальной выводимости и содержательной истинности: непротиворечивый формальный вывод не может противоречить содержанию неформальной теории. Следствия из этой теоремы (теоремы полноты, компактности, Лёвенгейма—Сколема) углубляют понимание взаимосвязей между формальным и содержательным. В § 30 с разной степенью подробности рассматриваются подходы к формализации тех математических теорий, которые лежат в основаниях школьного курса математики — теории равенств, теории множеств, числовых систем, математического анализа, геометрии. Неотъемлемой частью данной главы мог бы стать и § 37, содержащий доказательство теоремы Гёделя о неполноте формальной арифметики. Но он помещен в гл. VII после изучения вопросов, связанных с теорией алгоритмов, поскольку методы этой теории существенно используются в ходе доказательства.

Многие математики, а также представители других наук высказывают серьезные сомнения в том, стоит ли формализовать (даже если это в принципе и возможно) математические (и иные) теории, считая, что плоды формализации не оправдывают усилий, ценой которых она достигается. С помощью материала настоящей главы хотелось бы показать такие подходы к математическим теориям, истоки которых находятся в школьном курсе математики, которые осуществляет современная математическая наука с помощью математической логики. В настоящее время только формализованный подход к математическим теориям позволяет так формулировать многие важные проблемы о них, что попытки решения этих проблем можно рассматривать всерьез.

§ 28. О формальных аксиоматических теориях

Аксиоматический метод, рассмотренный в гл. V, является как бы формой организации математической науки, способом исследования тех или иных математических объектов. Неформальные

аксиоматические теории наполнены теоретико-множественным содержанием, понятие выводимости в них довольно расплывчато и в значительной мере опирается на здравый смысл. Дальнейший шаг на пути изучения аксиоматических теорий состоит в отходе этих теорий от содержательности, в строгой формализации понятия правила вывода и в превращении самих теорий в объекты математического исследования.

В рассматриваемом материале § 28 приводится описание самого понятия формальной системы, а также рассматриваются тесно с ним связанные понятия, такие, как теоремы и метатеоремы формальной теории, интерпретации и модели формальной теории, семантическая выводимость.

Об истории идеи формальной аксиоматической теории. Нет сомнения в том, что истоки понятия формальной аксиоматической теории восходят к грандиозной мечте величайшего математика XVII — начала XVIII вв. Готфрида Вильгельма Лейбница «идеи заменить вычислениями». Лейбниц жил во времена, когда обычные для нас обозначения современной математики еще только предлагались в трудах математиков того времени. Свой вклад в этот процесс внес и Лейбниц, изобретя значки для дифференциалов, интеграла и т.п. Лейбниц глубоко осознавал, что беспримерный взлет новой математики существенно основывался на освобождении от размышлений о содержательном значении математических знаков и на возможности производить вычисления с этими содержательными значениями в самом подлинном смысле этого слова. Время Лейбница было эпохой, когда аксиоматическая геометрия древних греков, идущая от Аристотеля и Евклида, переживала новый расцвет. Ее методологическая схема *аксиома — доказательство — теорема — определение — доказательство — теорема — ...* выходила за рамки геометрии и математики и оказывала влияние на новые области философии и естествознания.

Лейбницу принадлежит мысль так сформулировать правила математического доказательства, чтобы при их применении уже не потребовались рассуждения о содержательном смысле математических выражений. Нужно создать *calculus ratiocinator*, т.е. исчисление, в котором естественные, содержательные доказательства были бы заменены формальными вычислениями и тем самым стали бы предметом математики. Такое исчисление, разумеется, предполагает символику, в которой были бы представлены аксиомы, теоремы и определения математики. Такая символика и была целью лейбницевого языка формул, знаменитой *characteristica universalis*. Но, увы, даже для такого гения, как Лейбниц, еще не время было создавать современную математическую логику и современные аксиоматические теории. Формальный язык, в котором все вопросы можно было бы решать вычислением, согласно лейбницевскому лозунгу *calculemus*, остался мечтой.

Важнейший шаг в направлении, указанном Лейбницем, был сделан в XX в. Гильбертом, который, работая над аксиоматическим построением евклидовой геометрии, развил следующую идею формализации математики. Предложения математики, равно как и законы логики, записываются при помощи особой символики в виде формул, без всякого участия словесных выражений. Процессы логического мышления заменяются манипуляциями с такого рода формулами по строго очерченным правилам, причем из уже построенных формул разрешается чисто механически, по точно указанным рецептам, составлять новые формулы, и это заменяет сознательные умозаключения, выводящие из одного предложения другое.

Таким образом, и математическое, и логическое содержание исследуемого отдела математики предстает пред нами в виде цепи формул. Эта цепь начинается с формул, изображающих математические и логические аксиомы, и может быть неограниченно продолжаема путем механического составления новых формул. При этом нет необходимости помнить, какое математическое содержание записано под видом той или иной формулы; нас интересует лишь формула сама по себе как вполне конкретная и обозримая конечная комбинация знаков. Тогда, в частности, проблема непротиворечивости будет состоять в том, чтобы доказать, что в этой цепи формул не может появиться формула, изображающая противоречие.

Появились работы Дедекинда и Кантора, которые сводили всю математику к теории множеств, работы Буля, Пеано, Пирса, Шрёдера, которые вводили начало математической символики для законов мышления, работа Фреге, пытавшегося свести всю математику к логике. Эти работы внушили безграничную веру в мощь формализации. Высокой степени точности формализация математического языка в рамках современных логических исчислений достигла в работах первоклассных математиков XX в. Рассела, Уайтхеда, Гильберта, Барнаиса, Гёделя, Чёрча, А. А. Маркова, А. И. Мальцева и др. Поэтому сегодня уже можно говорить о математическом языке как о части математики, о языке как об одном из предметов, исследуемых математикой, и спорить о реализуемости мечты Лейбница.

Мощное развитие логики и логического языка привело к созданию новой области математики — оснований математики, предметом изучения которой стало строение математических утверждений и математических теорий и которая поставила своей целью ответить на вопросы типа: «Как должна быть построена теория, чтобы в ней не возникло противоречий?», «Какими качествами должны обладать методы доказательства, чтобы считаться достаточно строгими?» и т. д. Одной из фундаментальных идей, на которые опираются исследования по основаниям мате-

матики, является идея формализации математических теорий, т.е. последовательного проведения аксиоматического метода построения теорий.

Понятие формальной аксиоматической теории. Формализация аксиоматической теории состоит в том, что аксиомы рассматриваются как формальные последовательности символов (выражения) некоторого алфавита, а методы доказательств — как методы получения одних выражений из других с помощью операций над символами. При этом не допускается пользоваться какими-либо предположениями об объектах теории, кроме тех, которые сформулированы явно в аксиомах. Такой подход гарантирует четкость исходных утверждений и однозначность выводов. Но может создаться впечатление, что осмысленность и истинность в формализованной теории не играют никакой роли. Внешне это так. Тем не менее в действительности и аксиомы, и правила вывода стремятся выбирать таким образом, чтобы построенной с их помощью формальной теории можно было придать содержательный смысл.

Определение 28.1. *Формальная аксиоматическая теория T считается определенной, если выполнены следующие условия:*

1) задан *алфавит* теории T , представляющий собой некоторое счетное множество символов. Конечные последовательности символов алфавита теории T называются *словами* или *выражениями* теории T ;

2) имеется подмножество выражений теории T , называемых *формулами* теории T (обычно имеется эффективная процедура, позволяющая по данному выражению определить, является ли оно формулой);

3) выделено некоторое множество формул, называемых *аксиомами* теории T (обычно имеется эффективная процедура, позволяющая по данной формуле определить, является ли она аксиомой);

4) имеется конечное множество $R_1, \dots, R_n$ отношений между формулами, называемых *правилами вывода*. При этом для каждого R_i ($1 \leq i \leq n$) существует целое положительное j , такое, что для каждого множества, состоящего из j формул, и для каждой формулы F эффективно решается вопрос о том, находятся ли данные j формул в отношении R_i с формулой F , и если да, то F называется *непосредственным следствием* данных j формул по правилу R_i .

Построенное в § 15 формализованное исчисление высказываний может служить примером формальной аксиоматической теории. Алфавит состоит из символов: $X_1, X_2, \dots, X_n, \dots, \neg, \rightarrow, (,)$. Определено понятие формулы (см. определение 2.1). Из множества всех формул выделено множество всех аксиом (они определяются схемами аксиом (A1) — (A3)). Наконец, единственным отношением R , называемым *правилом вывода*, является тернарное

отношение, в которое входят такие тройки формул F , G , H , что средняя формула G имеет вид $F \rightarrow H$. Таким образом, формула H называется непосредственным следствием формул F и $F \rightarrow H$. Это правило вывода было названо *правилом заключения*, или *модус поненс* (MP).

Определение 28.2. Выводом в формальной аксиоматической теории T называется всякая последовательность $B_1, \dots, B_n$ формул этой теории, такая, что для любого i ($1 \leq i \leq n$) формула B_i есть либо аксиома теории T , либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода. Формула F теории T называется *теоремой* этой теории, если существует вывод в T , последней формулой которого является F ; такой вывод называется *выводом* (или *доказательством*) формулы F .

В примере 15.2 был приведен вывод формулы $F \rightarrow F$ в формализованном исчислении высказываний, т. е. доказательство того, что эта формула есть теорема данной формальной теории.

Далее, аналогично соответствующему понятию в формализованном исчислении высказываний (см. определение 15.1) определяется понятие вывода формулы F из множества формул Γ в формальной аксиоматической теории T и устанавливаются простейшие свойства этого понятия (см. теорему 15.3).

Вторым примером формальной аксиоматической теории может служить формализованное исчисление предикатов, рассмотренное в § 25.

Итак, формальная аксиоматическая теория отличается от неформальной (содержательной), во-первых, тем, что она имеет дело с выражениями, составленными из символов некоторого алфавита, лишенных какого бы то ни было содержательного смысла, а во-вторых, расплывчатое понятие логического умозаключения, на основании которого мы выводили из одних содержательных утверждений другие, теперь заменено четким понятием отношения между выражениями из символов. Таким образом, развитие формальной аксиоматической теории есть процесс оперирования с формальными символами на основе четких формальных правил. Раз так, то такой процесс может быть поручен электронно-вычислительной машине, что сделано в отношении, например, формализованного исчисления высказываний и некоторых других формальных аксиоматических теорий.

Язык и метаязык, теоремы и метатеоремы формальной теории. Описание формальных аксиоматических теорий ведется на некотором общепонятном языке, например на русском. Такой язык по отношению к языку формальной теории называется *метаязыком*. Он используется для формулировок утверждений о формальной теории. Язык же формальной теории (символы алфавита, слова) используется для формулировок высказываний внутри самой формальной теории и называется *предметным языком* (или *язы-*

ком-объектом). Используя метаязык, можем изучать формальную аксиоматическую теорию как бы извне, можем формулировать и доказывать те или иные свойства формальной теории — свойства ее теорем, доказательств, ее самой. Причем при доказательстве этих свойств должны использоваться общепонятные и бесспорные средства обычной логики. В результате получаем набор теорем о формальной теории, устанавливающих те или иные ее свойства. Такие теоремы называются *метатеоремами*. Различие между теоремами и метатеоремами в рассмотренных формальных теориях не всегда проводилось явно, но его непременно нужно иметь в виду. Например, если удалось построить вывод формулы G из формул $F_1, \dots, F_m$, то высказывание « $F_1, \dots, F_m \vdash G$ » является метатеоремой. В частности, теорема о дедукции, производные правила вывода в ФИВ и ФИП, а также теоремы о непротиворечивости, полноте (или неполноте), разрешимости тех или иных формальных теорий являются метатеоремами по отношению к этим теориям. В частности, утверждение «Теория групп непротиворечива» есть утверждение на метаязыке о формальной теории групп, т.е. является метатеоремой. Напротив, утверждение « $(\forall x)(\forall y)(\forall z)(x * y = x * z \rightarrow y = z)$ » есть высказывание самой теории групп, записанное на предметном языке, т.е. теорема.

Интерпретации и модели формальной теории. Обычно теории (и не только формальные) создаются для того, чтобы описать те или иные явления окружающего мира. Поэтому ценность всякой теории в конечном счете определяется тем, насколько хорошо справляется теория с этой задачей, т.е. насколько предоставляемое ею описание адекватно описываемому явлению, участвующим в нем объектам и связям между ними. Теория (и в особенности математическая теория), созданная для описания одних объектов, нередко оказывается применимой и для описания других. Поэтому один из первых для любой теории вопросов — это вопрос о том, для описания каких объектов пригодна данная теория.

Применительно к формальным аксиоматическим теориям проблема адекватности такой формальной аксиоматической теории первого порядка сигнатуры σ и описываемых ею объектов представляет собой чисто математическую задачу о соответствии между множеством теорем этой теории, построенном как формальное исчисление, и содержательно построенной теорией, рассматриваемой как множество объектов с операциями и отношениями на нем (т.е. как алгебраическая система), или моделью формальной аксиоматической теории.

Придадим точный математический смысл интуитивно осознаваемым понятиям интерпретации и модели формальной теории. Пусть задана сигнатура $\sigma = \{c_0, c_1, \dots, f_0^{n_0}, f_1^{n_1}, \dots, P_0^{m_0}, P_1^{m_1}, \dots\}$, т.е. $c_0, c_1, \dots$ — символы предметных или индивидуальных констант (симво-

лы выделенных элементов), $f_0^{n_0}, f_1^{n_1}, \dots$ — функциональные буквы, $P_0^{m_0}, P_1^{m_1}, \dots$ — предикатные буквы. При этом верхние индексы предикатных и функциональных букв указывают число аргументов предиката или функции соответственно, которые могут быть подставлены вместо этих букв. Дадим интерпретацию каждому символу этой сигнатуры. Для этого выберем некоторое множество M и однозначно сопоставим каждой m -местной предикатной букве P_i m -арное отношение P_i^M на M (т.е. интерпретируем букву P_i как конкретное отношение P_i^M на конкретном множестве), каждой n -местной функциональной букве f_j сопоставим n -арную операцию (n -местную функцию) f_j^M на M , каждой предметной константе c_k — элемент c_k^M из M . Постоянные термы (не содержащие предметных переменных) при таком определении также отображаются на элементы из M . Таким образом, мы приходим к алгебраической системе $\mathbf{M} = \langle M; c_0^M, c_1^M, \dots; f_0^M, f_1^M, \dots; P_0^M, P_1^M, \dots \rangle$, которая и представляет собой *интерпретацию* формальной теории данной сигнатуры σ .

Всякая замкнутая (т.е. не содержащая свободных предметных переменных) формула формальной теории (узкого исчисления предикатов) сигнатуры σ при этой интерпретации превращается в высказывание об элементах из M , отношениях и функциях на M , которое может быть истинным или ложным. Открытая формула превращается в некоторое отношение (предикат) на M . Открытая формула F называется *выполнимой* в данной интерпретации $\mathbf{M}$, если существует такая подстановка α предметных констант, при которой она превращается в истинное высказывание. Запись: $\mathbf{M} \models_{\alpha} F$. Открытая формула F называется *истинной в данной интерпретации $\mathbf{M}$* ; или говорят, что F *выполняется* в $\mathbf{M}$, если она превращается в истинное высказывание при любой подстановке констант. Этот факт записывают так: $\mathbf{M} \models F$ и говорят, что интерпретация (алгебраическая система) $\mathbf{M}$ является *моделью* формулы F . Формула, истинная во всех интерпретациях, называется *общезначимой*, или *тавтологией*. Запись: $\models F$. Интерпретация (алгебраическая система) $\mathbf{M}$ называется *моделью (для) множества формул Φ* , если любая формула из Φ истинна в данной интерпретации. Запись: $\mathbf{M} \models \Phi$. Интерпретация M называется *моделью теории T* , если она является моделью множества всех теорем теории T , т.е. если всякая формула, доказуемая (выводимая) в T , истинна в данной интерпретации. Для множества Φ формул обозначим через $\mathbf{M}(\Phi)$ совокупность (класс) всех моделей этого множества формул.

Существо формального подхода состоит в том, что в символы теории (даже самые привычные) не вкладывается никакого смысла, пока не введена интерпретация этих символов. В то же время никакая интерпретация не относится к числу средств самого исчисления: она позволяет осмыслить формулы исчисления, но не участвует в формальном выводе теорем. О формальных свойствах

самого исчисления, его формул и их формальных преобразований принято говорить как о *синтаксисе исчисления*; свойства исчисления, выражаемые в терминах его интерпретаций, — это *семантика исчисления*. В частности, если формула F выводима в формальной теории из множества формул Φ : $\Phi \vdash F$, то говорят, что F *синтаксически выводима* из Φ . Имеется также понятие и семантической выводимости F из Φ , связанное с интерпретациями.

Семантическая выводимость. Вообще под *семантикой* в математической логике понимается исследование интерпретаций формальных аксиоматических теорий, изучение смысла и значения конструкций формализованного языка теории, способов понимания его логических связей и формул. Семантика рассматривает возможности точного описания и формального определения таких содержательных понятий, как «истина», «определимость», «обозначение». В несколько более узком смысле под семантикой формализованного языка понимают систему соглашений, определяющих понимание формул языка, задающих условия истинности этих формул. Построение четкой семантики достаточно сложных формализованных языков (например, типа языков аксиоматической теории множеств) является трудной проблемой. Это связано с тем, что процесс абстрагирования в математике является весьма сложным и многоступенчатым. Построение формальных языков и теорий — абстрагирование весьма высокого уровня. В его ходе используются глубокие и неочевидные абстракции, в результате чего объем объектов исследования, способы обращения с этими объектами и способы доказательства утверждений относительно таких объектов становятся весьма неопределенными. Часто семантические понятия для некоторого языка могут быть точно сформулированы в рамках более богатого языка, играющего для первого роль метаязыка. Именно такую ситуацию мы имеем для формул языка первого порядка, определяя для них семантические понятия истинности, выводимости и т. п.: мы привлекаем для этого алгебраические системы, описываемые на языке теории множеств. Этот последний и играет в данном случае роль метаязыка для формальной теории первого порядка.

Будем говорить, что формула F *семантически выводима* из множества формул Φ , и писать $\Phi \models F$, если в каждой интерпретации, в которой истинны все формулы из Φ , истинна и формула F , т. е. если каждая модель множества формул Φ будет также и моделью формулы F . Ясно, что понятие семантической выводимости формулы является обобщением понятия общезначимости формулы, и первое превращается во второе при $\Phi = \emptyset$ (пустое множество). В терминах классов моделей множеств формул Φ и $\{F\}$ семантическая выводимость F из Φ означает, что $M(\Phi) \subseteq M(\{F\})$.

Метаматематика (свойства формальных аксиоматических теорий). Исследование формальных теорий общепонятными логичес-

кими средствами и методами называется *метаматематикой*. В круг метаматематических вопросов входят вопросы, связанные прежде всего с непротиворечивостью, полнотой, разрешимостью формальных аксиоматических теорий.

Непротиворечивость — важнейшее свойство формальных аксиоматических теорий. В § 16 и § 27 рассматривалась непротиворечивость содержательных аксиоматических теорий и формализованного исчисления высказываний. Сформулированные там определения (16.8 и 27.1) применимы также и для любой формальной аксиоматической теории. Это свойство можно было бы назвать *внутренней непротиворечивостью* формальной теории. В § 27 отмечалось, что внутренняя непротиворечивость теории следует из наличия у теории (непротиворечивой) модели. Последнее свойство теории (наличие непротиворечивой модели) можно назвать *содержательной непротиворечивостью* теории. Таким образом, если теория содержательно непротиворечива, то она внутренне непротиворечива. Значительно труднее получить ответ на вопрос о справедливости обратного утверждения: *всякая внутренне непротиворечивая формальная теория имеет модель, т. е. содержательно непротиворечива*. Это еще одна теорема Гёделя. Доказательство этой сложной и важной теоремы математической логики будет проведено в следующем параграфе, посвященном свойствам формализованного исчисления предикатов.

Еще одним важным метаматематическим понятием является понятие разрешимости формальной аксиоматической теории.

Определение 28.3. Формальная аксиоматическая теория T называется *разрешимой*, если имеется эффективная процедура (алгоритм), позволяющая для каждой данной формулы этой теории узнавать, существует ли ее вывод в T , т. е. является ли она теоремой теории T . Если такого алгоритма не существует, то теория называется *неразрешимой*.

Другими словами, разрешимая теория — это такая теория, для которой можно изобрести машину, испытывающую формулы на свойство быть теоремой этой теории. Для выполнения той же задачи в неразрешимой теории такой машины построить нельзя, и для каждой конкретной формулы приходится изобретать свои методы определения того, будет ли она теоремой данной теории. Для разрешимости теории вовсе не требуется алгоритм, позволяющий доказывать (находить доказательство) каждую теорему теории. Именно таков характер теоремы 16.11 о разрешимости формализованного исчисления высказываний: на основании ее можно для каждой формулы ответить на вопрос, будет ли она доказуема, но построить доказательство нельзя. Что же касается разрешимости формализованного исчисления предикатов, то в начале § 23 отмечалось, что проблема разрешения общезначимости формулы в логике предикатов неразрешима. Этим, в частности, обус-

довливается и неразрешимость формализованного исчисления предикатов.

Дальнейшее рассмотрение свойств формальных аксиоматических теорий приводит нас к необходимости более подробно изучить свойства формализованного (или узкого) исчисления предикатов, являющегося логическим основанием конкретных формальных математических теорий (или формальных теорий первого порядка, или элементарных теорий). Этому и посвящается следующий § 29. Но прежде чем перейти к нему, обратимся еще раз к формализованному исчислению высказываний и установим еще два его свойства как формальной аксиоматической теории.

Формализованное исчисление высказываний как формальная аксиоматическая теория. Итак, формализованное исчисление высказываний представляет собой пример формальной аксиоматической теории. Более того, в § 16 была установлена полнота данной теории относительно алгебры высказываний, ее непротиворечивость и разрешимость. Рассмотрим вопросы внутренней полноты исчисления высказываний, т. е. выясним, будет ли эта теория абсолютно полной и полной в узком смысле (см. определения 27.5 и 27.6).

Если бы формализованное исчисление высказываний было абсолютно полным, т. е. для любой формулы F этой теории сама F или ее отрицание $\neg F$ были теоремами, то, на основании теоремы 16.1, для каждой формулы F алгебры высказываний либо F , либо $\neg F$ была бы тавтологией. Но многочисленные примеры формул F , таких, что ни F , ни $\neg F$ не есть тавтологии, опровергают подобное заключение. (Приведите примеры таких формул.) Итак, *формализованное исчисление высказываний не является абсолютно полным*. Иначе обстоит дело с его полнотой в узком смысле.

Теорема 28.4. *Формализованное исчисление высказываний полно в узком смысле.*

Доказательство. Пусть F — некоторая формула формализованного исчисления высказываний, не являющаяся его теоремой. Докажем, что если F присоединить в качестве схемы (A4) к трем схемам аксиом (A1) — (A3) формализованного исчисления высказываний (см. § 15), то получаемая на основе системы аксиом (A1) — (A4) формальная аксиоматическая теория будет противоречивой. Действительно, поскольку F — не теорема, то она, на основании теоремы 16.5, не является тавтологией. Поэтому в ее таблице истинности найдется такая строка, в которой стоит значение 0. Фиксируем какую-либо одну такую строку. По схеме F построим новую формулу следующим образом: все простые формулы, входящие в F и принимающие в фиксированной строке значение 1, заменим формулой $P \vee \neg P$, а все простые формулы, входящие в F и принимающие в фиксированной строке значение 0, — формулой $P \wedge \neg P$, где P — пропозициональная переменная. В результате получим некоторую формулу $G(P)$, завися-

шую от одной пропозициональной переменной P . Формула получена на основе схемы аксиом (A4) и потому является аксиомой новой формальной теории. Но в то же время при любых значениях P формула $G(P)$ принимает значение 0, т.е. является тождественно ложной. Следовательно, ее отрицание $\neg G(P)$ — тождественно истинная формула, а потому, на основании той же теоремы 16.5, есть теорема формализованного исчисления высказываний, т.е. $\neg G(P)$ выводима из аксиом (A1) — (A3). Но тогда эта формула выводима и из аксиом (A1) — (A4).

Итак, обе формулы $G(P)$ и ее отрицание $\neg G(P)$ являются теоремами новой формальной аксиоматической теории, построенной на основе системы аксиом (A1) — (A4). Следовательно, данная теория противоречива. Теорема доказана. $\square$

Формализация теории аристотелевых силлогизмов. Это еще один пример формальной аксиоматической теории. Рассматриваемый здесь способ формализации силлогистики был предложен в 1950-е гг. известным польским логиком Я. Лукасевичем [1.17, 1.24].

Пусть строчные латинские буквы $a, b, c, \dots$ обозначают переменные термины силлогистики, две прописные латинские буквы A и I — два силлогических бинарных отношения: Aab : «Всякое a есть b », Iab : «Некоторое a есть b ».

Понятие формулы или правильно построенного силлогического предложения дается посредством следующего индуктивного определения:

1) Aab и Iab — простые (или атомарные) формулы силлогистики;

2) если α и β — формулы силлогистики, то формулами силлогистики будут также $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$, $\neg\alpha$;

3) никаких других формул, кроме получающихся по правилам пунктов 1 и 2, нет.

Перейдем теперь к формулировке аксиом. Во-первых, считаем, что имеется некоторое формализованное исчисление высказываний, построенное, например, на базе системы из трех аксиом (§ 15). Так что эти аксиомы открывают список аксиом формальной силлогистики. В качестве специальных аксиом принимаются такие силлогические предложения:

(FS1): Aaa ;

(FS2): Iaa ;

(FS3): $(Abc \wedge Aab) \rightarrow Aac$ (силлогизм *Barbara*);

(FS4): $(Abc \wedge Iba) \rightarrow Iac$ (силлогизм *Datisi*).

С помощью следующих определений введем еще два силлогических бинарных отношения E и O : Eab означает $\neg Iab$, Oab означает $\neg Aab$. Для удобства построения выводов на основе этих определений формулируются правила о возможности замены всюду в формулах $\neg I$ на E и наоборот, а также $\neg A$ на O и наоборот. Таким

образом, в нашей формальной системе, которую будем обозначать FS, оказываются выраженными все четыре основных отношения силлогистики. Напомним, что в аристотелевой силлогистике отношение *Eab* означает «Никакое *a* не есть *b*», а *Oab* — «Некоторые *a* не есть *b*».

В качестве правил вывода в системе формализованной силлогистики FS принимаются два правила подстановки и правило заключения MP:

а) подстановка в выводимую формулу исчисления высказываний на место пропозициональной переменной (всюду, где она входит в формулу) одной и той же силлогической формулы дает выводимую формулу системы FS;

б) подстановка в выводимую формулу системы FS на место переменного термина (всюду, где он входит в формулу) другого переменного термина дает выводимую формулу системы FS;

в) правило MP: если формулы $\alpha \rightarrow \beta$, α выводимы в FS, то в FS выводима и формула β .

Обратим внимание на то, что в качестве третьей (FS3) и четвертой (FS4) аксиом выбраны правильные аристотелевы силлогизмы *Barbara* и *Datisi*. Остальные семнадцать правильных силлогизмов нам предстоит доказать на основе данной системы аксиом. Приступим теперь к доказательству теорем формальной силлогистики.

(FS5): (Силлогические законы противоречия): а) $\neg(Aab \wedge Oab)$; б) $\neg(Iab \wedge Eab)$.

Доказательство. Закон а) получается из закона отрицания противоречия исчисления высказываний $\neg(X \wedge \neg X)$ в результате подстановки $X|Aab$ (вместо X подставляется силлогическая формула Aab) и замены по определению $\neg Aab$ на Oab . Подстановкой $X|Iab$ в тот же закон и заменой по определению $\neg Iab$ на Eab доказывается закон б). $\square$

(FS6): (Силлогические законы исключенного третьего): а) $Aab \vee \neg Oab$; б) $Iab \vee Eab$.

Доказательство. Для обоих законов их доказательство вытекает из логического закона исключенного третьего $X \vee \neg X$ в результате очевидных подстановок и замен.

(FS7): (Закон обращения), $Iab \rightarrow Iba$.

Доказательство. В закон разделения посылок исчисления высказываний $((X \wedge Y) \rightarrow Z) \rightarrow (X \rightarrow (Y \rightarrow Z))$ делаем подстановку $X|Abc$, $Y|Iba$, $Z|Iac$ и из полученной формулы и аксиомы (FS4) по правилу MP выводим: $Abc \rightarrow (Iba \rightarrow Iac)$. Подстановка $b|a$, $c|a$, $a|b$ приводит к формуле $Aaa \rightarrow (Iab \rightarrow Iba)$, из которой и из аксиомы (FS1) по правилу MP следует требуемая формула: $Iab \rightarrow Iba$. $\square$

(FS8): (Законы подчинения): а) $Aab \rightarrow Iab$; б) $Eab \rightarrow Oab$.

Доказательство. а) В закон перестановки посылок исчисления высказываний $(X \rightarrow (Y \rightarrow Z)) \rightarrow (Y \rightarrow (X \rightarrow Z))$ делаем подстановку $X|Abc$, $Y|Iba$, $Z|Iac$. Посылка полученной формулы

представляет собой следующую формулу: $Abc \rightarrow (Iba \rightarrow Iac)$, выводимую в FS, что установлено в ходе доказательства предыдущей теоремы. Тогда из этих двух формул по правилу МР выводим формулу: $Iba \rightarrow (Abc \rightarrow Iac)$. Подстановка $b|a, c|b$ в последнюю формулу дает формулу $Iaa \rightarrow (Aab \rightarrow Iab)$. Из нее и аксиомы (FS2) по правилу МР выводим требуемый закон.

б) В закон контрапозиции исчисления высказываний $(X \rightarrow Y) \rightarrow (\neg Y \rightarrow \neg X)$ делаем подстановку $X|Aab, Y|Iab$ и из полученной формулы и предыдущего закона подчинения $Aab \rightarrow Iab$ по правилу МР выводим: $\neg Iab \rightarrow \neg Aab$. Применяя правила о замене $\neg I$ на E и $\neg A$ на O , получаем: $Eab \rightarrow Oab$. $\square$

В следующей теореме формулируются и доказываются в формальной силлогистике FS все оставшиеся 17 правильных аристотелевых силлогизмов.

Теорема 28.5 (Аристотелевы силлогизмы). *Следующие формулы являются теоремами формальной системы FS:*

Фигура I

- 1) $(Abc \wedge Iab) \rightarrow Iac$ (Daril);
- 2) $(Ebc \wedge Aab) \rightarrow Eac$ (Celarent);
- 3) $(Ebc \wedge Iab) \rightarrow Oac$ (Ferio);

Фигура II

- 4) $(Ac b \wedge Oab) \rightarrow Oac$ (Baroco);
- 5) $(Ac b \wedge Eab) \rightarrow Eac$ (Camestres);
- 6) $(Ec b \wedge Aab) \rightarrow Eac$ (Cesare);
- 7) $(Ec b \wedge Iab) \rightarrow Oac$ (Festino);

Фигура III

- 8) $(Abc \wedge Aba) \rightarrow Iac$ (Darapti);
- 9) $(Ibc \wedge Aba) \rightarrow Iac$ (Disamis);
- 10) $(Obc \wedge Aba) \rightarrow Oac$ (Bocardo);
- 11) $(Ebc \wedge Aba) \rightarrow Oac$ (Felapton);
- 12) $(Ebc \wedge Iba) \rightarrow Oac$ (Ferison);

Фигура IV

- 13) $(Icb \wedge Aba) \rightarrow Iac$ (Dimaris);
- 14) $(Ac b \wedge Aba) \rightarrow Iac$ (Bramantip);
- 15) $(Ac b \wedge Eba) \rightarrow Eac$ (Camenes);
- 16) $(Ec b \wedge Aba) \rightarrow Oac$ (Fesapo);
- 17) $(Ec b \wedge Iba) \rightarrow Oac$ (Fresison).

Доказательство. Приведем доказательства некоторых из этих силлогизмов.

1) Используя теорему о дедукции, нетрудно убедиться в том, что следующая формула $((X \wedge Y) \rightarrow Z) \rightarrow ((V \rightarrow Y) \rightarrow ((X \wedge V) \rightarrow Z))$ является теоремой формализованного исчисления высказываний. Делаем в нее подстановку: $X|Abc, Y|Iba, Z|Iac$. Получаем формулу $((Abc \wedge Iba) \rightarrow Iac) \rightarrow ((V \rightarrow Iba) \rightarrow ((Abc \wedge V) \rightarrow Iac))$. Вместе с аксиомой (FS4) она по правилу МР дает формулу $(V \rightarrow Iba) \rightarrow ((Abc \wedge V) \rightarrow Iac)$. Делаем сюда подстановку $V|Iab$. Получаем $(Iab \rightarrow Iba) \rightarrow ((Abc \wedge Iab) \rightarrow Iac)$. Из этой формулы и формулы теоремы (FS7) по правилу МР выводим требуемую формулу.

4) Начинаем со следующей теоремы формализованного исчисления высказываний: $((X \wedge Y) \rightarrow Z) \rightarrow ((X \wedge \neg Z) \rightarrow \neg Y)$. Подстановка $X|Abc, Y|Aab, Z|Aac$ в нее дает $((Abc \wedge Aab) \rightarrow Aac) \rightarrow ((Abc \wedge \neg Aac) \rightarrow \neg Aab)$. Из этой формулы и аксиомы (FS3) по правилу МР выводим формулу $(Abc \wedge \neg Aac) \rightarrow \neg Aab$.

Используя правило о замене $\neg A$ на O , получаем: $(Abc \wedge Oac) \rightarrow \rightarrow Oab$. Наконец, подстановка $b|c, c|b$ приводит нас к требуемой формуле.

8) В ходе доказательства формулы 1) была выведена формула $(V \rightarrow Iba) \rightarrow ((Abc \wedge V) \rightarrow Iac)$. Сделаем в нее подстановку $V|Aba$. Получим: $(Aba \rightarrow Iba) \rightarrow ((Abc \wedge Aba) \rightarrow Iac)$. Используя теорему (FS8a) (в которой сделать подстановку $a|b, b|a$), по правилу МР получаем требуемую формулу.

9) Подстановка $a|c, c|a$ в аксиому (FS4) дает $Aba \wedge Ibc \rightarrow Ica$, а подстановка $a|c, b|a$ в теорему (FS7) приводит к формуле $Ica \rightarrow \rightarrow Iac$. Наконец, подстановка $X|Aba \wedge Ibc, Y|Ica, Z|Iac$ в выводимую формулу исчисления высказываний (закон силлогизма) $(X \rightarrow \rightarrow Y) \rightarrow ((Y \rightarrow Z) \rightarrow (X \rightarrow Z))$ дает формулу $((Aba \wedge Ibc) \rightarrow Iac) \rightarrow \rightarrow ((Ica \rightarrow Iac) \rightarrow ((Aba \wedge Ibc) \rightarrow Iac))$. Используя полученные выше формулы для двукратного применения правила МР и исходя из последней формулы, получаем: $(Aba \wedge Ibc) \rightarrow Iac$.

Далее, сделав подстановку $X|Ibc, Y|Aba$ в выводимую формулу $(X \wedge Y) \rightarrow (Y \wedge X)$, получаем формулу $(Ibc \wedge Aba) \rightarrow (Aba \wedge Ibc)$. В использованный выше закон силлогизма сделаем другую подстановку: $X|Ibc \wedge Aba, Y|Aba \wedge Ibc, Z|Iac$. Получим формулу $((Ibc \wedge Aba) \rightarrow (Aba \wedge Ibc)) \rightarrow (((Aba \wedge Ibc) \rightarrow Iac) \rightarrow ((Ibc \wedge Aba) \rightarrow \rightarrow Iac))$. Теперь применим дважды правило вывода МР: сначала к этой формуле и предыдущей, а затем к полученному результату и последней формуле предыдущего абзаца. В результате получим требуемую формулу.

13) Сделав в доказанную формулу 1) подстановку $c|a, a|c$, получаем: $(Aba \wedge Icb) \rightarrow Ica$. Сделав подстановку $X|Aba \wedge Icb, Y|Ica, Z|Iac$ в закон силлогизма $(X \rightarrow Y) \rightarrow ((Y \rightarrow Z) \rightarrow (X \rightarrow Z))$, получим формулу $((Aba \wedge Icb) \rightarrow Ica) \rightarrow ((Ica \rightarrow Iac) \rightarrow ((Aba \wedge Icb) \rightarrow \rightarrow Iac))$. Применяя дважды правило МР (учитывая при этом теорему (FS7)), получаем: $(Aba \wedge Icb) \rightarrow Iac$.

Сделав в закон силлогизма другую подстановку $X|Icb \wedge Aba, Y|Aba \wedge Icb, Z|Iac$, придем к формуле $((Icb \wedge Aba) \rightarrow (Aba \wedge Icb)) \rightarrow \rightarrow (((Aba \wedge Icb) \rightarrow Iac) \rightarrow ((Icb \wedge Aba) \rightarrow Iac))$. Учитывая выводимость посылки этой формулы (см. второй абзац в доказательстве формулы 9)) и только что установленную выводимость посылки остающейся формулы, после двукратного применения правила МР придем к требуемой формуле.

14) Из $Aab \rightarrow Iab$ (теорема (FS8a)) с помощью подстановки $a|c$ получаем: $Acb \rightarrow Icb$. В выводимую формулу исчисления высказываний $((X \wedge Y) \rightarrow Z) \rightarrow ((V \rightarrow X) \rightarrow ((V \wedge Y) \rightarrow Z))$ делаем подстановку $X|Icb, Y|Aba, Z|Iac, V|Acb$. В результате получаем формулу $((Icb \wedge Aba) \rightarrow Iac) \rightarrow ((Acb \rightarrow Icb) \rightarrow ((Acb \wedge Aba) \rightarrow Iac))$. Учитывая формулу 13) и выведенную вначале формулу, после двукратного применения правила МР приходим к требуемой формуле.

Докажите выводимость остальных аристотелевых силлогизмов. $\square$

§ 29. Свойства формализованного исчисления предикатов

Формализованное исчисление предикатов (ФИП) развито достаточно глубоко (см. § 25 и Задачник, § 11), и теперь, как и в случае формализованного исчисления высказываний, надлежит рассмотреть свойства (или метатеорию) этого исчисления. Но теперь в области предикатов логика достигает такой выразительной силы, что становится логическим основанием конкретных математических теорий, и теоремы (по сути, метатеоремы) о логике рассуждений достигают поистине философской глубины.

Оправданность аксиоматизации. Теорема оправданности аксиоматизации утверждает, что если $\Phi \vdash F$, то $\Phi \models F$, т.е. из синтаксической выводимости следует семантическая выводимость. Ее очевидным следствием будет утверждение о том, что всякая теорема ФИП является общезначимой формулой (тавтологией) логики предикатов. Смысл этой теоремы состоит в утверждении фактически того, что мы не были «излишне щедры» в выборе аксиом и правил вывода для нашего формального исчисления и не включили в их число ничего лишнего, ибо доказуемыми в этом исчислении оказываются лишь общезначимые формулы логики предикатов. Доказательство этой теоремы не очень сложное, и мы получим ее в качестве следствия несколько более общей теоремы. Обратное же утверждение «если $\Phi \models F$, то $\Phi \vdash F$ » (т.е. при выборе аксиом и правил вывода мы не проявили и «излишней скромности», и для всякой общезначимой формулы логики предикатов в нашем ФИП вполне достаточно формальных средств, чтобы доказать ее), уже не столь очевидно, и доказательство его, приводимое дальше, потребует от нас значительно больших усилий.

Теорема оправданности имеет глубокий смысл: она оправдывает наши занятия математикой, убеждая в том, что наши логические рассуждения и умопостроения не уведут нас от смысла и от практики.

Теорема 29.1. *Если в алгебраической системе $\mathbf{M}$ выполняются все формулы из множества Φ и из Φ синтаксически выводима формула F , то F также выполняется в $\mathbf{M}$: $\mathbf{M} \models \Phi$ и $\Phi \vdash F \Rightarrow \mathbf{M} \models F$.*

Доказательство разделим на три этапа. На первом отметим, что каждая аксиома ФИП есть тождественно истинная формула. Что касается аксиом A_1 , A_2 , A_3 исчисления высказываний, то их тождественная истинность установлена нами в алгебре высказываний (см. теоремы 3.1 з, 3.3, а, л). Общезначимость аксиом PA_1 и PA_2 установлена в теореме 21.13.

На втором этапе покажем, что все три правила вывода, используемые в ФИП, обладают следующим семантическим свойством. Если алгебраическая система $\mathbf{M}$ служит моделью для всех посылок правила вывода, то $\mathbf{M}$ будет моделью и для формулы,

получаемой из данных формул с помощью данного правила вывода. Докажем это утверждение для трех из правил вывода.

Правило МР. Допустим, что $\mathbf{M} = F \rightarrow G$ и $\mathbf{M} = F$. Докажем, что тогда $\mathbf{M} = G$. Возьмем любую подстановку α констант из $\mathbf{M}$. Тогда, по условию, каждое из высказываний $F(\alpha) \rightarrow G(\alpha)$ и $F(\alpha)$, получаемых соответственно из формул $F \rightarrow G$ и F в результате подстановки предметных констант α , будет истинным. Тогда истинным будет и высказывание $G(\alpha)$, т.е. $\mathbf{M} =_{\alpha} G$. Это и означает, что $\mathbf{M} = G$.

$\forall$ -правило. Допустим, что $\mathbf{M} = G(y) \rightarrow F(x, y)$, где x не входит свободно в формулу G , а y обозначает все свободные предметные переменные в формулах F и G (в F — кроме x). Тогда сделанное допущение означает, что для любых элементов $a, b \in \mathbf{M}$ (где $\mathbf{M}$ — носитель алгебраической системы $\mathbf{M}$) высказывание $G(b) \rightarrow F(a, b)$ истинно в $\mathbf{M}$. Рассмотрим теперь высказывание $G(b) \rightarrow (\forall x)(F(x, b))$ и покажем, что оно истинно в $\mathbf{M}$ при любом $b \in \mathbf{M}$. В самом деле, если $G(b)$ ложно, то рассматриваемое высказывание истинно. Если же $G(b)$ истинно, то, по отмеченному выше, истинным будет и высказывание $F(a, b)$. Поскольку оно будет истинным при любом $a \in \mathbf{M}$, то отсюда вытекает истинность для таких $b \in \mathbf{M}$ высказывания $(\forall x)(F(x, b))$. Это, в свою очередь, влечет истинность высказывания $G(b) \rightarrow (\forall x)(F(x, b))$ для тех $b \in \mathbf{M}$, для которых $G(b)$ истинно. Итак, высказывание $G(b) \rightarrow (\forall x)(F(x, b))$ истинно для любых $b \in \mathbf{M}$. Это и означает, что $\mathbf{M} = G(y) \rightarrow (\forall x)(F(x, y))$.

$\exists$ -правило. Подобно предыдущему правилу, доказывается, что если $\mathbf{M} = F(x) \rightarrow G$, то $\mathbf{M} = (\exists x)(F(x)) \rightarrow G$.

Наконец, на третьем этапе докажем утверждение самой теоремы. Пусть $\mathbf{M} = \Phi$ и $\Phi \vdash F$. Последнее означает, что имеется вывод $B_1, B_2, \dots, B_m$ формулы F из множества формул Φ (в частности, $B_m \equiv F$). Покажем, что каждый элемент этой последовательности является формулой, выполняющейся в $\mathbf{M}$. Доказательство проведем индукцией по номеру k формулы в рассматриваемом выводе. При $k = 1$, если $B_1 \in \Phi$, то, по условию, $\mathbf{M} = B_1$. Если B_1 — аксиома, то она общезначима и, в частности, $\mathbf{M} = B_1$. Предположим теперь, что при всех $k < n$ ($n \geq 2$) все формулы B_k выполняются в $\mathbf{M}$, т.е. $\mathbf{M} = B_k$. Рассмотрим формулу B_n . Если $B_n \in \Phi$ или B_n — аксиома, то, как отмечено выше, $\mathbf{M} = B_n$. Если же B_n получена из предыдущих формул последовательности по одному из трех правил вывода, то (на основании выполнимости всех предыдущих формул в $\mathbf{M}$) в силу утверждений (см. второй этап) заключаем, что и B_n выполняется в $\mathbf{M}$, т.е. $\mathbf{M} = B_n$. Окончательно заключаем, что все формулы последовательности $B_1, B_2, \dots, B_m$ истинны в $\mathbf{M}$, в частности $\mathbf{M} = F$. Теорема полностью доказана. $\square$

Следствие 29.2 (теорема оправданности). *Из синтаксической выводимости следует семантическая выводимость, т.е. если $\Phi \vdash F$, то $\Phi = F$.*

Доказательство. Пусть $\Phi \vdash F$ и пусть $\mathbf{M}$ — любая алгебраическая система, в которой выполняются все формулы из Φ , т. е. $\mathbf{M} \models \Phi$. Тогда по доказанной теореме $\mathbf{M} \models F$. По определению семантического следствия это и означает, что $\Phi \models F$.

Следствие 29.3. *Всякая доказуемая формула является общезначимой (т. е. любая теорема истинна): если $\vdash F$, то $\models F$.*

Доказательство получается из предыдущего следствия при $\Phi = \emptyset$.

Непротиворечивость формализованного исчисления предикатов. Важнейшим компонентом критерия оправданности всякой математической теории является ее непротиворечивость, т. е. невозможность доказательства в ней некоторого утверждения и его отрицания одновременно. Трудности, связанные с доказательством этого свойства математических теорий (а одной из причин этих трудностей, несомненно, было отсутствие в содержательных математических теориях точного понятия доказательства), привели к тому, что в математике более естественным стал другой признак непротиворечивости теории, основанный на возможностях реализации этой теории, ее моделируемости. Но в то же время этот подход и привел к возникновению парадоксов в математике, которые, в свою очередь, привели к возникновению науки об основаниях математики и к концепциям формального подхода к понятиям доказательства и математической (аксиоматической) теории. Одной из задач этого подхода была выработка такого формального понятия доказательства, при котором для конкретной математической теории понятие ее формальной непротиворечивости совпало бы с понятием ее содержательной непротиворечивости. Факт такого совпадения, в силу точности определения доказательства, становится математической теоремой (точнее, метатеоремой). Отметим, что привыкание в математике к эквивалентности этих двух понятий непротиворечивости было непростым. В частности, неприятие современниками неевклидовых геометрий Лобачевского — Бояи объясняется также и тем, что законность этих теорий обосновывалась отсутствием в них противоречий — аргументом, совпадающим по существу с современным понятием формальной непротиворечивости. Геометрические модели для этих теорий, доказывающие их содержательную непротиворечивость, были найдены позднее.

Наша задача состоит в том, чтобы в рамках формализованного (узкого) исчисления предикатов дать точные определения двух понятий непротиворечивости и установить их эквивалентность.

Напомним, что формула логики предикатов называется *общезначимой*, если она истинна в любой интерпретации, и *противоречивой*, если она ложна в любой интерпретации, т. е. если ее отрицание общезначимо. Эти семантические понятия, связывающие непротиворечивость с истинностью, позволяют сформулировать понятие семантически непротиворечивой теории.

Определение 29.4. Формальная теория называется *семантически непротиворечивой*, если ни одна из ее теорем (формул) не является противоречивой, т.е. ложной при любой ее интерпретации. Аналогично, множество Φ формул называется *семантически непротиворечивым*, если ни одна формула, выводимая из Φ , не является противоречивой.

В теореме 16.1 доказано, что всякая теорема формализованного исчисления высказываний общезначима (тождественно истинна), а потому не является противоречивой. Это означает, что формализованное исчисление высказываний семантически непротиворечиво. Аналогичная теорема доказана и для формализованного исчисления предикатов (см. следствие 29.3 из теоремы 29.1 выше). Значит, и ФИП семантически непротиворечиво. Семантическая непротиворечивость ФИВ и ФИП означает, что эти формальные теории пригодны для описания любых классов алгебраических систем, т.е. они войдут в теории этих классов составными частями, что вполне соответствует общенаучному принципу универсальности законов логики (Лейбниц формулировал его как выполнимость логических законов «во всех мыслимых мирах»).

Произвольная формальная теория T есть теория множества $M(T)$ всех своих моделей, а значит, теория T семантически непротиворечива, если и только если $M(T) \neq \emptyset$, т.е. для теории T существует модель. Если отождествить пригодность математической теории, ее целесообразность с ее семантической непротиворечивостью, то можно сказать, что сформулированный критерий пригодности теории известен уже давно. Отыскание модели для теории до возникновения оснований математики было единственным общепризнанным методом доказательства «законности» теории. Математическая логика выработала аналог этого критерия, не опирающийся на наличие модели теории — внешний фактор по отношению к теории, а опирающийся на внутренние свойства самой теории, — понятие синтаксической непротиворечивости теории.

Определение 29.5. Формальная теория T называется *синтаксически (или дедуктивно, или формально) непротиворечивой*, если не существует такой формулы F , что F и $\neg F$ являются теоремами теории T , т.е. в T невыводимыми являются одновременно формула и ее отрицание. Аналогичное определение можно сформулировать и для произвольного множества Φ формул: Φ называется *синтаксически непротиворечивым*, если из Φ невыводимы одновременно формула и ее отрицание.

В теореме 16.9 доказана синтаксическая непротиворечивость формализованного исчисления высказываний. Аналогично доказывается следующая теорема.

Теорема 29.6. Формализованное исчисление предикатов синтаксически непротиворечиво.

Доказательство. Допустим противное, т.е. предположим, что ФИП синтаксически противоречиво. Значит, найдется такая формула F , что F и $\neg F$ будут теоремами ФИП. Тогда по следствию 29.3 из теоремы 29.1 формулы F и $\neg F$ будут общезначимыми, что невозможно на основании определения общезначимости. $\square$

Теперь перейдем к установлению взаимосвязей между понятиями семантической и синтаксической непротиворечивости. Наша задача состоит в том, чтобы доказать их эквивалентность. Начнем с достаточно простой, но важной леммы.

Лемма 29.7. *Если множество формул имеет модель, то это множество семантически непротиворечиво.*

Доказательство. Если множество Φ формул имеет модель M , то ни одна формула, выводимая из Φ , не является противоречивой, т.е. ложной во всякой интерпретации, ибо в противном случае она была бы ложна и в M (что невозможно в силу теоремы 29.1). Это и означает, что Φ семантически непротиворечиво. $\square$

Теорема 29.8. *Если множество формул семантически непротиворечиво, то оно синтаксически непротиворечиво.*

Доказательство. Допустим, что некоторое множество Φ формул узкого исчисления предикатов семантически непротиворечиво, но противоречиво синтаксически. Следовательно, из него выводима некоторая формула F и ее отрицание $\neg F$. Но тогда из Φ выводима и их конъюнкция (по правилу введения конъюнкции) $F \wedge \neg F$. Но эта формула ложна в любой интерпретации, что означает, что множество Φ семантически противоречиво. Получаем противоречие, доказывающее, что Φ синтаксически непротиворечиво. $\square$

Непосредственно из предыдущих леммы и теоремы вытекает такое следствие.

Следствие 29.9. *Если множество формул имеет модель, то оно синтаксически непротиворечиво.*

Теорема Гёделя о существовании модели. Утверждение, обратное следствию, также оказывается справедливым. Но с конструктивной точки зрения оно оказывается более глубоким. Смысл его состоит в том, что всякое множество формул не только имеет модель, но эту модель можно конструктивно построить. Доказательство этого факта как раз и заключается в изложении метода такого построения. Это еще одна из замечательных теорем Гёделя (теорема о существовании модели), относящаяся к важнейшим теоремам математической логики. Она доказана Гёделем в 1930 г.

Теорема 29.10 (теорема Гёделя о существовании модели). *Любое синтаксически непротиворечивое множество Σ замкнутых формул узкого исчисления предикатов сигнатуры σ имеет модель.*

Доказательство. Пусть сигнатура $\sigma = \{a_0, a_1, \dots; f_0, f_1, \dots; P_0, P_1, \dots\}$. Требуется построить модель $M = \langle M; a_0, a_1, \dots; f_0, f_1, \dots; \rangle$

$P_0, P_1, \dots$, такую, что $\mathbf{M} \models \Sigma$ (т.е. в алгебраической системе $\mathbf{M}$ выполняются все формулы из Σ). Эта модель будет строиться из слов некоторого алфавита. Под непротиворечивостью всюду в этом доказательстве будем понимать синтаксическую непротиворечивость.

Прежде всего расширим данную сигнатуру σ до σ' введением новых индивидуальных констант: $\sigma' = \sigma \cup \{c_0, c_1, \dots, c_n, \dots\}$, где все c_i отличны от всех символов из σ . Далее будем работать с формулами расширенной сигнатуры σ' . Поскольку все такие (замкнутые) формулы являются конечными словами некоторого счетного алфавита, то множество всех таких формул имеет счетную мощность и мы можем все их расположить в последовательность (т.е. занумеровать натуральными числами). Итак, пусть $A_0, A_1, \dots, A_n, \dots$ — множество всех предложений (замкнутых формул) сигнатуры σ' .

Построим далее последовательность (цепочку)

$$\Sigma_0 \subseteq \Sigma_1 \subseteq \dots \subseteq \Sigma_n \subseteq \dots \quad (1)$$

множеств замкнутых формул следующим образом:

- а) $\Sigma_0 = \Sigma$;
- б) если $\Sigma_n \cup \{A_n\}$ противоречиво, то $\Sigma_{n+1} = \Sigma_n \cup \{\neg A_n\}$;
- в) если $\Sigma_n \cup \{A_n\}$ непротиворечиво и A_n не начинается с квантора существования, то $\Sigma_{n+1} = \Sigma_n \cup \{A_n\}$;
- г) если $\Sigma_n \cup \{A_n\}$ непротиворечиво и $A_n \equiv (\exists x)(B(x))$, то $\Sigma_{n+1} = \Sigma_n \cup \{A_n, B(c_k)\}$, где $c_k \in \sigma' \setminus \sigma$ — новая константа с наименьшим номером k , не встречающаяся в формуле A_n и во всех формулах множества Σ_n .

1) Докажем сначала, что каждое множество Σ_n построенной последовательности будет непротиворечивым множеством формул исчисления предикатов сигнатуры σ' . Доказательство будем вести индукцией по n .

а) База индукции: $n = 0$. Так как $\Sigma_0 = \Sigma$, то по условию Σ_0 непротиворечиво в исчислении предикатов сигнатуры σ . Докажем, что оно непротиворечиво и в исчислении сигнатуры σ' . Допустим противное, т.е. $\Sigma_0 \vdash F$ и $\Sigma_0 \vdash \neg F$, где F — формула сигнатуры σ' . Следовательно, $\Sigma \vdash F$ и $\Sigma \vdash \neg F$. Это означает, что в Σ имеется такое конечное подмножество формул $G_1, \dots, G_m$, что $G_1, \dots, G_m \vdash F, \neg F$. Пусть $B_1, B_2, \dots, B_s \equiv F$ — вывод формулы F из гипотез $G_1, \dots, G_m$ в исчислении предикатов сигнатуры σ' . Допустим, что $c_{i_1}, c_{i_2}, \dots, c_{i_p}$ — все те новые константы, которые входят в формулы этого вывода.

Поскольку $\forall$ - и $\exists$ -правила вывода к константам не применяются, то, заменив все новые константы $c_{i_1}, c_{i_2}, \dots, c_{i_p}$ предметными переменными, не входящими в формулы $B_1, B_2, \dots, B_s$, получим новую последовательность формул $\bar{B}_1, \bar{B}_2, \dots, \bar{B}_s$ исчисления предикатов уже сигнатуры σ , представляющую собой вывод в этом ис-

числении ее последней формулы $\bar{B}_i \equiv \bar{F}$. Аналогично доказыва-
ется, что в исчислении сигнатуры σ из множества Σ выводима фор-
мула $\neg\bar{F}$. Получается противоречие с условием, согласно кото-
рому Σ — непротиворечиво в исчислении сигнатуры σ .

Таким образом, Σ_0 непротиворечиво в исчислении сигнатуры σ' .

Шаг индукции. Предположим, что Σ_n непротиворечиво в
исчислении предикатов сигнатуры σ' . Покажем, что тогда таким
же свойством обладает и множество Σ_{n+1} . Согласно определению
для него возможны следующие случаи:

б) $\Sigma_n \cup \{A_n\}$ противоречиво. В этом случае $\Sigma_{n+1} = \Sigma_n \cup \{\neg A_n\}$.
Допустим, что последнее множество противоречиво. Тогда Σ_n ,
 $\neg A_n \vdash F$ и $\Sigma_n, \neg A_n \vdash \neg F$ для некоторой формулы F . Тогда для неко-
торого конечного подмножества $\Gamma \subset \Sigma_n$: $\Gamma, \neg A_n \vdash F$ и $\Gamma, \neg A_n \vdash \neg F$.
Отсюда по производному правилу вывода $\neg$ -вв получим $\Gamma \vdash \neg\neg A_n$,
т.е. $\Gamma \vdash A_n$, а значит, $\Sigma_n \vdash A_n$.

В то же время из условия противоречивости множества $\Sigma_n \cup \{A_n\}$
аналогичные рассуждения приведут к заключению: $\Sigma_n \vdash \neg A_n$.

Эти два заключения говорят о противоречивости множества
 Σ_n , что противоречит предположению индукции;

в) $\Sigma_n \cup \{A_n\}$ непротиворечиво и A_n не начинается с квантора
существования. В этом случае по определению $\Sigma_{n+1} = \Sigma_n \cup \{A_n\}$, а
значит, Σ_{n+1} — непротиворечиво;

г) $\Sigma_n \cup \{A_n\}$ непротиворечиво и A_n начинается с квантора суще-
ствования: $A_n \equiv (\exists x)(B(x))$. В этом случае Σ_{n+1} получается добавле-
нием к Σ_n двух формул A_n и $B(c_k)$, где $B(c_k)$ получена из $B(x)$
подстановкой константы c_k (первой из $c_0, c_1, \dots$, не входящей в A_n
и все формулы из Σ_n) вместо предметной переменной x : $\Sigma_{n+1} =$
 $= \Sigma_n \cup \{A_n, B(c_k)\}$. Допустим, что Σ_{n+1} противоречиво, т.е. $\Sigma_{n+1} \vdash F$,
 $\neg F$. Тогда найдется такое конечное подмножество $\Gamma \subset \Sigma_n$, что Γ ,
 $(\exists x)(B(x)), B(c_k) \vdash F$ и $\Gamma, (\exists x)(B(x)), B(c_k) \vdash \neg F$.

Поскольку в выводах этих формул $\forall$ -правило и $\exists$ -правило выво-
да не применяются к константе c_k , то, заменив в них эту константу
новой переменной y , не участвующей в выводах этих формул, полу-
чим выводы, доказывающие, что $\Gamma, (\exists x)(B(x)), B(y_k) \vdash F$, и Γ ,
 $(\exists x)(B(x)), B(y_k) \vdash \neg F$, где F получена из F заменой константы
 c_k на предметную переменную y (y — фиксированная переменная
в этих выводах). Из двух последних выводимостей по производ-
ному правилу вывода (введения отрицания $\neg$ -вв) получаем: Γ ,
 $(\exists x)(B(x)) \vdash \neg B(y)$. Отсюда по правилу введения квантора общ-
ности (ВКО, см. Задачник, № 11.7, а) получаем

$$\Gamma, (\exists x)(B(x)) \vdash (\forall y)(\neg B(y)). \quad (2)$$

Кроме того, по теореме из задачи № 11.6, б Задачника легко
получается выводимость $(\forall y)(\neg B(y)) \vdash \neg(\exists y)(B(y))$. Наконец, в
силу выбора переменной y , которая свободна для x в формуле

$B(x)$, и на основании правила переименования связанных переменных (см. Задачник, № 11.4, б) из последней выводимости заключаем, что

$$(\forall y)(\neg B(y)) \vdash \neg(\exists x)(B(x)). \quad (3)$$

Из выводимостей (2) и (3), в силу транзитивности отношения выводимости (см. теорему 15.3, в), получаем: $\Gamma, (\exists x)(B(x)) \vdash \neg(\exists x)(B(x))$.

Учитывая, что $(\exists x)(B(x)) \equiv A_n$, можно заключить, что множество $\Gamma \cup \{A_n\}$ противоречиво. Поскольку $\Gamma \subset \Sigma_n$, то $\Gamma \cup \{A_n\} \subset \Sigma_n \subset \{A_n\}$, а значит, множество $\Sigma_n \cup \{A_n\}$ также противоречиво, что противоречит исходному условию.

Следовательно, и в этом случае множество Σ_{n+1} непротиворечиво.

2) Рассмотрим теперь множество $\Sigma^* = \bigcup \Sigma_n$ (объединение берется по n от 0 до ∞). Отметим два свойства этого множества формул. Во-первых, множество Σ^* непротиворечиво. В самом деле, если бы из Σ^* выводились формулы F и $\neg F$, то они выводились бы из конечного подмножества множества Σ^* , которое включалось бы в некоторое Σ_n , которое, следовательно, было бы противоречивым. Но это не так в силу предыдущего п. 1 доказательства. Во-вторых, для любой формулы A исчисления предикатов сигнатуры σ' $A \in \Sigma^*$ или $\neg A \in \Sigma^*$ (свойство полноты множества Σ^*). Это вытекает непосредственно из построения Σ^* , так как $A = A_n$ для некоторого натурального n .

Последнее свойство можно сформулировать несколько в ином виде. Сначала отметим, что $A \in \Sigma^* \Leftrightarrow \Sigma^* \vdash A$. В самом деле, импликация слева направо очевидна. Предположив, что $\Sigma^* \vdash A$ и $A \notin \Sigma^*$, в силу отмеченного свойства получим $\neg A \in \Sigma^*$. В итоге получаем, что Σ^* противоречиво, что противоречит первому отмеченному выше свойству.

Следовательно, второе отмечаемое утверждение принимает вид: $\Sigma^* \vdash A$ или $\Sigma^* \vdash \neg A$ для любой формулы A .

3) Построим теперь саму модель $\mathbf{M}$. Напомним, что ее сигнатура $\sigma = \{a_0, a_1, \dots; f_0, f_1, \dots; P_0, P_1, \dots\}$. Рассмотрим всевозможные термы расширенной сигнатуры σ' , не содержащие предметных переменных, а содержащие лишь предметные константы $a_0, a_1, \dots, c_0, c_1, \dots$. Напомним, что термы представляют собой либо сами эти константы, либо выражения вида $f_i(t_1, \dots, t_{n_i})$, где f_i — функциональный символ из σ , а $t_1, \dots, t_{n_i}$ — термы. Множество всех этих термов и есть базисное множество M модели $\mathbf{M}$.

Сигнатурные операции на этом множестве зададим следующим образом: $a_i^M = a_i$, $f_i^M(t_1, \dots, t_{n_i}) = f_i(t_1, \dots, t_{n_i})$, ($i = 0, 1, \dots$).

Наконец, выполнимость на $\mathbf{M}$ соответствующего сигнатурного отношения определим следующим образом:

$$\mathbf{M} = P_j^M(t_1, \dots, t_{m_j}) \Leftrightarrow \Sigma^* \vdash P_j(t_1, \dots, t_{m_j}). \quad (4)$$

4) Проверим, что алгебраическая система $\mathbf{M}$ сигнатуры σ действительно является моделью исходного множества Σ формул исчисления предикатов сигнатуры σ , т.е. $\mathbf{M} \models \Sigma$. Для этого докажем сначала, что для всякой формулы $F(x_1, \dots, x_n)$ сигнатуры σ' и любых термов $t_1, \dots, t_n \in M$ имеет место следующее утверждение:

$$\mathbf{M} \models F(t_1, \dots, t_n) \Leftrightarrow \Sigma^* \vdash F(t_1, \dots, t_n). \quad (5)$$

Доказательство будем вести индукцией по числу k логических знаков, используемых при построении формулы F .

База индукции: $k = 0$. Тогда F — атомарная формула, имеющая вид $P_j(t_1, \dots, t_{m_j})$, а для нее утверждение (5) верно по определению (4).

Шаг индукции. Предположим, что для всех формул, в записи которых число логических символов $\leq k$, утверждение (5) верно. Пусть F — произвольная формула, в записи которой участвует $k+1$ логический символ. Покажем, что тогда утверждение (5) будет справедливо и для нее. На основании определения (формулы) формула F имеет один из следующих видов: $\neg A$, $A \rightarrow B$, $(\forall x)(B(x))$, $(\exists x)(B(x))$. Рассмотрим последовательно каждый из этих случаев.

а) $F \equiv \neg A$. Предположим, что $\mathbf{M} \models \neg A(t_1, \dots, t_n)$. Тогда по определению отрицания это означает, что $A(t_1, \dots, t_n)$ не выполняется на $\mathbf{M}$: $\mathbf{M} \not\models A(t_1, \dots, t_n)$. Отсюда по предположению индукции заключаем, что $\Sigma^* \not\vdash A(t_1, \dots, t_n)$. Следовательно, по свойству полноты множества Σ^* , отмеченному в п. 2 настоящего доказательства, $\Sigma^* \vdash \neg A(t_1, \dots, t_n)$. Легко видеть, что каждое утверждение настоящего рассуждения допускает обращение, так что

$$\mathbf{M} \models \neg A(t_1, \dots, t_n) \Leftrightarrow \Sigma^* \vdash \neg A(t_1, \dots, t_n).$$

б) $F \equiv A \rightarrow B$. Предположим, что $\mathbf{M} \models A(t_1, \dots, t_n) \rightarrow B(t_1, \dots, t_n)$. Используя определения импликации, конъюнкции и отрицания, определение (4), полноту Σ^* и предположение индукции для формул A и B , проводим следующее рассуждение:

$\mathbf{M} \models A \rightarrow B \Leftrightarrow \mathbf{M} \models \neg(A \wedge \neg B) \Leftrightarrow \mathbf{M} \not\models A \wedge \neg B \Leftrightarrow \mathbf{M} \not\models A$, или $\mathbf{M} \not\models \neg B \Leftrightarrow \mathbf{M} \not\models A$, или $\mathbf{M} \models B \Leftrightarrow \Sigma^* \not\vdash A$, или $\Sigma^* \vdash B \Leftrightarrow \Sigma^* \vdash \neg A$, или $\Sigma^* \vdash B$.

Теперь мы находимся в области формализованного исчисления высказываний. Дальнейшие рассуждения таковы. Из каждого из утверждений $\Sigma^* \vdash \neg A$ и $\Sigma^* \vdash B$ по правилу $\vee$ -вв следует $\Sigma^* \vdash \neg A \vee B$, т.е. $\Sigma^* \vdash A \rightarrow B$. Теперь нужно проделать обратное рассуждение. Предположим, что $\Sigma^* \vdash A \rightarrow B$ и $\Sigma^* \vdash \neg A$. Следовательно, по второму свойству множества Σ^* из п. 2 настоящего доказательства $\Sigma^* \vdash A$. Тогда из выводимостей $\Sigma^* \vdash A \rightarrow B$ и $\Sigma^* \vdash A$ и правила МР ($A \rightarrow B$, $A \vdash B$) следует, что $\Sigma^* \vdash B$.

Итак, мы доказали, что $\mathbf{M} \models A \rightarrow B \Leftrightarrow \Sigma^* \vdash A \rightarrow B$.

в) $F \equiv (\forall x)(B(x, t_1, \dots, t_n))$. Предположим, что $\mathbf{M} \models (\forall x)(B(x, t_1, \dots, t_n))$. По определению квантора общности это означает, что $\mathbf{M} \models B(t, t_1, \dots, t_n)$ для каждого элемента $t \in M$. Таким образом, по

предположению индукции (5) получим, что $\Sigma^* \vdash B(t, t_1, \dots, t_n)$. Отсюда, в силу правила введения квантора общности, заключаем, что $\Sigma^* \vdash (\forall x)(B(x, t_1, \dots, t_n))$.

Обратно, пусть $\Sigma^* \vdash (\forall x)(B(x, t_1, \dots, t_n))$. Вместе с аксиомой PA1: $(\forall x)(B(x, t_1, \dots, t_n)) \rightarrow B(t, t_1, \dots, t_n)$, в силу правила МР, это дает: $\Sigma^* \vdash B(t, t_1, \dots, t_n)$. На основании предположения индукции (5) отсюда следует, что $\mathbf{M} \models B(t, t_1, \dots, t_n)$. Поскольку данная выполнимость на модели $\mathbf{M}$ имеет место для любого элемента $t \in M$, поэтому на основании определения квантора общности отсюда следует, что $\mathbf{M} \models (\forall x)(B(x, t_1, \dots, t_n))$.

2) $F \equiv (\exists x)(B(x, t_1, \dots, t_n))$. Предположим, что $\mathbf{M} \models (\exists x)(B(x, t_1, \dots, t_n))$. Тогда по определению квантора существования $\mathbf{M} \models B(a_0, t_1, \dots, t_n)$ для некоторого элемента $a_0 \in M$. В силу предположения индукции (5) отсюда получаем $\Sigma^* \vdash B(a_0, t_1, \dots, t_n)$. Вместе с аксиомой PA2: $B(a_0, t_1, \dots, t_n) \rightarrow (\exists x)(B(x, t_1, \dots, t_n))$, в силу правила МР, это дает: $\Sigma^* \vdash (\exists x)(B(x, t_1, \dots, t_n))$.

Обратно, пусть $\Sigma^* \vdash (\exists x)(B(x, t_1, \dots, t_n))$. Поскольку $(\exists x)(B(x, t_1, \dots, t_n))$ — замкнутая формула сигнатуры σ' , то она содержится в последовательности $A_1, A_2, \dots, A_n, \dots$ всех таких формул. Предположим, что это формула A_m . Тогда множество $\Sigma_m \cup \{A_m\}$ непротиворечиво. (Если бы оно было противоречиво, то Σ_{m+1} равнялось бы $\Sigma_m \cup \{\neg A_m\}$, т.е. формула $\neg A_m$ входила бы в множество Σ^* и последнее было бы противоречивым, что не так в силу п. 2 настоящего доказательства.) Поскольку, кроме того, A_m начинается с квантора существования, то в этом случае $\Sigma_{m+1} = \Sigma_m \cup \{A_m, B(c_k, t_1, \dots, t_n)\}$ и, значит, $B(c_k, t_1, \dots, t_n) \in \Sigma^*$. Следовательно, для формулы $B(c_k, t_1, \dots, t_n)$ по предположению индукции имеем $\mathbf{M} \models B(c_k, t_1, \dots, t_n)$ для некоторой константы $c_k \in M$. Тогда по определению квантора существования $\mathbf{M} \models (\exists x)(B(x, t_1, \dots, t_n))$.

Итак, мы доказали, что всякая формула, выводимая из Σ^* (и, в частности, принадлежащая Σ^*), истинна (выполнима) на модели $\mathbf{M}$. В частности, на $\mathbf{M}$ выполняются и все формулы исходной совокупности $\Sigma = \Sigma_0 \subset \Sigma^*$, т.е. $\mathbf{M}$ — действительно модель непротиворечивого множества формул Σ . Теорема полностью доказана. $\square$

Теорема Гёделя о существовании модели позволяет доказать теорему, обратную к теореме 29.8, и они вместе образуют следующую важную метатеорему.

Теорема 29.11 (о непротиворечивости). *Множество формул узкого исчисления предикатов семантически непротиворечиво тогда и только тогда, когда оно синтаксически непротиворечиво.*

Доказательство. Необходимость есть теорема 29.8. Обратно, если множество формул синтаксически непротиворечиво, то по теореме 29.10 оно имеет модель, а тогда по лемме 29.7 оно семантически непротиворечиво. $\square$

Наконец, объединим в одну метатеорему следствие из теоремы 29.8 и теорему 29.10. Получим следующее.

Теорема 29.12 (о непротиворечивости). *Множество формул узкого исчисления предикатов синтаксически (дедуктивно) непротиворечиво тогда и только тогда, когда оно имеет модель.* $\square$

Приведем интересный комментарий, который дает теореме о непротиворечивости известный логик Р. Линдон [7.16, с. 79—80], по мнению которого доказательства (дедуктивной) непротиворечивости какой-либо теории посредством указания ее модели широко распространены в абстрактной математике. Менее очевидное из утверждений теоремы о непротиворечивости — о существовании модели у каждой дедуктивно непротиворечивой теории — используется далеко не так часто. Возможно, это объясняется тем, что математики не слишком-то большое значение придают понятию существования; теорему о непротиворечивости можно как раз и рассматривать как скромное, но зато точное выражение довольно-таки расплывчатого мнения, что существование в математике — это не что иное, как непротиворечивость.

Возможности применения теоремы о непротиворечивости к проблемам установления непротиворечивости конкретных теорий весьма ограничены: дело в том, что построение модели обычно требует принятия в метаязыке допущений, значительно более сильных, нежели те, которые выражаются предметной теорией. Другой путь установления непротиворечивости какой-нибудь аксиоматической теории состоит в том, чтобы с помощью чисто синтаксических рассуждений показать, что в данной теории нельзя доказать тождественно ложную формулу. Область применения этого метода, однако, также невелика. Теорема Гёделя не позволяет надеяться на получение доказательства непротиворечивости теории, если не допускать в теории, предназначенной для такого доказательства на метаязыке, по меньшей мере столь же сильных средств, что и в рассматриваемой предметной теории. Убеждение в непротиворечивости достаточно сложных математических теорий базируется в конечном счете на интуиции и опыте.

Полнота и адекватность формализованного исчисления предикатов. Доказав теорему Гёделя о существовании модели (теорема 29.10), можно доказать теорему, обратную теореме оправданности (следствие 29.2 из теоремы 29.1), т.е. утверждение о том, что из семантической выводимости следует синтаксическая выводимость. В самом деле, пусть $\Phi \models F$. Покажем, что тогда множество формул $\Phi \cup \{\neg F\}$ противоречиво. Допустим на время, что это не так. Тогда по теореме 29.10 это множество имеет модель $\mathbf{M}$, т.е. на $\mathbf{M}$ выполняется формула $\neg F$ и все формулы из Φ . Из последнего, ввиду условия $\Phi \models F$, следует, что на $\mathbf{M}$ выполняется и формула F . Получаем противоречие. Итак, множество $\Phi \cup \{\neg F\}$ противоречиво. Значит, из него выводима любая формула, в частности $\Phi \cup \{\neg F\} \vdash F$. Тогда по теореме о дедукции имеем $\Phi \vdash \neg F \rightarrow F$. Учитывая, что, кроме того, формула $(\neg F \rightarrow F) \rightarrow F$ является теоремой ФИВ, по правилу МР заключаем, что $\Phi \vdash F$.

Итак, мы доказали, что если $\Phi = F$, то $\Phi \vdash F$. Объединив это утверждение со следствием 29.1 из теоремы 29.2, приходим к следующей важной метатеореме.

Теорема 29.13 (теорема адекватности). *Формула F синтаксически выводима из множества формул Φ тогда и только тогда, когда она семантически выводима из Φ : $\Phi \vdash F \Leftrightarrow \Phi = F$. $\square$*

Если теорема оправданности означала, что при выборе аксиом и правил вывода мы не были слишком щедры (настолько, что сможем доказать лишь общезначимые формулы), то обратная теорема — теорема адекватности — означает, что при этом выборе мы не были и излишне скупы (ровно настолько, что сможем доказать всякую общезначимую формулу).

Заметим, что нетрудно показать, что теорема о существовании модели вытекает из теоремы адекватности. В самом деле, предположим, что Φ — непротиворечивое множество формул, не имеющее модели. Тогда ясно, что для любой формулы F справедливо семантическое следование $\Phi = F$. В силу теоремы адекватности отсюда следует, что $\Phi \vdash F$ для любой F , что означает противоречивость множества Φ , в противоречие с условием.

Теорема 29.14 (теорема Гёделя о полноте ФИП). *Класс доказуемых замкнутых формул совпадает с классом общезначимых (или тождественно истинных) формул: $\vdash F \Leftrightarrow \models F$.*

Доказательство. Эта теорема непосредственно вытекает из предыдущей при $\Phi = \emptyset$. $\square$

Справедлива она и для открытых формул. В самом деле, если $\models F(x_1, \dots, x_n)$, где $x_1, \dots, x_n$ — свободные предметные переменные в формуле F , то в силу определения квантора общности это будет равносильно тому, что $\models (\forall x_1) \dots (\forall x_n)(F(x_1, \dots, x_n))$. По теореме 29.14 это равносильно тому, что $\vdash (\forall x_1) \dots (\forall x_n)(F(x_1, \dots, x_n))$. В силу свойств выводимости последнее утверждение равносильно тому, что $\vdash F(x_1, \dots, x_n)$.

Неполнота формализованного исчисления предикатов в абсолютном и узком смыслах. В учебнике обсуждаются два понятия полноты аксиоматической теории: абсолютная полнота и полнота в узком смысле (см. определение 27.6). Доказанная теорема 29.14 может быть истолкована как некая внешняя полнота формализованного исчисления предикатов, его полнота относительно логики предикатов: в этой теории могут быть формально доказаны все общезначимые формулы логики предикатов. Рассмотрим вопросы внутренней полноты формализованного исчисления предикатов, т.е. выясним, будет ли эта теория абсолютно полной и полной в узком смысле (см. определения 27.5 и 27.6). Поскольку на основании теоремы 29.14 множество теорем формализованного исчисления предикатов совпадает с множеством тавтологий (общезначимых формул) логики предикатов, а в логике предикатов существуют выполнимые, но не общезначимые формулы, формализо-

ванное исчисление предикатов не является абсолютно полной теорией. Здесь ситуация аналогична соответствующей ситуации в формализованном исчислении высказываний. Что же касается полноты формализованного исчисления предикатов в узком смысле, то исчисление предикатов (в отличие от исчисления высказываний, см. теорему 28.4) таким свойством не обладает. Для доказательства приведем пример формулы, не являющейся теоремой формализованного исчисления предикатов, добавление которой к аксиомам исчисления предикатов (с сохранением правил вывода) приводит к непротиворечивой формальной аксиоматической теории.

Пример 29.15. Рассмотрим формулу $(\exists x)(F(x)) \rightarrow (\forall x)(F(x))$. Нетрудно убедиться в том, что она не является общезначимой (приведите пример конкретного одноместного предиката, превращающего эту формулу в ложное высказывание). Поэтому на основании теоремы К. Гёделя о полноте она не доказуема в формализованном исчислении предикатов. С другой стороны, добавив к аксиомам формализованного исчисления предикатов рассматриваемую формулу, получим непротиворечивую формальную теорию T . Ее непротиворечивость можно доказать следующим образом.

Рассмотрим модель этой теории на одноэлементном множестве $M = \{a\}$. Ясно, что данная формула тождественно истинна на M . Далее, учитывая, что на M можно определить для каждого натурального n лишь два n -местных предиката P_1^n и P_2^n , причем $\lambda(P_1^n(a, \dots, a)) = 0$ и $\lambda(P_2^n(a, \dots, a)) = 1$, нетрудно доказать, что все аксиомы новой теории T тождественно истинны на этой модели и правила вывода от тождественно истинных на M формул приводят к тождественно истинным на M формулам. Таким образом, доказывается утверждение: всякая теорема теории T тождественно истинна на одноэлементном множестве M .

Следовательно, если бы для некоторой формулы F обе формулы F и $\neg F$ были теоремами теории T , то они были бы тождественно истинны на одноэлементном множестве M , что невозможно. Поэтому расширенная теория T непротиворечива, что и доказывает неполноту в узком смысле формализованного исчисления предикатов.

Теорема компактности. Мы уже отмечали (см. теорему 15.3, б) и неоднократно использовали тот простой факт, непосредственно вытекающий из определения понятия вывода, что $\Phi \vdash F$ тогда и только тогда, когда $\Phi_0 \vdash F$, где Φ_0 — некоторое конечное подмножество множества Φ формул. Теорема адекватности, установленная на основании выдающейся теоремы Гёделя о существовании модели, позволяет получить из этого тривиального соображения аналогичную теорему семантического содержания, уже отнюдь не столь очевидную.

Теорема 29.16 (теорема К. Гёделя — А. И. Мальцева). Если $\Phi = F$, то для некоторого конечного подмножества $\Phi_0 \subset \Phi$ имеет место $\Phi_0 = F$.

Доказательство. Если $\Phi = F$, то по теореме 29.13 (теорема адекватности) $\Phi \vdash F$. В силу сделанного перед настоящей теоремой замечания найдется такое конечное подмножество $\Phi_0 \subset \Phi$, что $\Phi_0 \vdash F$. Отсюда по теореме оправданности (следствие 29.2 из теоремы 29.1) заключаем, что $\Phi_0 = F$. $\square$

Следствие 29.17 (локальная теорема К. Гёделя — А. И. Мальцева). Множество Σ замкнутых формул узкого исчисления предикатов сигнатуры σ имеет модель тогда и только тогда, когда каждое его конечное подмножество имеет модель.

Доказательство. Необходимость очевидна. Обратно, пусть каждое конечное подмножество множества Σ имеет модель. Тогда Σ — синтаксически непротиворечиво. (Если бы это было не так, то для некоторой формулы F имелись бы выводимости $\Sigma \vdash F$ и $\Sigma \vdash \neg F$, а значит, нашлось бы такое конечное подмножество $\Sigma_0 \subset \Sigma$, что $\Sigma_0 \vdash F$ и $\Sigma_0 \vdash \neg F$, т.е. Σ_0 было бы синтаксически противоречиво, а значит, по теореме 29.12 не имело бы модели, что противоречило бы условию.) Следовательно, по теореме 29.10 о существовании модели множество Σ имеет модель. Следствие доказано. $\square$

В заключение приведем еще одну теорему о формулах узкого исчисления предикатов и их моделях.

Теорема 29.18 (Лёвенгейм — Сколем). Пусть σ — счетная сигнатура и Σ — множество замкнутых формул узкого исчисления предикатов сигнатуры σ . Если Σ имеет модель, то Σ имеет счетную модель.

Доказательство. Пусть $\sigma = \{a_0, a_1, \dots; f_0, f_1, \dots; P_0, P_1, \dots\}$ и множество Σ формул имеет модель. Тогда (по теореме 29.12) Σ синтаксически непротиворечиво и модель этого множества формул может быть построена, как в доказательстве теоремы 29.10. Построенная таким образом модель будет счетной: она состоит из элементов $a_0, a_1, \dots; c_0, c_1, \dots$ и всех термов (не содержащих переменных), построенных из констант a_i, c_j . Эти термы можно занумеровать, например, по следующему правилу:

$$v(a_i) = 4i + 1, v(c_i) = 4i + 3, v(f_i(t_1, \dots, t_{n_i})) = 2^{n_i+1} 3^{v(t_1)} 5^{v(t_2)} \dots p_{n_i}^{v(t_{n_i})},$$

где $p_0 = 2, p_1 = 3, p_2 = 5, \dots, p_{n_i}, \dots$ — последовательность простых чисел. $\square$

Эта теорема может быть доказана и в более общей мощностной формулировке: если множество Σ формул имеет бесконечную модель и мощность множества всех букв, из которых составлены формулы из Σ , равна n , то для любой бесконечной мощности $m \geq n$ существует модель множества Σ мощности m .

Укажем два следствия этой теоремы: 1) если Σ — множество формул мощности n , имеющее бесконечную модель, то Σ имеет бес-

конечные модели любых мощностей, превышающих n ; 2) всякое конечное множество или счетное непротиворечивое множество формул либо имеет только конечные модели, либо имеет бесконечные модели любых мощностей.

Теорема Лёвенгейма — Сколема дает ряд поразительных следствий двух типов: одни из них гласят, что некоторая теория имеет неожиданно обширные модели, другие — что теория имеет неожиданно узкие модели. Дальнейшее развитие эта мысль получит в следующем параграфе.

§ 30. Формальные теории первого порядка

В § 25 (см. также Задачник, § 11) построено чистое формализованное исчисление предикатов первого порядка, а затем в § 29 рассмотрены его свойства (метатеория). В этом исчислении не участвуют функциональные буквы и предметные константы основного алфавита, хотя язык исчисления (т.е. его формулы) определен с учетом того, что такие символы в нем будут использоваться. Если в аксиомах и других формулах исчисления предикатов участвуют функциональные буквы и предметные константы, то говорят о прикладном исчислении предикатов, или о формальной аксиоматической теории, или об элементарной теории, или о теории первого порядка. Здесь можно отметить, что термин «теория первого порядка» означает, что в теории кванторы применяются лишь по предметным переменным и не применяются по переменным предикатным. Таким образом, каждая из теорий первого порядка является расширением формализованного исчисления предикатов. Система аксиом теории первого порядка получается в результате добавления к аксиомам формализованного исчисления предикатов, называемых в данной ситуации логическими аксиомами, собственных или нелогических аксиом теории. В записи нелогических аксиом используются символы отношений, символы операций и нелогические константы, присущие данной формальной теории. Другой важной особенностью прикладных исчислений является то, что в схемах аксиом (PA1) и (PA2) участвуют уже не предметные переменные, а произвольные термы. Более точно, эти схемы аксиом принимают следующий вид:

$$(PA1'): (\forall x)(F(x)) \rightarrow F(t);$$

$$(PA2'): F(t) \rightarrow (\exists x)(F(x)),$$

где терм t не содержит предметной переменной x , а $F(t)$ — результат подстановки терма t в $F(x)$ вместо всех свободных вхождений x , причем все переменные t должны быть свободными в $F(t)$.

Формальные теории возникают как некие формальные конструкции для соответствующих содержательных теорий. Если для семантической (содержательной) теории удастся построить не-

противоречивую и полную формальную теорию, то исходную содержательную теорию называют *аксиоматизируемой* или *формализуемой* теорией. Ранее мы установили, что логика высказываний и логика предикатов формализуемы с помощью соответствующих исчислений.

В настоящем параграфе будут рассмотрены формальные подходы к тем аксиоматическим теориям, которые лежат в основаниях математики и о которых речь шла в § 26. Сначала кратко коснемся формальных теорий с равенством, а затем достаточно обстоятельно поговорим о формальных теориях множеств, в частности о формальной теории Цермело — Френкеля. Затем будет рассмотрена формальная арифметика и дана характеристика теоремы Гёделя о ее неполноте. Далее будут рассмотрены пути формализации теорий числовых систем, геометрии и математического анализа.

Теории первого порядка с равенством. Во многих теориях, которые могут быть формализованы как теории первого порядка, участвует понятие равенства. Формализация этого понятия осуществляется следующим образом. В число предикатных символов теории вводится символ « $=$ » двухместного предиката равенства. В определение формулы добавляется пункт: «если x, y — предметные переменные, то $(x = y)$ — формула». (Следует отметить, что если в нашей формальной теории кроме предиката равенства имеются еще какие-то и функциональные символы, то данный пункт определения будет звучать так: «если t_1, t_2 — термы, то $(t_1 = t_2)$ — формула».) Наконец, в список аксиом вводятся две нелогические аксиомы, описывающие свойства равенства:

(PA3): $(\forall x)(x = x)$ (конкретная аксиома);

(PA4): $(\forall x, y)(x = y \rightarrow (F(x, x) \rightarrow F(x, y)))$ (схема аксиом),

где формула $F(x, y)$ получается из формулы $F(x, x)$ заменой некоторых (не обязательно всех) вхождений x на y при условии, что у в этих вхождениях также остается свободным. Последняя аксиома выражает свойство равенства, часто называемое правилом замены равного равным: два равных объекта (x и y) обладают одинаковыми (равносильными) свойствами. Всякая формальная теория, в которой (PA3) и (PA4) являются аксиомами или теоремами, называется теорией (или исчислением) с равенством. Дело в том, что из (PA3) и (PA4) выводимы основные свойства равенства: рефлексивность, симметричность, транзитивность. (Так что такое равенство при интерпретации формальной теории мыслится не как совпадение элементов модели, а как их эквивалентность, т. е. принадлежность одному классу отношения эквивалентности.)

Теорема 30.1. В любой формальной теории с равенством:

- 1) $\vdash t = t$ для любого терма t (рефлексивность равенства);
- 2) $\vdash x = y \rightarrow y = x$ (симметричность равенства);
- 3) $\vdash x = y \rightarrow (y = z \rightarrow x = z)$ (транзитивность равенства).

Доказательство. 1) непосредственно следует из аксиом (РА3) и (РА1') (где $F(x)$ имеет вид $x = x$) по правилу заключения МР;

2) запишем аксиому (РА4) для случая, когда $F(x, y)$ есть $y = x$: $(x = y) \rightarrow (x = x \rightarrow y = x)$. Используя эту аксиому и дважды применяя правило МР, нетрудно показать, что $x = y, x = x \vdash y = x$. Поскольку формула $x = x$ является аксиомой теории, поэтому из числа гипотез ее можно исключить, так что $x = y \vdash y = x$. Наконец, из этой выводимости по теореме о дедукции для ФИП заключаем, что $\vdash x = y \rightarrow y = x$;

3) заменим в (РА4) x на y , а y на x , в качестве $F(y, y)$ возьмем $y = z$, в качестве $F(y, x)$ возьмем $x = z$. Получим: $y = x \rightarrow (y = z \rightarrow x = z)$. В силу правила МР отсюда заключаем, что $y = x \vdash y = z \rightarrow x = z$. На основании предыдущего свойства равенства имеем $x = y \vdash y = x$. Из этих двух выводимостей заключаем, что $x = y \vdash y = z \rightarrow x = z$. Отсюда по теореме о дедукции следует, что $\vdash x = y \rightarrow (y = z \rightarrow x = z)$. $\square$

О формальных теориях множеств. В § 26 (пример 26.7) были рассмотрены различные аксиоматики содержательной («наивной», канторовской) теории множеств. Одной из важнейших ролей теории множеств является та, которую она играет в вопросах доказательства в тех или иных математических теориях, т. е. фактически в самых основах математики. Мы говорили, что одним из основных методов доказательства непротиворечивости математической теории является метод моделей (или интерпретаций). В качестве основных понятий и отношений выбираются элементы какого-либо конкретного множества и отношения между ними, а затем проверяется, будут ли выполняться для выбранных понятий и отношений аксиомы данной теории. Строя модель исследуемой теории, мы сводим вопрос о ее непротиворечивости к вопросу о непротиворечивости другой математической теории. Интерпретации для многих математических теорий строятся с использованием теории множеств, поэтому непротиворечивость всей математики в значительной мере упирается в непротиворечивость теории множеств.

Парадоксы «наивной» теории множеств. С момента создания теории множеств Кантором в начале 1870-х гг. и до конца XIX в. математики считали ее незыблемой основой всего математического здания. Но в конце XIX в. в самой теории множеств были обнаружены противоречия, получившие название *антиномий* (парадоксов) теории множеств. Причем в рассуждениях, приводящих к этим противоречиям, не содержалось никаких логических ошибок. Это обстоятельство поколебало веру в безусловную надежность математических доказательств.

Первый такой парадокс обнаружил сам Кантор в 1895 г. и сообщил об этом Гильберту. В 1897 г. его переоткрыл и впервые опубликовал Бурали-Форти. Хотя ни Кантор, ни Бурали-Форти не были

способны в то время предложить разрешение антиномии, ситуация не казалась слишком серьезной: эта первая антиномия возникла в довольно специальной области теории вполне упорядоченных множеств, и, вероятно, казалось, что легкий пересмотр доказательств теорем, входящих в эту область, мог бы спасти положение и все здание теории множеств затронуто не будет. Но в 1902 г. английский философ, логик и математик Бертран Рассел обнаруживает антиномию, относящуюся к самым началам теории множеств и показывающую, что в основаниях этой дисциплины что-то неблагополучно. Антиномия Рассела потрясла основы не только теории множеств, но и логики: требовалось лишь легкое изменение в формулировке, чтобы перевести антиномию Рассела в противоречие, которое можно сформулировать в терминах самых основных понятий логики. Антиномия Рассела сильнейшим образом затронула самые фундаментальные понятия двух самых «точных» наук — логики и математики.

Суть *парадокса (антиномии) Рассела* состоит в следующем. Распределим все множества по двум классам: в первый класс включим все те множества, которые содержат себя в качестве своего элемента, во второй класс — все те множества, которые не содержат себя в качестве своего элемента. (Например, множество всех планет не является планетой и поэтому не есть собственный элемент. Напротив, множество всех множеств является своим собственным элементом.) Рассмотрим множество M , элементами которого являются все множества второго класса. Спрашивается, к какому из двух вышеназванных классов принадлежит множество M ? Допустим, что оно принадлежит к первому классу. Тогда множество M содержит себя как элемент. Но элементами множества M являются множества второго класса, а значит, множество M принадлежит ко второму классу. Мы пришли к противоречию. Допустим теперь, что множество M принадлежит ко второму классу. Так как все множества второго класса являются элементами множества M , то M содержит себя как элемент и поэтому принадлежит первому классу. Мы вновь пришли к противоречию.

Таким образом, множество M не принадлежит ни к первому, ни ко второму классу, что противоречит тому, что все множества распределены по этим двум классам.

Противоречию относительно M можно придать и следующий (логический) вид, если задаться вопросом, какое утверждение для M имеет место: $M \in M$ или $M \notin M$. Ответ будет обескураживающим. В самом деле, если $M \in M$, то M принадлежит второму классу и, значит, $M \notin M$. Если же предположить, что $M \notin M$, то по определению второго класса M принадлежит ему. Но все элементы второго класса являются элементами множества M . Следовательно, $M \in M$. Итак, мы доказали, что $M \in M \Leftrightarrow M \notin M$ — явное противоречие.

Парадоксу Рассела были приданы различные словесные формулировки. Одна из них выглядит так. Житель некой деревни, называемый брадобреем, должен брить тех и только тех жителей деревни, которые не умеют бриться сами. Задавшись вопросом, как брадобрый должен поступить в отношении себя, мы аналогичными рассуждениями приходим к парадоксальному выводу: брадобрый должен брить себя в том и только в том случае, когда он не должен брить себя.

Парадоксы теории множеств показали, что наивная концепция множества, фигурирующая в канторовском «определении» множества и в получающихся из него общеизвестных следствиях, не может служить удовлетворительной основой теории множеств, не говоря уже о математике в целом. Роль антиномий как фактора, контролирующего и ставящего ограничения на дедуктивные системы логики и математики, можно сравнить с ролью эксперимента, проверяющего правильность полудедуктивных систем таких наук, как физика и астрономия, и вносящего в них видоизменения. И хотя в 1899 г. в своей книге «Основания геометрии» Гильберт сказал, что «никто не может изгнать нас из рая, который создал нам Кантор», открытие парадоксов предредило уход математиков из этого канторовского «рая».

Поиск путей выхода из кризиса. С начала XX в. был намечен ряд путей обеспечения более надежного фундамента теории множеств. Большую часть этих попыток можно разбить на три группы, характеризующиеся соответственно как логистическая, аксиоматическая (или формалистическая) и интуиционистская (или конструктивная) позиции.

Чтобы кратко охарактеризовать первую позицию (к числу ее сторонников относятся Рассел и Уайтхед), вернемся к парадоксу Рассела. Попытаемся понять, в чем заключается дефект в рассуждениях, который привел к этому парадоксу. По мнению некоторых математиков, недопустимо определять объект (множество M) с помощью некоторой совокупности (множество M определено с помощью совокупности всех множеств и множеств второго класса), а затем причислять его к этой совокупности (множество M причислялось к первому, а затем ко второму классу), так как при этом оказывается, что он в известной степени участвует в своем собственном определении. Чтобы ликвидировать этот дефект, Расселом и Уайтхедом была построена так называемая теория типов, исключающая рассмотрение множеств, приводящих к антиномии. В силу этой теории множество M , которое рассматривается в антиномии Рассела, следует рассматривать как новое образование, которое не имеет смысла причислять ни к первому, ни ко второму классам. Множества можно образовывать только на основании точной процедуры, надстраивая их классы один над другим в порядке некоторой иерархии (иерархия типов). Иерархия типов, построен-

ная Расселом и Уайтхедом, приводит к чрезмерным ограничениям, в силу которых математика становится чрезвычайно сложной.

Другая попытка устранения антиномий теории множеств была предпринята немецким математиком Э. Цермело (1908), который построил теорию множеств в виде формальной аксиоматической теории.

Прежде чем сформулировать систему аксиом данной аксиоматической теории, отметим два обстоятельства. Во-первых, формальная теория множеств создавалась как аксиоматическая теория для уже существовавшей содержательной (или «наивной») канторовской теории множеств. Задача состояла в том, чтобы аксиоматизировать эту теорию, т. е. зафиксировать первоначальные (неопределяемые) понятия и выбрать совокупность известных утверждений о них, которую объявить системой аксиом. Во-вторых, формальная теория множеств должна стать элементарной теорией первого порядка, базирующейся на формализованном исчислении предикатов, т. е. прикладным исчислением первого порядка. В 1908 г., когда Цермело сформулировал свои аксиомы, аксиоматизация теории предикатов в математической логике еще не была достигнута и точная форма языка формальной теории еще не была известна. (Важнейшие шаги в этом направлении были сделаны Расселом и Уайтхедом в их монографии *Principia Mathematica* (1913), польским математиком К. Куратовским, который в 1921 г. свел понятие упорядоченной пары к понятию неупорядоченной пары и тем самым к отношению принадлежности, математиками школы Гильберта. Итоги этих исследований были изложены в завершенном виде в первом томе книги Гильберта и Бернайса «Основания математики», вышедшей в 1934 г.) Но когда формализация языка теории множеств была закончена, оказалось, что система аксиом Цермело прекрасно выражается на нем и почти полностью удовлетворяет потребностям математики. В 1922 г. немецкий математик А. Френкель добавил к этой системе лишь аксиому подстановки. Полученная система аксиом стала называться *системой аксиом Цермело — Френкеля* и обозначаться ZF.

Система аксиом Цермело — Френкеля и некоторые следствия из нее. Прежде — о первоначальных (неопределяемых) понятиях. Первым нелогическим конкретным неопределяемым предикатным символом является двухместный предикатный символ отношения принадлежности « $\in$ », так что атомарные формулы имеют вид « $x \in y$ » (читается: « x принадлежит y »), « x есть член (элемент) y », « x содержится в y », « y содержит x в качестве члена (элемента)». Вместо « $\neg(x \in y)$ » условимся писать « $x \notin y$ ». Вторым предикатным символом является двухместный предикатный символ отношения равенства « $=$ », так что второй вид атомарных формул такой: « $x = y$ ». Первая аксиома характеризует отношение равенства.

(ZF1): *Аксиома объемности или аксиома экстенциональности* (восходит к Лейбницу, введена Г. Фреге в 1893 г.):

$$(\forall x, y)[(\forall z)(z \in x \leftrightarrow z \in y) \leftrightarrow x = y]$$

утверждает, что множества совпадают в том и только в том случае, если они состоят из одних и тех же элементов. Множества x и y называются *различными*, если существует такой z , что $z \in x$ и $z \notin y$, или же существует z , что $z \notin x$ и $z \in y$. Запись: $x \neq y$.

С помощью следующих определений вводится отношение включения:

$$x \subseteq y \Leftrightarrow (\forall z)(z \in x \rightarrow z \in y)$$

(запись « $x \subseteq y$ » читается: « x включается в y » или « y включает x ») и отношение строгого включения:

$$x \subset y \Leftrightarrow x \subseteq y \wedge x \neq y.$$

Между отношениями $\in$ и $\subseteq$ имеется весьма глубокое различие, которое необходимо понимать. Первое в нашем изложении является первоначальным, а второе вводится по определению. Но самое главное, что каждое множество включает себя само и свои подмножества, но, вообще говоря, не содержит (в качестве элементов) ни себя, ни своих подмножеств.

(ZF2): *Аксиома пустого множества*:

$$(\exists x)(\forall y)(\neg(y \in x)).$$

В этой аксиоме утверждается существование множества, не имеющего ни одного элемента. Такое множество называется *пустым* (или *нулевым*) и обозначается $\emptyset$.

(ZF3): *Аксиома неупорядоченных пар*:

$$(\forall x, y)(\exists z)(\forall t)(t \in z \leftrightarrow (t = x \vee t = y)).$$

Множество z , существование которого для x, y утверждается этой аксиомой, будем обозначать $\{x, y\}$. Кроме того, через $\{x\}$ будем обозначать $\{x, x\}$. Множество $\{x\}$ называется *единичным*, или *одноэлементным*.

С помощью понятия неупорядоченной пары можно ввести понятие упорядоченной пары (это сделал К. Куратовский в 1921 г.). Двухэлементное множество $\{\{x\}, \{x, y\}\}$ называется *упорядоченной парой*, составленной из x, y , и обозначается (x, y) . Докажем следующее важнейшее свойство упорядоченной пары: если $(x, y) = (u, v)$, то $x = u$ и $y = v$. В самом деле, рассмотрим следующие два случая: $x = u$ и $x \neq u$. При $x = u$ каждый элемент множества (u, v) , т. е. $\{u\}$ и $\{u, v\}$ совпадает с $\{x\}$, откуда следует, что $x = u = v$. При $x \neq u$ множество $\{x\}$ является элементом множества $(u, v) = \{\{u\}, \{u, v\}\}$, т. е. одним из множеств $\{u\}, \{u, v\}$. Случай $\{x\} = \{u, v\}$ исключается,

так как это равенство влечет $x = u = v$, откуда $\{u\} = \{u, v\}$ и $\{x, y\} = \{u\} = \{u, v\}$, $x = y = u$, что противоречит допущению $x \neq u$. Следовательно, $\{x\} = \{u\}$, а значит, $x = u$. Кроме того, в этом случае второй элемент $\{x, y\}$ множества (x, y) должен совпадать с $\{u\}$ или с $\{u, v\}$. Совпадение $\{x, y\} = \{u\}$ влечет $x = y = u$, что противоречит допущению $x \neq u$. Поэтому $\{x, y\} = \{u, v\}$, откуда $y = u$ или $y = v$. Поскольку $x \neq u$ и $x = u$, то случай $y = u$ невозможен. Остается $y = v$.

После того как определено понятие упорядоченной пары, представляется возможным определить понятие функции. *Функция* (или *отображение*) — это такое множество f упорядоченных пар (x, y) , что если $(x, y) \in f$ и $(x, z) \in f$, то $y = z$. При этом множество всех таких x , что $(x, y) \in f$ (для некоторого y), называется *областью определения* f . Множество всех таких y , что $(x, y) \in f$ (хотя бы для одного x), называется *областью значений* f .

(ZF4): *Аксиома суммы, или некоторого объединения* (введена Г. Кантором в 1899 г. и Цермело в 1908 г.):

$$(\forall x)(\exists y)(\forall z)[z \in y \leftrightarrow (\exists t)(z \in t \wedge t \in x)]$$

утверждает, что существует множество y , являющееся объединением всех множеств из x . Оно обозначается $\bigcup x$. В частности, если мы имеем два множества u и v , то на основании аксиомы (ZF3) образуем двухэлементное множество $w = \{u, v\}$, а по аксиоме (ZF4) получаем существование такого множества y , что $z \in y \leftrightarrow (z \in u \vee z \in v)$. Такое множество z называется *объединением* множеств u и v и обозначается $z = u \cup v$.

(ZF5): *Аксиома множества подмножеств, или аксиома степени* (сформулирована Цермело в 1908 г.):

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow z \subseteq x)$$

утверждает, что для каждого x существует множество y всех подмножеств этого x . Оно обозначается $P(x)$ и называется *множеством всех подмножеств* x , или *множеством-степенью* x .

(ZF6): *Аксиома подстановки* (сформулирована А. Френкелем в 1922 г. и Т. Скулемом в 1923 г.):

$$(\forall x)(\exists y)(F(x, y)) \rightarrow (\forall u)(\exists v) [(\forall t)(t \in v \leftrightarrow (\exists s)(s \in u \wedge F(s, t)))],$$

где F — формула, не содержащая свободных вхождений u .

Таким образом, эта аксиома есть схема аксиом. Она утверждает, что образ при произвольном взаимно-однозначном отображении произвольного множества есть множество. В самом деле, условие данной аксиомы фактически означает, что формула $F(x, y)$ определяет y однозначно как функцию от x , т.е. $y = f(x)$. Тогда заключение утверждает, что совокупность всех таких элементов t , которые являются образами при отображении f элементов из множества u (т.е. $t = f(s)$, $s \in u$), образует множество v .

Эта аксиома является исключительно сильной. Из нее может быть выведено следующее более слабое утверждение.

(ZF6'): *Аксиома выделения*:

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (z \in x \wedge S(z))),$$

где $S(z)$ — формула, содержащая свободную переменную z и не содержащая свободной переменной y .

Аксиома утверждает, что для каждого x существует некоторое множество y , состоящее из всех тех z из x , которые обладают свойством S . В связи с аксиомой выделения имеет смысл еще раз вернуться к парадоксу Рассела и проанализировать причину появления этого парадокса и ему подобных в «наивной» теории множеств. Это в значительной мере обусловлено тем, что в «наивной» теории множеств мы наивно полагаем будто *каждое* свойство определяет некоторое множество. Парадокс Рассела как раз и демонстрирует нам, что это не так. Рассматривая свойство « $x \notin x$ » и множество R объектов, обладающих им: $R = \{x : x \notin x\}$, приходим к следующему противоречию: по определению R $(\forall x)(x \in R \leftrightarrow x \notin x)$, тогда после подстановки R вместо x сразу получаем $R \in R \leftrightarrow R \notin R$ — противоречие. Таким образом, при построении формальной теории множеств надо стараться избегать таких свойств, которые могут привести к «абсурдным» множествам типа только что рассмотренного множества R Рассела. Это и достигается с помощью аксиомы выделения: она допускает рассматривать не безграничные совокупности объектов, удовлетворяющие тому или иному свойству, а лишь те объекты, удовлетворяющие данному свойству, которые находятся внутри наперед заданного множества. Аксиома выделения является, пожалуй, самой характерной особенностью системы Цермело, отличая ее как от доаксиоматического подхода к теории множеств, так и от других аксиоматических систем.

Аксиома выделения позволяет доказать следующие две теоремы, предоставляющие в наше распоряжение две важные теоретико-множественные конструкции.

Теорема 30.2 (о пересечении множеств). *Для любых двух множеств a и b существует вполне определенное множество членов, содержащихся как в a , так и в b :*

$$(\forall a, b)(\exists c)(\forall x)(x \in c \leftrightarrow (x \in a \wedge x \in b)).$$

(Более общо, для каждого непустого множества u существует вполне определенное множество v членов, содержащихся во всех членах из u :

$$(\forall u)[u \neq \emptyset \rightarrow (\exists v)(\forall x)(x \in v \leftrightarrow (\forall t)(t \in u \rightarrow x \in t))].$$

Множество c называется *пересечением* множеств a и b и обозначается $a \cap b$. Множество v называется *пересечением* множеств из u и обозначается $\cap u$.)

Доказательство. Множество $a \cap b$ может быть определено как подмножество множества a , соответствующее условию $x \in b$ в аксиоме (ZF6'). Что касается $\cap u$, то по аксиоме (ZF4) существует множество $s = \cup u$: каждый элемент из s содержится по крайней мере в одном члене из u . Возьмем в качестве $S(z)$ условие: « z содержится в каждом члене из u ». Тогда по аксиоме (ZF6') существует подмножество v множества s , членами которого будут в точности те, что содержатся во всех членах u , т.е. $v = \cap u$. (Если ни одного z , общего для всех членов u , нет, то имеем $\cap u = \emptyset$). $\square$

Множество t называется *дизъюнктным* (или *расчлененным*), если никакие два члена из t не пересекаются, т.е.

$$(\forall x, y)(x \in t \wedge y \in t \wedge x \neq y \rightarrow x \cap y = \emptyset).$$

Теорема 30.3 (о декартовом произведении множеств). *Для каждого дизъюнктного множества t существует вполне определенное множество, членами которого являются в точности все те множества, которые содержат по единственному члену из каждого члена t .*

(Это множество называется *декартовым* или *прямым произведением* членов t и обозначается $\times t$; пишут также $\times t = t' \times t'' \times \dots$, где $t', t'', \dots$ — суть члены t .)

Если t содержит член $\emptyset$, то $\times t = \emptyset$.

Доказательство. Поскольку члены искомого множества суть некоторые подмножества $\cup t$, мы будем исходить из множества-степени множества $\cup t$, т.е. из $P(\cup t) = U$, существующего согласно аксиомам (ZF4) и (ZF5). В качестве условия $S(z)$ выберем следующее: « $z \in U$ и для каждого $\tau \in t$ пересечение $\tau \cap z$ есть одноэлементное множество». Тогда по аксиоме (ZF6') существует множество $U_S \subset U$, членами которого являются те подмножества множества $\cup t$, которые содержат в точности по одному члену из каждого члена t .

Утверждение теоремы в случае $\emptyset \in t$ очевидно: поскольку $\emptyset$ не содержит членов, никакое множество не имеет с $\emptyset$ общих членов. Теорема доказана. $\square$

Таким образом, из трех операций над множествами, известными из «наивной» теории множеств, — объединения, пересечения и прямого произведения — выполнимость первой в системе ZF постулирована аксиомой (ZF4), а выполнимость двух других доказана при помощи аксиом (ZF4), (ZF5) и (ZF6').

(ZF7): *Аксиома бесконечности* (введена Цермело в 1908 г.):

$$(\exists x)[\emptyset \in x \wedge (\forall y)(y \in x \rightarrow y \cup \{y\} \in x)]$$

постулирует существование бесконечного множества. Ясно, что «первые» члены любого множества, удовлетворяющего этой аксиоме, суть следующие: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$ и т.д.

Если опустить эту аксиому, то в качестве модели для оставшейся системы аксиом можно взять совокупность всех конечных множеств, которые можно построить, отправляясь от пустого

множества $\emptyset$. Ясно, что эта совокупность действительно будет моделью для всех остальных аксиом системы ZF, так как ни одна из них не выводит за пределы класса конечных множеств, т. е., будучи применена к конечному множеству, утверждает существование такого множества, которое также должно быть конечным. Ясно, что никакое конечное множество не удовлетворяет аксиоме (ZF7), а значит, на рассматриваемой модели из конечных множеств эта аксиома не выполняется. Это означает, что аксиома бесконечности (ZF7) не зависит от остальных аксиом системы ZF.

(ZF8): *Аксиома фундирования, или аксиома регулярности* (предложена Дж. фон Нейманом в 1925 г.):

$$(\forall x)[x \neq \emptyset \rightarrow (\exists y)(y \in x \wedge (\forall z)(z \in x \vee z \in y))]$$

утверждает, что всякое непустое множество x содержит такой элемент y , что x и y не имеют общих элементов. Из нее следует, что каждое непустое множество x содержит элемент, минимальный по отношению к $\in$ (но не к $\subseteq$). Следовательно, не может существовать такого множества s , что $s \in s$. В противном случае мы могли бы рассмотреть одноэлементное (и, значит, непустое) множество $\{s\}$, для которого аксиома фундирования не выполнялась бы: $s \in \{s\}$ и множества s и $\{s\}$ имеют общий элемент s . Исключается существование таких множеств s, t, u , для которых $s \in t$ и $t \in s$, или $s \in t, t \in u, u \in s$ и т. д. Наконец, исключается существование бесконечных цепей, убывающих по отношению к $\in$, т. е. таких множеств s , которые имеют бесконечную убывающую последовательность своих членов: $\dots \in s_{k+1} \in s_k \in \dots \in s_2 \in s_1 \in s$. Правда, при нарушении аксиомы фундирования такие убывающие цепи строятся лишь с помощью аксиомы выбора.

(ZF9): *Аксиома выбора* (введена Цермело в 1908 г.): если x — дизъюнктное множество непустых множеств, то существует такое множество y , которое из каждого множества из x содержит точно по одному элементу (или: прямое произведение $\times x$ не пусто).

Иначе говоря, среди подмножеств множества $\bigcup x$ имеется по крайней мере одно, пересечение которого с каждым членом из x есть одноэлементное множество. Каждое такое подмножество u множества $\bigcup x$ называется множеством представителей множества x ; множество представителей, вообще говоря, не единственно.

Эту аксиому формулируют также в терминах понятия функции: для любого дизъюнктного множества S непустых множеств существует хотя бы одна такая функция $f(s)$, областью определения которой служит S , что $f(s) \in s$. Каждая такая функция определяет множество представителей множества S и называется *функцией выбора*.

Аксиома выбора предоставляет наряду с аксиомой выделения еще один способ для получения подмножеств каких-либо множеств. Эта аксиома, пожалуй, одна из самых интересных и наибо-

лее активно обсуждавшихся (несмотря на свое сравнительно позднее происхождение) аксиом математики. В этом отношении она уступает только евклидовой аксиоме о параллельных, имеющей более чем двухтысячелетнюю историю. Основные и важнейшие теоремы и методы теории множеств, алгебры, анализа, геометрии, топологии опираются на аксиому выбора. Поразительно большое количество теорем оказывается в точности эквивалентными аксиоме выбора. Фундаментальнейшая теорема Цермело о том, что всякое непустое множество можно вполне упорядочить, т.е. задать на нем такое линейное отношение порядка, что всякое непустое подмножество будет иметь наименьший элемент, — из числа важнейших эквивалентов аксиомы выбора. Хотя эта аксиома была осознана и явно сформулирована лишь в начале XX в., анализ показал, что применялась она в неявном виде задолго до этого времени. К аксиоме выбора математики пришли точно так же, как и к другим математическим принципам, — путем последующей проверки и логического анализа понятий, методов и доказательств, уже содержащихся фактически в математике. Так, греческие математики догадались включить в число основных геометрических принципов аксиому о параллельных — утверждение, бытовавшее в математике задолго до Евклида. Гениальность этого достижения была полностью оценена лишь более двух тысячелетий спустя.

Итак, мы завершили перечисление аксиом теории множеств системы ZF Цермело — Френкеля. В настоящее время это наиболее употребительная в основаниях математики система аксиом, которой охватывается вся традиционная математика.

О других аксиоматиках формальной теории множеств. Кроме рассмотренной системы аксиом Цермело — Френкеля (ZF) имеются и другие аксиоматические системы теории множеств, позволяющие формализовать обычные математические доказательства, но в то же время избежать известных парадоксов «наивной» теории множеств. Их можно разделить на следующие три группы.

Первую группу составляют системы, аксиомы которых выбраны в связи с каким-либо объяснением парадоксов. Согласно одному из взглядов на парадоксы возникающее противоречие обусловлено так называемым непредикативным определением объекта, т.е. таким определением его, в котором участвует он сам. Для устранения этой причины парадоксов Б. Расселом разработана так называемая теория типов, в которой множество и его элементы разнесены по различным слоям (уровням). Имеются и другие теории типов, в которых производится дальнейшее расчленение предметных областей вплоть до доведения их до бесконечного числа. Так возникают разветвленная теория типов Рассела, простая теория типов, теория типов с трансфинитными индексами.

Вторая группа аксиоматических систем включает модификации систем первой группы и системы ZF, преследующие определенные логические или математические цели. Сюда относятся, прежде всего, система аксиом NBG фон Неймана — Бернаиса — Гёделя и система аксиом Куайна. Построение системы аксиом NBG вызвано желанием исключить из системы ZF схемы аксиом, т.е. иметь не бесконечный список аксиом, а конечный. В системе Куайна реализуется стремление преодолеть расслоение понятий, имеющее место в теории типов.

Сторонники перечисленных направлений стремятся устранить антиномии путем ограничения понятия множества или употребления этого понятия в математике — ограничения до такого объема, который соответствует этой цели. При этом структура математической теории не подвергается коренным изменениям.

Третья группа систем образует так называемое логическое направление в преодолении антиномий. С точки зрения логицизма антиномии — это симптомы, свидетельствующие об определенном неблагополучии не только в самой теории множеств, но и в существе применяемых в математике методов. Исходя из этого логицисты считают, что порочна не столько сама математика, сколько логика и ее использование для математических нужд, и предлагают предпринять глубокую реформу логики, которая задолго уже привела бы и к преодолению антиномий. Это направление характеризуется использованием средств нетрадиционных логик: неклассических (в частности, многозначных, интуиционистских и др.) логик, нестандартных средств логического вывода, дополнительных условий на доказательства, бесконечных правил вывода. Системы, относящиеся к этому направлению, менее развиты.

Знаменитые проблемы теории множеств. Методы аксиоматической теории множеств позволили отчетливо сформулировать и решить ряд трудных проблем, имевших свое происхождение в классических разделах математики.

Важнейшей из таких проблем является *проблема континуума*. Именно ее поставил на первое место Д.Гильберт в своей знаменитой речи на II Международном математическом конгрессе, проходившем в Париже с 6 по 12 августа 1900 г., в которой им были сформулированы 23 актуальные математические проблемы. Еще Г.Кантор в 1878 г. сформулировал гипотезу, получившую название континуум-гипотезы: *всякое бесконечное подмножество континуума R равномощно либо множеству натуральных чисел N , либо R , т.е. не существует множества промежуточной мощности между счетной мощностью и мощностью континуума*. Кантору не удалось ни доказать, ни опровергнуть эту гипотезу. Среди математиков росло убеждение в принципиальной неразрешимости проблемы континуума. Но только после того как вся проблемная среда, связан-

ная с континуум-гипотезой, была формализована, т.е. приобрела характер формальной аксиоматической теории, стало возможным математически точно поставить, а затем и решить вопрос о формальной неразрешимости континуум-гипотезы.

В 1939 г. К. Гёдель показал, что если система Цермело — Френкеля ZF непротиворечива, то она остается непротиворечивой и после добавления к ней континуум-гипотезы. Это означает, что в системе ZF в предположении ее непротиворечивости невозможно доказать (вывести) отрицание континуум-гипотезы, т.е. отрицание континуум-гипотезы не зависит от остальных аксиом теории множеств, т.е. континуум-гипотеза не может быть опровергнута. В 1963 г. американский математик П. Коэн доказал аналогичное утверждение относительно континуум-гипотезы, т.е. континуум-гипотеза не может быть доказана, тем самым полностью закрыв проблему континуума. Таким образом, ни континуум-гипотеза, ни ее отрицание не зависят от остальных аксиом теории множеств. Это означает, что возможна теория множеств с континуум-гипотезой и возможна теория множеств с отрицанием континуум-гипотезы. Ситуация здесь оказалась сходной с той, которая возникла в начале XIX в. с пятым постулатом Евклида, когда была открыта геометрия Лобачевского.

Основным методом установления невыводимости формулы A в ZF является построение такой модели ZF, в которой выполняется отрицание $\neg A$. Разработанный Коэном, а затем усовершенствованный другими авторами метод вынуждения сильно расширил возможности построения моделей теории множеств и в настоящее время лежит в основе почти всех дальнейших результатов о невыводимости.

Совершенно аналогичной оказалась ситуация и с аксиомой выбора (ZF9). Гёдель в 1939 г. доказал, что если система $ZF \setminus (ZF9)$ непротиворечива, то непротиворечива и система ZF, т.е. отрицание аксиомы выбора невыводимо из остальных аксиом системы ZF. Невыводимость самой аксиомы выбора (ZF9) из системы $ZF \setminus (ZF9)$ тоже установил Коэн в 1962 г.

С 1920 г. начинается история еще одной знаменитой математической проблемы XX в. — *проблемы М. Я. Суслина*. Мы расскажем о ней ниже в пункте «О формальных теориях числовых систем».

Установлено, что в системе $ZF \setminus (ZF9)$ не может быть ни доказано, ни опровергнуто (т.е. является неразрешимым) следующее утверждение: всякое подмножество множества действительных чисел измеримо по Лебегу. Выяснено взаимоотношение с системой ZF многих важных проблем так называемой дескриптивной теории множеств, значительный вклад в которую внесли математики Московской математической школы, созданной академиком Н. Н. Лузиным (одним из ярких представителей которой является М. Я. Суслин). Получены многочисленные результаты об отсутствии

эффективно определенных объектов в этой теории. Наконец, формализация теории множеств позволила обнаружить неизвестные ранее связи между проблемами «наивной» теории множеств.

Еще раз подчеркнем, что все эти проблемы удалось четко поставить и успешно разрешить только после формализации содержательной («наивной») канторовской теории множеств.

О формальной арифметике. Язык и аксиомы. Это — логико-математическое исчисление (или прикладное исчисление первого порядка), формализующее элементарную теорию чисел. Наиболее популярная формализация основана на подходе Пеано, предложенном им в 1889 г. и рассмотренном нами в § 26 (пример 26.3). Язык этого исчисления кроме логических связок и равенства содержит нелогическую константу 0, двухместные функциональные символы +, ·, одноместный функциональный символ '. Термы строятся из константы 0 и переменных с помощью функциональных символов; в частности, натуральные числа изображаются термами вида $0''\dots'$. Атомарные формулы — это равенство термов; остальные формулы строятся из атомарных с помощью логических связок. В качестве аксиом выбираются логические аксиомы, это аксиомы формализованного исчисления предикатов (см. § 25) и следующие нелогические (арифметические) формулы:

$$\begin{aligned}x &= y \rightarrow (x = z \rightarrow y = z), \neg(x' = 0); \\x &= y \rightarrow x' = y', \quad x' = y' \rightarrow x = y; \\x + 0 &= x, \quad x + y' = (x + y)'; \\x \cdot 0 &= 0, \quad x \cdot y' = (x \cdot y) + x; \\(F(0) \wedge (\forall x)(F(x) \rightarrow F(x')))) &\rightarrow (\forall x)(F(x)),\end{aligned}$$

где $F(x)$ — произвольная формула теории с одной свободной предметной переменной x . Последняя формула есть схема аксиом, называемая *схемой аксиом индукции*.

Средства формальной арифметики оказываются достаточными для вывода теорем, устанавливаемых в стандартных курсах элементарной теории чисел. Более того, формальная арифметика оказывается эквивалентной аксиоматической теории множеств ZF Цермело — Френкеля без аксиомы бесконечности (ZF7): в каждой из этих систем может быть построена модель другой.

Программа Гильберта формализации математики и теорема Гёделя о неполноте. Формальная арифметика играет исключительно важную роль в основаниях математики. Это связано с тем, что именно арифметика лежит в основаниях классической математики, проблема непротиворечивости которой сводится к проблеме непротиворечивости арифметики. Эта содержательная сторона нашла свое наивысшее выражение и на формальном уровне.

Одним из путей выхода из кризиса в основаниях математики в начале XX в., обусловленного обнаружением парадоксов (ан-

тиномий) в теории множеств, должен был стать гильбертовский путь формализации математики и логики. Каждая конкретная математическая теория должна быть переведена на язык подходящей формальной системы таким образом, чтобы каждое осмысленное (ложное или истинное) предложение содержательной теории выражалось бы некоторой формулой формальной системы. Тогда естественно было надеяться, что этот метод формализации позволит строить все положительное содержание математических теорий на такой точной и, казалось бы, надежной основе, как понятие выводимой формулы (теоремы формальной системы). Кроме того, такие принципиальные вопросы, как проблема противоречивости математических теорий, решались бы в форме доказательства соответствующих утверждений о формализующих эти теории формальных системах. Поскольку описанные нами формальные системы сами оказываются точными, или, как говорили в школе Гильберта, финитными, математическими объектами, можно было ожидать, что удастся получить *финитные доказательства* утверждений о непротиворечивости, т.е. доказательства, которые в определенном смысле были бы эффективными, не зависящими от тех мощных средств, вроде абстракции актуальной бесконечности, которые в классических математических теориях как раз и являются причиной трудностей в их обосновании. Но результаты, полученные Гёделем в начале 1930-х гг., привели к краху основных надежд, связывавшихся с этой программой Гильберта. Гёдель доказал следующие две теоремы, получившие общее название «*теорема о неполноте формальной арифметики*»:

1) всякая естественная непротиворечивая формализация S арифметики или любой другой математической теории, содержащей арифметику (например, теории множеств), неполна и неполнима. Неполнота означает, что в S имеется содержательно истинная, но неразрешимая формула, т.е. такая формула A , что ни A , ни ее отрицание $\neg A$ не выводимы в S . Неполнимостью S означает, что каким бы конечным множеством дополнительных аксиом (например, неразрешимыми в S формулами) ни расширить систему S , в новой формальной системе неизбежно появятся свои неразрешимые формулы;

2) если формализованная арифметика в действительности непротиворечива, то хотя утверждение о ее непротиворечивости выразимо на ее собственном языке, но доказательство этого утверждения средствами, формализуемыми в ней самой, невозможно.

Эта теорема, как и первая, распространяется на всякую непротиворечивую формальную систему, содержащую формальную арифметику.

Доказательство первой теоремы проводится разработанным Гёделем методом арифметизации синтаксиса языка формальной

теории, который стал одним из основных методов теории доказательств (метаматематики). Этим методом строится формально неразрешимая формула. Фиксируется нумерация основных формальных объектов (формул, конечных последовательностей формул и т.д.) натуральными числами, такая, что основные свойства этих объектов (быть аксиомой, быть выводом по правилам системы и т.д.) оказываются распознаваемыми по их номерам с помощью весьма простых алгоритмов. Столь же просто вычисляются по номерам исходных данных номера результатов комбинаторных преобразований (например, подстановки терма в формулу вместо переменной). При этом оказывается возможным написать арифметическую формулу $B(a, b)$, имеющую вид $f(a, b) = 0$ (где f — примитивно рекурсивная функция) и выражающую условие: b есть номер формулы, которая получается из формулы с номером a путем подстановки натурального числа a вместо переменной x . Если p — номер формулы $(\forall b)(\neg B(x, b))$, то формула $(\forall b)(\neg B(p, b))$ выражает свою собственную невыводимость. Она и оказывается формально неразрешимой. Отсюда и следует, что в любой непротиворечивой системе с минимальными выразительными арифметическими возможностями имеется истинное, но невыводимое суждение указанного вида. Достаточно подробно доказательство этой теоремы будет изложено в § 37 после того, как будут изучены основы теории алгоритмов и рекурсивных функций.

Доказательство второй теоремы получается путем формализации доказательства первой и существенно использует особенности арифметизации синтаксиса рассматриваемой системы.

Из первой теоремы Гёделя о неполноте арифметики видно, что (семантическое) понятие истинности в арифметике, а следовательно, и во всей математике нельзя исчерпывающим образом формализовать посредством (синтаксического) понятия доказуемости в какой-либо *одной* формально-логической системе. Вторая теорема Гёделя о неполноте арифметики показывает, что и основная цель первоначальной программы Гильберта по формализации математики оказывается недостижимой. Эта цель состояла в том, чтобы доказать формальную непротиворечивость арифметики, пользуясь при этом так называемыми «финитными» методами, т.е. лишь такими методами доказательств, которые применяются в самой арифметике. Но всякое разумное уточнение понятия финитного доказательства, по-видимому, формализуемо в формальной арифметике и потому, согласно второй теореме Гёделя, невозможно.

Гильберту и представителям его школы для выполнения гильбертовской программы удалось доказать строго финитными методами непротиворечивость весьма широкой подсистемы арифметики; подсистема эта имеет лишь тот недостаток, что принцип индукции формулируется в ней в ослабленной форме, что пре-

пятствует применению его к квантифицированным предложениям. Вторая теорема Гёделя показывает, что такой частичный успех гильбертовской школы объясняется отнюдь не недостатком изобретательности ее представителей, а, как выяснилось впоследствии, объективной картиной явления. Напротив, теперь мы знаем, что они продвинулись в этом направлении настолько далеко, насколько это вообще было возможно.

Упомянем также еще об одной важной теореме метаматематики, доказанной в 1936 г. американским логиком А. Чёрчем. В ней утверждается, что *не существует эффективной процедуры для решения вопроса относительно произвольной формулы формальной теории, содержащей арифметику натуральных чисел, является ли такая формула теоремой теории*, т.е. всякая такая формальная теория неразрешима. Из этой теоремы вытекает, в частности, и теорема Гёделя о неполноте. Впоследствии была доказана неразрешимость большого числа формальных теорий, в частности элементарной теории групп, элементарной теории полей.

После этих результатов Гёделя стало ясно, что для решения одного из основных вопросов математики — проблемы непротиворечивости, по-видимому, не обойтись без других, отличных от финитистских, средств и идей. Непротиворечивость формальной системы может быть обоснована только средствами более сильными, чем те, которые формализованы в данной системе. Здесь оказались возможными разные подходы, не для всех математиков в равной степени приемлемые или убедительные, в частности, ввиду существования различных точек зрения на допустимость тех или иных логических средств. В 1936 г. Г. Генцен получил доказательство непротиворечивости формальной арифметики, использующее средство, отсутствующее в арифметике, — так называемую трансфинитную (бесконечную) индукцию до некоторого счетного трансфинитного числа.

Теорема Тарского. Приведем еще одну теорему — теорему А. Тарского об истинности, показывающую, что формальным системам присуща ограниченность еще одного типа. Содержательное понятие истинности, которым мы постоянно пользуемся, также поддается формализации. Понятие истинности в формальной системе T определяется относительно другой формальной системы T' . Эта система T' должна быть в определенном смысле сильнее системы T . В 1956 г. Тарский доказал, что понятие истинности (множество всех истинных предложений, множество истинности предиката) в непротиворечивой формальной теории, включающей формальную арифметику, неопределимо в этой теории.

Таким образом, если теорема Гёделя о неполноте обнаруживает принципиальную ограниченность *дедуктивных возможностей* любой достаточно богатой системы, то теорема Тарского вскрывает ограниченность *выразительных возможностей* таких систем.

Перефразируя образное изречение Куайна, можно сказать, что формальные системы попытались проглотить больший кусок онтологии, чем они в состоянии переварить.

Нестандартная модель формальной арифметики и ее некатегоричность. В § 27 мы отмечали, что аксиоматическая теория натуральных чисел, построенная на базе системы аксиом Пеано, категорична, т.е. имеет единственную с точностью до изоморфизма модель. С использованием теоремы Гёделя о неполноте формальной арифметики можно доказать существование неизоморфных моделей формальной арифметики. Таким образом, формальная арифметика, основывающаяся на аксиомах, перечисленных ранее, является *некатегоричной* формальной системой. Этот интересный факт можно объяснить разной трактовкой входящей в обе системы аксиомы индукции. В аксиоме индукции из системы Пеано участвует множество M , на которое не накладывается никаких ограничений и которое может рассматриваться как множество истинности произвольного предиката $F(x)$, т.е. множество натуральных чисел, удовлетворяющих любому мыслимому свойству F натуральных чисел. В соответствующей аксиоме формальной арифметики за F может быть принято не любое свойство натуральных чисел, а лишь такое, которое выразимо средствами данного формализма. Меньшее количество свойств, допустимых в «формальной» аксиоме индукции, априори допускает наличие большего количества объектов (моделей), удовлетворяющих ей. Так и происходит в действительности. Таким образом, различие между этими аксиомами незаметно, пока речь идет о теоремах элементарной теории чисел, и весьма существенно, когда выясняются свойства формальной теории.

Ясно, что моделью формальной арифметики является обычное множество натуральных чисел N , в котором $0' = 1$, $x' = x + 1$ и $+$, $\cdot$ — обычные операции сложения и умножения натуральных чисел.

Пользуясь локальной теоремой Гёделя — Мальцева (см. следствие 29.17 из теоремы 29.16), установив наличие у формальной арифметики одной необычной модели. Она называется *нестандартная модель арифметики*.

Рассмотрим следующую бесконечную совокупность формул формальной арифметики:

$$(\exists y)(x = y + y), (\exists y)(x = y + y + y), \dots, (\exists y)(x = y + y + \dots + y), \dots$$

(в последней формуле в правой части равенства n слагаемых). Первая из этих формул утверждает, что число x делится на 2, вторая — что x делится на 3 и т.д., $(n - 1)$ -я — что x делится на n и т.д. Поэтому обозначим эти формулы соответственно: $2|x$, $3|x$, ...,

$n|x, \dots$ Рассмотрим далее следующую бесконечную совокупность формул:

$$\Sigma_0 = \{(\exists x)(2|x), (\exists x)(2|x \wedge 3|x), \dots, (\exists x)(2|x \wedge 3|x \wedge \dots \wedge n|x), \dots\}.$$

Наконец, обозначив через Σ совокупность из девяти аксиом формальной арифметики, рассмотрим следующее множество формул формальной арифметики $\Sigma_1 = \Sigma \cup \Sigma_0$. Применим к Σ_1 локальную теорему Гёделя — Мальцева. Ясно, что каждое конечное подмножество формул из Σ_1 содержит лишь конечное число формул из Σ_0 и потому имеет модель: его моделью будет обычная система натуральных чисел. Тогда по упомянутой теореме все множество Σ_1 имеет модель. Ее особенностью будет то свойство, что в этой модели будет существовать (натуральное) число, делящееся на все натуральные числа.

О формальных теориях числовых систем. Вопрос о природе понятия числа никогда не стоял на обочине магистрального пути математических исследований во все времена. Математика, достигнув того или иного уровня в своем развитии, неизменно обращалась к своим основам, где центральную роль всегда играло понятие числа. Во второй половине XIX в. в связи с необходимостью обоснования математического анализа и приведения в систему огромного количества результатов, полученных в этой области математики, числа снова оказались в центре внимания математиков. Математика XX в. и прежде всего значительно развившаяся математическая логика еще выше подняли уровень требований к строгости обоснования основ математической науки и в первую очередь понятия числа. Потребовалось создание формальных аксиоматических теорий основных систем чисел. Ведь в конечном итоге математика не интересуется природа чисел и вопрос о том, откуда они берутся. Его интересует, каковы свойства этих чисел, и желательно перечисление всех таких свойств чисел, из которых чисто логически вытекали бы все теоремы соответствующей математической дисциплины и в первую очередь математического анализа.

Первый этап формализации. Выше рассказывалось о формальной арифметике, т.е. о формализации теории натуральных чисел. Здесь будут кратко описаны формальные теории других систем чисел — целых, рациональных, действительных.

Систему целых чисел можно охарактеризовать с помощью следующих условий. Кольцо целых чисел — это есть кольцо с единицей e , не содержащее отличного от него подкольца с единицей и обладающее тем свойством, что $ne \neq 0$ для любого натурального числа n . В самом деле, нетрудно показать, что множество всех элементов вида ne изоморфно системе $\langle \mathbb{N}; + \rangle$ натуральных чисел. Следовательно, данное кольцо содержит подкольцо Z_0 , изоморфное кольцу Z целых чисел, поскольку кольцо Z — минимальное из таких колец. Но так как Z_0 содержит единицу e , то, по усло-

вию, Z_0 должно совпасть с данным кольцом, которое, следовательно, будет кольцом целых чисел.

Систему рациональных чисел можно охарактеризовать с помощью следующих условий. Поле рациональных чисел — это простое поле характеристики нуль. (Поле называется простым, если оно не имеет подполей, отличных от него самого. Говорят, что поле имеет характеристику нуль, если $na \neq 0$ для любого его элемента $a \neq 0$ и любого целого числа $n \neq 0$.) Можно показать, что любое такое поле совпадает со своим подполем частных и, значит, изоморфно полю рациональных чисел. Другими словами, можно сказать, что поле рациональных чисел в известном смысле является минимальным среди всех полей характеристики нуль или что любое поле характеристики нуль содержит в качестве подполя поле рациональных чисел.

Для *системы действительных чисел* известно довольно много разнообразных аксиоматических характеристик, т. е. таких систем аксиом, для которых система действительных чисел является единственной с точностью до изоморфизма моделью. Согласно одной из них множество вещественных чисел характеризуется как полное упорядоченное поле, т. е. как поле, в котором любое ограниченное сверху множество имеет точную верхнюю грань.

Гильберт охарактеризовал множество вещественных чисел как максимальное архимедово упорядоченное поле (т. е. любое поле, являющееся его расширением, уже не архимедово).

Наконец, третья характеристика утверждает, что система действительных чисел и только она является плотным в себе полным по Дедекинду линейно упорядоченным множеством без наименьшего и наибольшего элементов, в котором существует счетное всюду плотное подмножество. (Плотность означает, что между любыми двумя элементами множества расположен еще хотя бы один элемент. Полнота по Дедекинду: всякое непустое ограниченное сверху подмножество имеет точную верхнюю грань. Существование всюду плотного подмножества, называемое свойством сепарабельности (отделимости), означает, что для каждого элемента множества существует как угодно близкий к нему элемент этого подмножества.)

Проблема М. Я. Суслина. С этой характеристикой системы действительных чисел связана одна из знаменитейших проблем XX в. — проблема М. Я. Суслина. Эта проблема состоит в том, что требуется узнать, сохранится ли указанная характеристика системы действительных чисел, если в ней последнее условие сепарабельности заменить более слабым требованием, называемым условием Суслина: любая система из попарно не пересекающихся непустых интервалов не более чем счетна. Другими словами, будет ли изоморфно системе действительных чисел линейно упорядо-

ченное множество, удовлетворяющее перечисленным выше условиям, кроме сепарабельности, и условию Суслина.

Судьба этой проблемы оказалась поистине исторической, и на ее решение потребовалось более 40 лет. Предположение о ее положительном решении получило название гипотезы Суслина. Контрпример к гипотезе (хотя пока и не существующий), т.е. упорядоченное множество, удовлетворяющее всем условиям проблемы М.Я. Суслина, но не изоморфное действительной прямой, получил название континуум Суслина. Эта проблема встала в один ряд с континуум-проблемой Кантора, и полное решение их обеих было получено лишь в начале 1960-х гг., когда американский математик П. Коэн открыл принципиально новый метод доказательства, получивший название метода форсинга (вынуждения). (За это открытие он был удостоен в 1966 г. на Международном математическом конгрессе в Москве высшей международной награды, которой удостоиваются ученые-математики, — Филдсовской премии.) Выяснилось, что проблему Суслина, как и континуум-проблему Кантора, вообще невозможно решить в обычном смысле слов — решить проблему, т.е. дать определенный ответ «да» или «нет» на поставленный вопрос. Гипотеза Суслина, как и континуум-гипотеза Кантора, оказалась не зависящей от остальных аксиом теории множеств. Другими словами, возможна теория множеств, в которой гипотеза Суслина справедлива, и возможна теория множеств, в которой эта гипотеза не выполняется. Кроме того, была также установлена взаимная независимость и самих двух гипотез — гипотезы Суслина и континуум-гипотезы Кантора.

Вопросы, связанные с гипотезой Суслина, продолжают исследоваться в многочисленных работах по теории множеств. Рассматриваются обобщения этой гипотезы, вводятся новые, связанные с ней понятия и конструкции, которые называются именем Суслина. Они широко используются не только в теории множеств, но и проникают в смежные с ней области — теорию моделей, теоретико-множественную топологию. В обширном потоке современных публикаций по этим дисциплинам часто встречается имя М.Я. Суслина: суслинские множества, критерий Суслина, гипотеза Суслина, континуум Суслина, свойство Суслина, дерево Суслина, число Суслина, коэффициент Суслина и т.д.

М.Я. Суслин (1894—1919) родился в селе Красавка Самойловского района Саратовской области. О его жизни и математических открытиях можно прочитать в книге В.И. Игошина¹.

Углубление формализации: элементарная теория вещественно замкнутых полей. С точки зрения строго формального подхода и к описанным только что фор-

¹ Игошин В.И. Михаил Яковлевич Суслин (1894—1919). — М., 1996.

мальным теориям числовых систем, и к формальной арифметике, описанной выше, можно высказать серьезные претензии. Суть их состоит в том, что все эти теории все же еще не до конца формализованы. Дело в том, что приведенные выше характеристики, например системы действительных чисел, сформулированы в терминах не только основных, элементарных понятий, таких, как $+$, $\cdot$, $\leq$ и т.п., но и в терминах, относящихся к понятиям более высокого типа, таких, как «ограниченное сверху множество», «счетное всюду плотное подмножество» и т.п. Другими словами, эти характеристики выражены не на языке первой ступени, а на языке более высокой ступени, в котором понятие множества выступает как самостоятельный индивид. На первый взгляд может показаться, что для углубления формализации понятия действительного числа далее следует приступить к формализации концепции множества. Но теория множеств таит в себе немало проблем и подводных камней (таких, как, например, континуум-гипотеза), которые могут не иметь никакого отношения к предмету изучения. На практике множества, нужные в такой области, как теория чисел, — это лишь такие, которые могут быть описаны с помощью совсем специальных свойств. Поэтому возможен другой подход к формализации теорий числовых систем — изгнать из аксиоматик упоминания о множествах и заменить их соответствующими свойствами. Так, содержательная аксиома индукции Пеано «Любое множество натуральных чисел, которое содержит 0 и вместе с любым своим элементом x содержит также следующий элемент x' , — это множество всех натуральных чисел» при таком подходе превращается в схему формальных аксиом

$$(F(0) \wedge (\forall x)(F(x) \rightarrow F(x'))) \rightarrow (\forall x)(F(x)),$$

где $F(x)$ — произвольная формула с одной свободной предметной переменной x . Таких формул бесконечно много, и соответствующая формальная аксиома формулируется для каждой из них. Можно показать, что такая схема аксиом не может исчерпать всей силы содержательной аксиомы индукции в том смысле, что нельзя посредством такой схемы (наряду с другими формальными аксиомами формальной арифметики) обеспечить, чтобы единственной с точностью до изоморфизма моделью такой системы аксиом было множество натуральных чисел (что, напомним, обеспечивала содержательная система аксиом Пеано). Тем не менее для многих целей вполне достаточно употреблять эту форму аксиомы индукции.

Аналогично обстоит дело с содержательным свойством полноты поля действительных чисел: всякое ограниченное сверху множество имеет точную верхнюю грань. При его формализации приходится вводить схему аксиом (называемую аксиомой полноты),

в которой снова понятие множества заменено на определяющее его свойство $F(x)$:

$$[(\exists x)(F(x)) \wedge (\exists b)(\forall x)(F(x) \rightarrow x \leq b)] \rightarrow \\ \rightarrow (\exists b)[(\forall x)(F(x) \rightarrow x \leq b) \wedge (\forall c)[(\forall x)(F(x) \rightarrow x \leq c) \rightarrow b \leq c]].$$

Словесно эту запись можно прочесть так: если существует число, обладающее свойством F , и всякое число, обладающее этим свойством, меньше некоторого числа, то существует наименьшее такое число, что все числа, обладающие свойством F , меньше его. В связи с такой формализацией возникает естественный вопрос, до какой степени она отражает «полное содержание» исходной аксиомы полноты в ее содержательной теоретико-множественной формулировке. Еще раз отметим, что представленный в наше распоряжение формальный язык узкого исчисления предикатов первого порядка не позволяет говорить о множествах как элементах области индивидов. Поэтому, рассматривая множества, мы говорим об определяющих их свойствах, точнее, о выразимых в данном языке свойствах индивидов, а именно вещественных чисел. Например, чтобы сказать, что множество вещественных чисел x , обладающих свойством $F(x)$, не пусто, мы пишем просто $(\exists x)(F(x))$; существование верхней грани выражается формулой $(\exists b)(\forall x)(F(x) \rightarrow x \leq b)$ и т.д. Это и дает приведенную выше формальную запись аксиомы полноты. Вопрос о том, насколько мы при этом отделились от первичной теоретико-множественной аксиомы полноты, — это по существу, вопрос о том, каков класс множеств, определимых свойствами $F(x)$.

Таким образом, формальная (элементарная) теория вещественных чисел может быть построена на базе системы следующих аксиом:

аксиомы поля;

аксиомы порядка: $x \leq x$,

$$(x \leq y \wedge y \leq x) \rightarrow x = y,$$

$$(x \leq y \wedge y \leq z) \rightarrow x \leq z,$$

$$x \leq y \vee y \leq x,$$

$$x \leq y \rightarrow x + z \leq y + z,$$

$$(x \leq y \wedge z \geq 0) \rightarrow x \cdot z \leq y \cdot z;$$

аксиома полноты (схема аксиом).

Это означает, что система действительных чисел есть полное линейно упорядоченное поле.

Иногда аксиому полноты формулируют в более ограниченном виде — не для произвольного свойства $F(x)$ действительных чисел x , а для конкретного свойства: $a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0 = 0$ — быть корнем алгебраического многочлена. В этом случае аксиома полноты формулируется так:

$$(\forall a_0, \dots, a_m, b, c) [b < c \wedge p_m(b) < 0 \wedge p_m(c) > 0 \rightarrow (\exists z)(b < z < c \wedge \wedge p_m(z) = 0],$$

где $p_m(x) = a_mx^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$. Или же в этом случае аксиома полноты распадается на две части:

$(\forall x)(\exists y)(x = y^2 \vee -x = y^2)$ (из каждого вещественного числа или противоположного ему числа можно извлечь квадратный корень);

$(\forall a_0, a_1, \dots, a_{2n+1})(\exists z)(p_{2n+1}(z) = 0)$ (каждый алгебраический многочлен нечетной степени имеет хотя бы один вещественный корень).

Аксиомы поля и аксиомы порядка (т.е. аксиомы линейно упорядоченного поля) и аксиома полноты в одной из двух последних формулировок образуют систему аксиом элементарной теории так называемых *вещественно-замкнутых полей*.

Разрешимость и абсолютная полнота элементарной теории вещественно-замкнутых полей. Приведенные в предыдущем пункте системы аксиом представляют собой попытки аксиоматизировать совокупность свойств, справедливых в системе действительных чисел. Считается, что самый большой успех аксиоматизации достигнут, если с ее помощью удастся обосновать эффективную разрешающую процедуру, т.е. процедуру, которая для любого предложения S , сформулированного на данном формальном языке, распознает за конечное число шагов его истинность в подразумеваемой структуре, в данном случае в системе действительных чисел. В 1930-е гг. А. Тарский доказал, что для любого данного суждения о действительных числах, которое может быть выражено на формальном языке элементарной теории вещественно-замкнутых полей, либо само это суждение, либо его отрицание доказуемо в этой теории, т.е. выводимо из ее аксиом. Это означает, что элементарная теория вещественно-замкнутых полей абсолютно полна, а соответствующая система аксиом по существу определяет алгебраические свойства действительных чисел. При этом разрешающая процедура (алгоритм) основана на так называемом *методе элиминации* (ликвидации) *кванторов*, который впервые применили Ленгфорд и Пресбургер в 1920-е гг. Этот метод оказался чрезвычайно эффективным и впоследствии нашел многочисленные применения для решения проблемы разрешимости в самых разных разделах математики [7.7].

Идея метода элиминации кванторов состоит в следующем. Вначале доказывается, что для любой формулы A (рассматриваемой теории первого порядка) вида $(\exists x)(A_1(x) \wedge \dots \wedge A_n(x))$, где $A_i(x)$ — атомарная формула или отрицание атомарной формулы, найдется такая бескванторная формула B , что в данной теории доказуема (выводима) эквивалентность $A \leftrightarrow B$. Основываясь на этом утверждении, к каждой замкнутой формуле (предложению) S

данной теории может быть применена процедура элиминации кванторов, которая состоит в следующем:

1) превратить самые внутренние кванторы этого предложения в кванторы существования, если они не таковы (пользоваться при этом законами де Моргана);

2) привести область действия каждого из этих кванторов к дизъюнктивной нормальной форме;

3) распределить кванторы существования по дизъюнктивным членам;

4) заменить все $\exists$ -формулы A эквивалентными им бескванторными формулами B на основании предыдущего утверждения;

5) если полученная формула все еще не является бескванторной, то повторить описанные шаги, начиная с п. 1; в противном случае рассматриваемое предложение S превратилось бы либо в истину, либо в ложь.

Таким образом, метод элиминации кванторов сводит логический вопрос о (раз)решении к математическому вопросу о критериях существования решения совершенно определенной задачи. Что касается теории вещественно-замкнутых полей, то решение обсуждаемой проблемы в ней основывается на классической теореме Штурма (доказанной еще в 1829 г.) и доставляющей средство определения числа (вещественных) корней алгебраического многочлена с целыми коэффициентами между двумя заданными границами, а также общего числа корней такого многочлена (см., например, [7.1, § 79]).

Теорема утверждает, что число корней между b и c ($b < c$) многочлена $p(x)$ равно (без учета кратности) числу перемен знака в так называемом ряду Штурма этого многочлена. В удобной для элиминации кванторов форме эта теорема может быть сформулирована следующим образом: для каждого многочлена $p(x, a_1, \dots, a_n)$ с целыми коэффициентами имеется такая бескванторная формула $B(a_1, \dots, a_n, b, c)$, что эквивалентность

$$(\exists x)(b < x < c \wedge p(x, a_1, \dots, a_n) = 0) \leftrightarrow (b < c \rightarrow B(a_1, \dots, a_n, b, c))$$

выводима из аксиом элементарной теории вещественно-замкнутых полей.

Заслуга А. Тарского состоит в том, что он доказал эту теорему в следующем обобщенном виде: для любой бескванторной формулы $A(x)$ найдется такая бескванторная формула $B(b, c)$, что эквивалентность $(\exists x)(b < x < c \wedge A(x)) \leftrightarrow (b < c \rightarrow B(b, c))$ выводима из аксиом элементарной теории вещественно-замкнутых полей. (Подробное доказательство этой *обобщенной теоремы Штурма* содержится в [5.28, с. 25—31].) С помощью этой теоремы уже легко обосновывается процедура элиминации кванторов для элементарной теории вещественно-замкнутых полей. В самом

деле, пусть $A(x)$ — бескванторная формула с единственной свободной переменной x и мы хотим элиминировать (удалить) квантор $\exists x$ из формулы $(\exists x)(A(x))$. Очевидно, что в любом линейно упорядоченном поле справедливо утверждение (эквивалентность)

$$(\exists x)(A(x)) \leftrightarrow [A(-1) \vee A(1) \vee (\exists x)(-1 < x < 1 \wedge A(x)) \vee (\exists x)(-1 < x < 0 \wedge A(x^{-1})) \vee (\exists x)(0 < x < 1 \wedge A(x^{-1}))].$$

Но ведь из этой формулы можно удалить кванторы на основании обобщенной теоремы Штурма.

Итак, выводимость из аксиом вещественно-замкнутых полей разрешима, т. е. разрешима элементарная теория вещественно-замкнутых полей. Более того, эта теория полна, т. е. для любого данного суждения о действительных числах, которое может быть выражено на формальном языке формальной теории вещественно-замкнутых полей, либо само это суждение, либо его отрицание выводимо из аксиом этой теории. Кроме того, А. Тарский показал, что теорема элементарной алгебры истинна в поле вещественных чисел тогда и только тогда, когда она верна во всех вещественно-замкнутых полях, т. е. выводима в элементарной теории вещественно-замкнутых полей.

О формальной геометрии. В вопросе о понятии математического пространства особенно остро проявляется проблема соотношения математики с окружающей действительностью. Математической наукой о физическом пространстве как раз и является геометрия. Ньютон считал, что основанием для геометрии является практика механики, и в действительности геометрия есть не что иное, как та часть механики в целом, которая точно устанавливает и обосновывает искусство измерения. Следовательно, смысл геометрии заключается в подведении под искусство измерения прочного и достаточно обязательного базиса: необходимо, чтобы математические следствия основных допущений о физическом пространстве можно было проверить фактическим измерением в этом пространстве. Но установление соответствия между математической теорией и эфемерным реальным пространством не является математической задачей. С точки зрения математики задача формализации геометрии выглядит примерно следующим образом. Нужно принять некоторую математическую концепцию реального физического пространства. Поскольку в качестве системы расстояний в евклидовой геометрии принимается поле R вещественных чисел, геометрию проще всего понимать, например, по Вейлю — как точечное пространство E над соответствующим векторным пространством V над полем R . Теперь программу формализации (аксиоматизации) можно сформулировать следующим образом. Выбрав конечное число первичных геометрических понятий (элементов) и отношений между ними, найти такую систему аксиом для этих элементов и отношений,

для которой из того, что некоторая элементарная теорема верна для принятого в E определения основных понятий, вытекает, что она выводима из принятых аксиом, и, обратно, выводимость влечет истинность. (Здесь, как и обычно, мы называем высказывание элементарным, если оно выразимо в языке первой ступени с рассматриваемыми отношениями на рассматриваемых элементах.) Эта программа аксиоматизации реализуется посредством так называемой координатизации исходного геометрического пространства E .

Координатизация геометрического пространства. Хорошо известна модель планиметрической части системы аксиом Гильберта, в которой точкой плоскости является упорядоченная пара (x, y) действительных чисел, а прямой линией — фактически алгебраическое уравнение первой степени. При ее создании геометрия строится из чисел. Задача координатизации состоит в обратном: построить числовую систему, исходя из геометрии (т.е. из точек и прямых). Точнее, пусть имеется некоторая планиметрия, объектами которой являются элементы двух множеств — множества точек (обозначаются заглавными латинскими буквами) и множества прямых (обозначаются малыми латинскими буквами), для которых справедливы аксиомы Гильберта в их планиметрической части. (При этом основным отношением является отношение инцидентности (принадлежности): $A \in l$ — точка A принадлежит прямой l .) Требуется построить такое поле K , изоморфное полю R вещественных чисел, чтобы точки в нашей геометрии задавались упорядоченными парами элементов (координатами) из K , а прямые — линейными алгебраическими уравнениями.

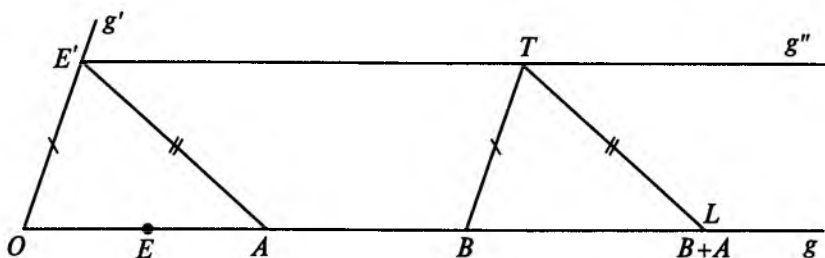
Из аксиом (I.1) — (I.3) первой группы аксиом системы аксиом Гильберта вытекает существование в нашей планиметрии фигуры, играющей важнейшую роль в процессе ее координатизации. Эта фигура состоит из двух прямых g, g' , пересекающихся в точке Q , и двух отличных от Q точек E и E' , лежащих соответственно на этих прямых. Элементами поля K будут точки прямой g . Для точек этой прямой мы введем операции поля — сложение и умножение — геометрически, т.е. определим их через инцидентность, причем точка E будет представлять единицу для умножения, а точка Q — нуль для сложения. Возможность использования этой фигуры для изображения конструкции сложения и умножения точек прямой основана на следующей лемме, которая легко выводится из аксиомы параллельности (V).

Лемма 30.4. *Если две различные прямые h и g пересекаются, то всякая прямая h' , параллельная h , также пересекается с g .*

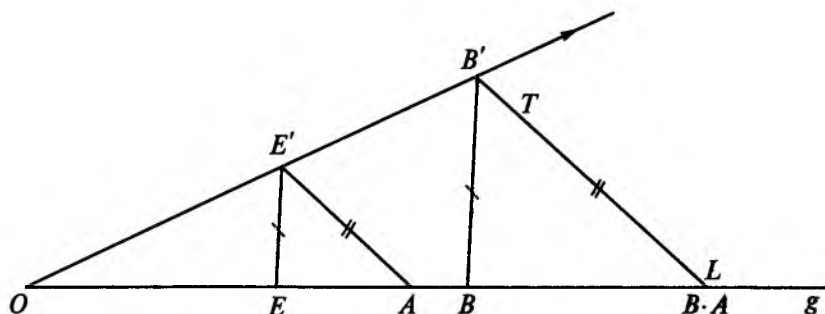
Доказательство. Если допустить, что это не так для некоторой прямой h' , то через точку пересечения прямых h и g , не принадлежащую прямой h' , проходит две различных прямых h и

g , не пересекающихся с h' , что противоречит аксиоме параллельности Евклида. $\square$

Теперь определяем сложение точек B и A прямой g с помощью следующих построений. В нашей фигуре g, g', O, E, E' проводим прямые: $g'': E' \in g'', g'' \parallel g$; $BT: B \in BT, BT \parallel g'$; $TL: T \in TL, TL \parallel AE'$. Тогда $BL = OA$, и, следовательно, $OB + OA = OB + BL = OL$.



Аналогично определяется умножение точек B и A прямой g с помощью следующих построений. Проводим прямые $BB': B \in BB', BB' \parallel EE'$ и $B'L: B' \in B'L, B'L \parallel E'A$. Тогда из подобия треугольников OAE' и OLB' вытекает, что $OA:OL = OE:OB$, т.е. $OL \cdot OE = OB \cdot OA$ (OE — единичный отрезок).



Можно показать, что так определяемые операции определены корректно и удовлетворяют всем аксиомам поля. Упорядочение в этом поле основывается на геометрическом отношении «между»: $\mu(ABC)$ — точка B лежит между точками A и C . Сначала определяется понятие положительности: $A > O \Leftrightarrow A \neq O \wedge \neg\mu(AOE)$. Затем, исходя из гильбертовых аксиом второй группы (аксиомы порядка), устанавливается выполнимость в построенном поле аксиом порядка: $\neg(O > O)$; $A > 0 \vee \neg A > 0 \vee A = 0$; $(A > 0 \wedge B > 0) \rightarrow \rightarrow (A + B > 0 \wedge A \cdot B > 0)$.

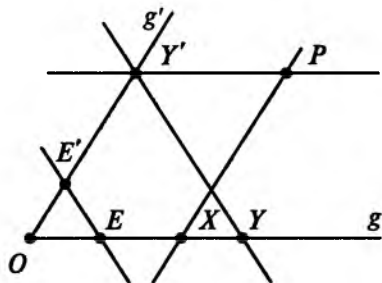
Наконец, чтобы наше упорядоченное поле было полным (всякое ограниченное сверху подмножество имело точную верхнюю грань), нужно, чтобы исходная геометрия удовлетворяла аксиоме непрерывности (или полноты). Известны различные формы

таких аксиом, например Кантора, Дедекинда. Приведем еще одну формулировку.

Аксиома полноты: пусть M и N — два непустых множества точек на прямой g и пусть имеется точка C , такая, что для всех $A \in M$ и $B \in N$ верно $\mu(CAB)$. Тогда имеется такая точка D , что для всех $A \in M$ и $B \in N$, отличных от D , верно $\mu(ADB)$.

Из геометрической аксиомы полноты (непрерывности) немедленно следует, что поле, построенное на прямой g , полно. Это фактически завершает доказательство того, что построенное поле изоморфно полю R вещественных чисел.

Поле, построенное на прямой g , можно использовать теперь, для координатизации всей плоскости. Для этого нужно сначала построить поле и на прямой g' так же, как это сделано на прямой g (E' — единичная точка на g'). Построенные на g' и g поля оказываются изоморфными: изоморфизм осуществляется проектированием параллельно прямой EE' . Теперь каждой точке P плоскости мы можем сопоставить упорядоченную пару (X, Y) точек (вещественных чисел), как показано на следующем рисунке.



Остается выразить требование взаимной перпендикулярности осей координат g и g' и равенства единичных отрезков $OE = OE'$. Это достигается с помощью гильбертовых аксиом III группы — аксиом конгруэнтности отрезков и углов.

Если $P(X_1, Y_1)$ и $Q(X_2, Y_2)$ — две точки плоскости со своими координатами, то точечное пространство упорядоченных пар (X, Y) можно рассматривать над векторным пространством векторов $\overrightarrow{PQ}$ ($X_2 - X_1, Y_2 - Y_1$), в котором скалярное произведение определяется по формуле $\overrightarrow{PQ} \cdot \overrightarrow{ST} = (X_2 - X_1)(X_4 - X_3) + (Y_2 - Y_1)(Y_4 - Y_3)$. В итоге точечное пространство упорядоченных пар (X, Y) оказывается изоморфно исходному евклидову точечному пространству E над векторным пространством V . С подробностями процесса координатизации можно познакомиться в [5.28, с. 57—68], [3.9, § 71].

Элементарная теория евклидовой планиметрии. Задача формализации аксиоматической геометрии, построенной, например, на базе системы аксиом Гильберта, снова ставит нас перед проблемой, уже возникавшей при формализации теорий

числовых систем: как адекватно выразить содержание аксиомы полноты (непрерывности), в формулировке которой участвуют множества M и N , в нашем формальном языке первой ступени, как понимать участвующие там множества? Здесь мы снова выбираем тот же выход, что и при формализации теорий числовых систем: мы заменяем множества определяющими их предикатами (свойствами) в языке первого порядка для элементарной геометрии с исходными понятиями по системе Гильберта. Получаемая таким образом в элементарной форме аксиома полноты (а точнее, схема аксиом, называемая схемой Тарского) может быть сформулирована следующим образом: для любых формул $P(\cdot)$ и $Q(\cdot)$ имеем

$$(\exists C)(\forall A)(\forall B)(P(A) \wedge Q(B) \rightarrow \mu(ABC)) \rightarrow (\exists D)(\forall A)(\forall B)(A \neq D \wedge B \neq D \wedge P(A) \wedge Q(B) \rightarrow \mu(ADB)).$$

Из этой схемы Тарского непосредственно следует, что построенное на прямой g упорядоченное поле удовлетворяет (элементарной) аксиоме полноты из теории вещественных чисел, т.е. в конечном итоге является вещественно-замкнутым полем. Поскольку, как было отмечено выше, эта элементарная теория полна и разрешима, то теперь с помощью изложенной в предыдущем пункте процедуры координатизации эти свойства переносятся и на элементарную теорию евклидовой геометрии.

Таким образом, элементарная теория евклидовой геометрии на плоскости, построенная на основе планиметрических аксиом системы Гильберта, полна, т.е. для любого предложения F в языке элементарной геометрии одно из предложений F или $\neg F$ выводимо из этих аксиом; более того, вопрос о выводимости данного предложения эффективно разрешим. Это связано с тем, что всякую формулу в языке элементарной геометрии можно в силу осуществленной координатизации воспринимать (или перевести) в языке линейной алгебры, основывающейся на полной и разрешимой теории вещественно-замкнутых полей. Фактически это означает справедливость своего рода метатеоремы, утверждающей, что формула элементарной геометрии выводима из аксиом геометрии тогда и только тогда, когда она (или соответствующий ее перевод на язык линейной алгебры) выводима из аксиом линейной алгебры. Подробно это доказательство приведено в статье А. Тарского¹.

О формальном математическом анализе. Это формальная аксиоматическая теория, специально предназначенная для формализации (точного описания доказательств) математического анализа. Таких теорий существует несколько: они характеризуются раз-

¹ *Tarski A. What is elementary geometry? // Henkin, Suppes, Tarski. The axiomatic method. Amsterdam, 1959. P. 16—29.*

личными подходами к формализации. При этом каждую из них стараются построить по возможности минимальной по своим дедуктивным и выразительным возможностям, но все же достаточной для формализации всего традиционного материала математического анализа.

Наиболее распространенной из формальных теорий математического анализа является *теория Гильберта — Бернайса*. Она строится следующим образом. К языку формальной арифметики, описанной в предыдущем пункте, добавляется новый вид переменных $X, Y, Z, \dots$, которые рассматриваются как пробегающие множества натуральных чисел. Добавляется новый вид атомарных формул: $(t \in X)$ (« t принадлежит множеству X »). Логические аксиомы формальной арифметики (т. е. аксиомы формализованного исчисления предикатов) и схема аксиом индукции естественно усиливаются таким образом, чтобы включать в себя формулы расширенного языка. Наконец, добавляется единственная новая схема аксиом — *схема аксиом свертывания*:

$$(\exists x)(\forall y)(y \in X \leftrightarrow A(y)),$$

где $A(y)$ — формула рассматриваемого языка, не содержащая свободно X ; y — переменная для натуральных чисел.

Эта теория Гильберта — Бернайса, хотя в ней речь идет лишь о натуральных числах и о множествах натуральных чисел, достаточна для естественной формализации математического анализа. Интересна проблема обоснования непротиворечивости этой теории. Согласно теореме Гёделя о неполноте формальной арифметики для этого необходимо использовать средства, выходящие за пределы формального математического анализа. В 1962 г. К. Спектор доказал непротиворечивость этой теории с помощью остроумной модификации модели Гёделя для интуиционистской арифметики, которая представляет собой некоторое далеко идущее расширение требований интуиционизма. Трудности в попытках доказательства непротиворечивости теории Гильберта — Бернайса связаны с той особенностью аксиомы свертывания этой теории, что в формуле $A(y)$ этой аксиомы разрешается свободно использовать кванторы по множествам. Таким образом, при выяснении принадлежности числа y определяемому в аксиоме множеству X необходимо использовать наличие всех множеств натуральных чисел, в том числе и определяемого множества X . Можно сказать, что аксиома свертывания формального анализа выражает до некоторой степени необходимость актуального существования всех множеств натуральных чисел одновременно (только после этого в формуле могут использоваться кванторы по переменным, пробегающим множество таких множеств). Эта особенность встречается в ряде формальных теоретико-множественных теорий и называется *непредикативностью* теории. Так что фор-

мальный анализ Гильберта — Бернайса является непредикативной формальной теорией.

Имеется эквивалентная формулировка анализа Гильберта — Бернайса, в которой вместо множеств натуральных чисел фигурируют функции, перерабатывающие натуральные числа в натуральные. Для такого вида функции к формальной арифметике добавляются переменные $\alpha, \beta, \gamma, \dots$ и новый вид термов: $\alpha(t)$ («результат применения α к t »); логические аксиомы и схема аксиом индукции естественно распространяются на формулы нового языка, и, наконец, добавляется единственная новая схема аксиом, называемая *аксиомой выбора анализа*:

$$(\forall x)(\exists y)(A(x, y)) \rightarrow (\exists \alpha)(\forall x)(A(x, \alpha(x))).$$

Эта аксиома утверждает, что если для всякого x найдется y , удовлетворяющий условию $A(x, y)$, то существует функция α , выдающая по x соответствующий y . Ценность этой формулировки состоит в том, что после исключения из числа логических аксиом теории закона исключенного третьего полученная система удобна для формализации в ней интуиционистского (или конструктивного) формального математического анализа, который представляет собой переработку традиционного материала математического анализа в соответствии с требованиями программы интуиционизма (или соответственно конструктивной математики).

Для устранения непредикативности были предложены различные формальные аксиоматические теории предикативного (или развитленного) анализа.

Общий взгляд на процесс формализации математической теории. Ознакомившись с рядом формальных аксиоматических теорий, так или иначе связанных с основаниями школьного курса математики, подведем итог, дав краткую общую характеристику методу формализации. Суть этого метода состоит в следующем. Допустим, у нас имеется некоторая содержательная математическая теория T_1 и нас интересует, является ли она непротиворечивой. Для выяснения этого вопроса данная теория T_1 подвергается формализации. Для этого сначала формализуется точный логико-математический язык Ω , такой, что все интересующие нас утверждения теории T_1 записываются в виде формул языка Ω (математика теории T_1 соединяется с логикой). Затем логические принципы, употреблявшиеся в теории для получения новых фактов, формализуются в виде аксиом и чисто формальных правил вывода, позволяющих выводить новые формулы языка Ω из аксиом и уже выведенных формул. Таким образом возникает формальная аксиоматическая теория (или, иначе, формальная система, исчисление T_1^* , точно описывающая некоторый интересующий нас фрагмент содержательной теории T_1 . Существенно при этом, что формулировка T_1^* не требует исчерпывающего проникновения в, быть

может, весьма сложную семантику теории T_1 . Исчисление T_1 строится по простым законам как чисто знаковая система, и для понимания устройства этой знаковой системы нет необходимости вникать в смысл выводимых в ней формул.

Такой подход открывает возможность строго математически сформулировать интересующие нас проблемы, относящиеся к выводимости некоторых формул в T_1^* . Кроме того, он дает возможность исследовать формальную теорию T_1^* средствами некоторой содержательной теории T_2 . В этой ситуации T_1^* называется *предметной теорией*, а T_2 — ее метатеорией. С точки зрения оснований математики важно, чтобы T_2 была в некотором отношении более надежной теорией, чем T_1 , так что исследование T_1^* средствами теории T_2 можно было бы действительно рассматривать как разъяснение и обоснование неясных деталей семантики T_1 с помощью более убедительной теории T_2 . Если же нас интересует не столько вопрос об интуитивной ясности T_1 , сколько просто факт о выводимости или невыводимости некоторых формул в T_1^* , то T_1^* может исследоваться средствами любой исторически сложившейся и убедительной для исследователя математической теории T_2 .

Один из важнейших вопросов о теории T_1^* есть вопрос о ее формальной непротиворечивости, который состоит в выяснении того, существует ли в языке Ω такая формула F , что сама F и ее отрицание $\neg F$ являются теоремами теории T_1^* (что равносильно выяснению вопроса о том, всякая ли формула языка Ω является теоремой теории T_1^*). Метаматематический метод доказательства непротиворечивости, предложенный в начале XX в. Гильбертом, состоит в том, что утверждение о непротиворечивости формальной системы T_1^* рассматривается как высказывание о возможных в этой системе доказательствах. Само же это высказывание уже принадлежит метатеории T_2 , которая и исследует это утверждение. Такой подход сводит вопрос о непротиворечивости T_1^* к вопросу непротиворечивости другой теории T_2 . При этом говорят, что T_1^* непротиворечива относительно T_2 . Большое значение имеет вторая теорема Гёделя, которая утверждает, что непротиворечивость формальной теории, содержащей формальную арифметику, невозможно доказать с помощью средств самой рассматриваемой теории (при условии, что эта теория действительно непротиворечива). Примером применения метаматематического метода может служить доказательство Г. Генцена непротиворечивости формальной арифметики, полученное им в 1936 г. и использующее трансфинитную индукцию — средство, выходящее за рамки формальной арифметики.

Существует и другой путь доказательства непротиворечивости формальной системы, идущий через понятие интерпретации и модели. Формальная система называется содержательно (или се-

мантически) непротиворечивой, если существует модель, в которой истинны все теоремы этой системы. Без труда устанавливается, что если формальная система содержательно непротиворечива, то она формально непротиворечива. Для формальных систем, основанных на классическом исчислении предикатов 1-го порядка, справедливо и обратное утверждение (теорема Гёделя о модели): всякая непротиворечивая формальная теория имеет модель. Таким образом, другой способ доказательства непротиворечивости формальной теории состоит в построении ее модели. Но и этот метод является относительным: он устанавливает непротиворечивость одной формальной системы относительно другой, в терминах которой построена модель первой.

Можно, далее, исследовать аналогичным образом и метатеорию T_2 , построив формальную систему T_2^* и изучая уже T_2^* средствами следующей содержательной теории T_3 , которая будет метатеорией по отношению к теории T_2 и *метаметатеорией* по отношению к теории T_1 .

О границах аксиоматического метода, метода формализации и логики. Насколько универсален и насколько всемогущ аксиоматический метод и его наивысшее математическое выражение — формализация? Прежде всего, границы методу формализации были поставлены двумя выдающимися теоремами К. Гёделя, доказанными им в 1931 г. Первая из них утверждает, что для всякой непротиворечивой формальной системы, содержащей аксиомы формальной арифметики, можно дать явное описание замкнутой формулы F , такой, что ни сама эта формула, ни ее отрицание $\neg F$ не выводимы в этой формальной системе. Вторая теорема утверждает, что при выполнении некоторых естественных условий в качестве F можно взять утверждение о непротиворечивости данной формальной системы, т. е. в непротиворечивой формальной системе, включающей формальную арифметику, содержится формула, выражающая ее непротиворечивость, и что эта формула недоказуема в этой системе. Доказательство этих утверждений означеновало собой строгое математическое установление того факта, что гильбертовская программа формализации математики не может быть реализована в том виде и в том объеме, в каких ее мыслил Гильберт.

Эти теоремы Гёделя фактически означали, что истинное утверждение не всегда может быть доказано. Эти логические теоремы по существу разрушали восходящее к Лейбницу и Декарту мнение, будто всякое истинное утверждение подвластно обоснованию методами математического доказательства. Но оставалась надежда, что выводимость ненамного меньше истинности, что недоказуемыми являются лишь экзотические формулы гёделевского типа, в которых зашифрованы утверждения, относящиеся к самим этим формулам. Однако результаты, полученные А. Тарским в 1936 г.,

окончательно разрушили и эту последнюю надежду (см. более подробно об этом в Заключении).

Конечно, эти результаты, показывающие, что расстояние от доказуемости (выводимости) до истинности столь велико, могут служить солидным основанием для значительной доли пессимизма в оценке роли логики (и в частности, математической логики) в процессе познания окружающего мира и истины. Некоторые определенные философы истолковывают эти результаты как полное отрицание роли логики в процессе познания, считая, что она нужна лишь для придания уже полученным результатам общепонятной и убедительной формы, а сам механизм получения этих результатов совершенно иной. Не следует истолковывать эти результаты и как полный крах формального подхода к математическим теориям. Эти результаты несомненно означают, что первоначальная «максималистская» гильбертовская программа финитистского подхода к обоснованию математики не может быть реализована в полном объеме: нельзя построить математику как некоторую фиксированную совокупность средств, которые можно было бы объявить единственно законными, и с их помощью строить метатеории любых теорий. Невозможность полной формализации содержательно определенных математических теорий — это не недостаток подхода или концепции, а объективный факт, неустранимый никакой концепцией, «суровая правда» об устройстве мира, изучаемого этой теорией. Невозможность адекватной формализации теории означает, что надо либо искать формализуемые ею фрагменты, либо строить какую-то более сильную формальную теорию, которая, правда, снова будет неполна, но, быть может, будет содержать всю исходную теорию.

Рассматриваемые выдающиеся результаты Гёделя и Тарского демонстрируют не только слабость математической логики в процессах познания, но и ее силу, еще раз являя уникальность этой науки. Она единственная из всех наук своими собственными строгими методами устанавливает границы своей применимости. Фактически средствами математической логики устанавливаются границы применимости математики. Наука с такими уникальными возможностями не может быть бесполезна для дела познания окружающего мира, и, думается, что ее будущие результаты заставят еще не раз как математиков, так и философов обратиться к их интерпретации.

Глава VII

ЭЛЕМЕНТЫ ТЕОРИИ АЛГОРИТМОВ

В предыдущих главах неоднократно использовались термины «алгоритм», «эффективная процедура». Настоящая глава посвящается уточнению и изучению этого понятия. В § 31 более детально обсуждается понятие алгоритма на интуитивной основе и устанавливается необходимость его уточнения, § 32 посвящен изучению одного из возможных уточнений понятия алгоритма — машинам Тьюринга, в § 33 и § 34 дан обзор других возможных уточнений понятия алгоритма — рекурсивных функций и нормальных алгоритмов Маркова. Изложение в них доводится до доказательства равносильности этих трех формализаций понятия алгоритма. § 35 посвящен так называемой общей теории алгоритмов, т. е. теории алгоритмов, не привязываемой ни к какой конкретной формализации понятия алгоритма, § 36 — неразрешимым алгоритмическим проблемам. Завершается глава основывающимся на теории алгоритмов доказательством теоремы Гёделя о неполноте формальной арифметики (см. § 37).

§ 31. Интуитивное представление об алгоритмах

Алгоритмы вокруг нас. Понятие алгоритма стихийно формировалось с древнейших времен. Современный человек понимает под *алгоритмом* четкую систему инструкций о выполнении в определенном порядке некоторых действий для решения всех задач какого-то данного класса.

Многочисленные и разнообразные алгоритмы окружают нас буквально во всех сферах жизни и деятельности. Многие наши действия доведены до бессознательного автоматизма, мы порой и не осознаем, что они регламентированы определенным алгоритмом — четкой системой инструкций. Например, наши действия при входе в магазин «Универсам» (сдать свою сумку, получить корзину с номером, пройти в торговый зал, заполнить корзину продуктами, оплатить покупку в кассе, предъявить чек контролеру, взять свою сумку, переложить в нее продукты, сдать корзину, покинуть магазин). Второй пример — приготовление манной каши (500 мл молока довести до кипения, при тщательном помешива-

нии засыпать 100 г манной крупы, при помешивании довести до кипения и варить 10 минут). Автоматизм выполнения этих и многих других действий не позволяет нам осознавать их алгоритмическую сущность.

Но есть немало таких действий, выполняя которые, мы тщательно следуем той или иной инструкции. Это главным образом непривычные действия, профессионально не свойственные нам. Например, если вы фотографируете один-два раза в год, то, купив проявитель для пленки, будете весьма тщательно следовать инструкции (алгоритму) по его приготовлению: «Содержимое большого пакета растворить в 350 мл воды при температуре 18—20 °С. Там же растворить содержимое малого пакета. Объем раствора довести до 500 мл. Раствор профильтровать. Проявлять 3—4 роликовых фотопленки». Второй пример: если вы никогда раньше не пекли торт, то, получив рецепт (алгоритм) его приготовления, постараетесь выполнить в указанной последовательности все его предписания.

Большое количество алгоритмов встречается при изучении математики буквально с первых классов школы. Это прежде всего алгоритмы выполнения четырех арифметических действий над различными числами — натуральными, целыми, дробными, комплексными. Вот пример такого алгоритма: «Чтобы из одной десятичной дроби вычесть другую, надо: 1) уравнивать число знаков после запятой в уменьшаемом и вычитаемом; 2) записать вычитаемое под уменьшаемым так, чтобы запятая оказалась под запятой; 3) произвести вычитание так, как вычитают натуральные числа; 4) поставить в полученной разности запятую под запятыми в уменьшаемом и вычитаемом».

Вот пример алгоритма сложения приближенных чисел. Найти сумму чисел p , q и s , где $p \approx 3,1416$, $q \approx 2,718$ и $s \approx 7,45$.

1. Выделим слагаемое с наименьшим числом десятичных знаков. Таким слагаемым является число 7,45 (два десятичных знака).

2. Округлим остальные слагаемые, оставляя в них столько десятичных знаков, сколько их имеется в выделенном слагаемом: $3,1416 \approx 3,14$; $2,718 \approx 2,72$.

3. Выполним сложение приближенных значений чисел: $3,14 + 2,72 + 7,45 = 13,31$.

Итак, $p + q + s \approx 13,31$.

Немало алгоритмов в геометрии: алгоритмы геометрических построений с помощью циркуля и линейки (деление пополам отрезка и угла, опускание и восстановление перпендикуляров, проведение параллельных прямых), алгоритмы вычисления площадей и объемов различных геометрических фигур и тел.

При изучении математики в вузе были освоены процедуры вычисления наибольшего общего делителя двух натуральных чисел (алгоритм Евклида), определителей различных порядков, рангов

матриц с рациональными элементами, интегралов от рациональных функций, приближенных значений корней уравнений и систем и т. д. Все эти процедуры являются не чем иным, как алгоритмами. Наконец, в изучаемом курсе математической логики были рассмотрены алгоритмы разрешимости формализованного исчисления высказываний (см. § 16) и разрешимости в логике предикатов (§ 23).

Одним словом, алгоритмы широко распространены как в практике, так и в науке и требуют более внимательного к себе отношения и тщательного изучения методами математической науки.

Неформальное понятие алгоритма. Прежде чем перейти к математическому изучению понятия алгоритма, постараемся внимательно проанализировать примеры алгоритмов, выявить их общие типичные черты и особенности.

Каждый алгоритм предполагает наличие некоторых *начальных*, или *исходных*, *данных*, а в результате применения приводит к получению определенного искомого *результата*. Например, в алгоритме с проявителем начальные данные — содержимое большого и малого пакетов, вода. Искомый результат — готовый к употреблению проявитель для пленки. При вычислении ранга матрицы начальными данными служит прямоугольная таблица, составленная из $m \cdot n$ рациональных чисел, результат — натуральное число, являющееся рангом данной матрицы.

Далее, применение каждого алгоритма осуществляется путем выполнения дискретной цепочки (последовательности) неких элементарных действий. Эти действия называют шагами, а процесс их выполнения называют *алгоритмическим процессом*. Таким образом, отмечается свойство *дискретности алгоритма*.

Существенной чертой алгоритма является его *массовый характер*, т. е. возможность применять его к обширному классу начальных данных, возможность достаточно широко эти начальные данные варьировать. Другими словами, каждый алгоритм призван решить ту или иную *массовую проблему*, т. е. решать класс однотипных задач. Например, задача нахождения наибольшего общего делителя чисел 4 и 6 есть единичная проблема (можно решить ее и без применения алгоритма Евклида), но задача нахождения наибольшего общего делителя произвольных натуральных чисел m и n — уже проблема массовая. Суть алгоритма Евклида состоит в том, что он приводит к желаемому результату вне зависимости от выбора конкретной пары натуральных чисел, в то время как при решении указанной единичной проблемы можно предложить такой способ, который окажется неприменимым для другой пары натуральных чисел.

Непременным условием, которому удовлетворяет алгоритм, является его *детерминированность*, или *определенность*. Это означает, что предписания алгоритма с равным успехом могут быть

выполнены любым другим человеком и в любое другое время, причем результат получится тот же самый. Другими словами, предписания алгоритма настолько точны и отчетливы, что не допускают никаких двусмысленных толкований и никакого произвола со стороны исполнителя. Они единственным и вполне определенным путем всякий раз приводят к искомому результату. Это наводит на мысль, что выполнение тех или иных алгоритмов может быть поручено машине, что широко и делается на практике.

Говоря о начальных данных для алгоритма, имеют в виду так называемые *допустимые начальные данные*, т.е. такие начальные данные, которые сформулированы в терминах данного алгоритма. Так, к числу допустимых начальных данных для алгоритма варки манной каши никак не отнесешь элементы множества натуральных чисел, а к числу начальных данных алгоритма Евклида — молоко и манную крупу (или даже комплексные числа).

Среди допустимых начальных данных для алгоритма могут быть такие, к которым он применим, т.е. отправляясь от которых можно получить искомый результат, а могут быть и такие, к которым данный алгоритм неприменим, т.е. отправляясь от которых искомого результата получить нельзя. Неприменимость алгоритма к допустимым начальным данным может заключаться либо в том, что алгоритмический процесс никогда не оканчивается (в этом случае говорят, что он бесконечен), либо в том, что его выполнение во время одного из шагов наталкивается на препятствие, заходит в тупик (в этом случае говорят, что он безрезультатно обрывается). Проиллюстрируем на примерах оба случая.

Пример 31.1. Приведем пример бесконечного алгоритмического процесса. Всем известен алгоритм деления десятичных дробей. Числа 5,1 и 3 являются для него допустимыми начальными данными, применение к которым алгоритма деления приводит к искомому результату 1,7. Иная картина возникает для чисел 20 и 3, которые также представляют собой допустимые начальные данные. Для них получается алгоритмический процесс:

$$\begin{array}{r|l}
 20 & 3 \\
 -18 & 6,66... \\
 \hline
 20 & \\
 -18 & \\
 \hline
 20 & \\
 \dots &
 \end{array}$$

Этот процесс не встречает препятствий и никогда не оканчивается, так что получить искомый результат для начальных данных 20 и 3 оказывается невозможно. Отметим, что обрыв процесса произвольным образом не предусматривается данным алгоритмом.

Пример 31.2. Теперь приведем пример алгоритма, заходящего в тупик, безрезультатно обрывающегося. Вот его предписания.

1. Исходное число умножить на 2. Перейти к выполнению п. 2.
2. К полученному числу прибавить 1. Перейти к выполнению п. 3.
3. Определить остаток y от деления полученной в п. 2 суммы на 3. Перейти к выполнению п. 4.
4. Разделить исходное число на y . Частное является искомым результатом. Конец.

Пусть натуральные (целые положительные) числа будут допустимыми начальными данными для этого алгоритма. Для числа 6 алгоритмический процесс будет проходить так:

1-й шаг: $6 \cdot 2 = 12$; переходим к п. 2;

2-й шаг: $12 + 1 = 13$; переходим к п. 3;

3-й шаг: $y = 1$, переходим к п. 4;

4-й шаг: $6 : 1 = 6$. Конец.

Искомый результат равен 6. Иначе будет протекать алгоритмический процесс для исходного данного 7:

1-й шаг: $7 \cdot 2 = 14$; переходим к п. 2;

2-й шаг: $14 + 1 = 15$; переходим к п. 3;

3-й шаг: $y = 0$; переходим к п. 4;

4-й шаг: $7 : 0$ — деление невозможно. Процесс зашел в тупик, натолкнулся на препятствие и безрезультатно оборвался.

Итак, подводя итоги обсуждению характерных свойств и особенностей алгоритма, можем сформулировать следующее интуитивно описательное определение этого понятия.

Под *алгоритмом* понимается четкая система инструкций, определяющая дискретный детерминированный процесс, ведущий от варьируемых начальных данных (входов) к искомому результату (выходу), если таковой существует, через конечное число тактов работы алгоритма; если же искомого результата не существует, то вычислительный процесс либо никогда не оканчивается, либо попадает в тупик.

Отметим в заключение, что сам термин «алгоритм» (или «алгорифм») происходит от имени великого среднеазиатского ученого Мухаммеда аль-Хорезми (787 — ок. 850). В своем трактате, написанном по-арабски, латинская версия которого относится к XII в. и начинается словами «Dixit algorizim», т. е. «Сказал аль-Хорезми», им среди прочего была описана индийская позиционная система чисел и сформулированы правила выполнения четырех арифметических действий над числами в десятичной записи.

Необходимость уточнения понятия алгоритма. Понятие алгоритма формировалось с древнейших времен, но до конца первой трети XX в. математики довольствовались интуитивным представлением об этом объекте. Термин «алгоритм» употреблялся в математике лишь в связи с теми или иными конкретными алгоритмами. Ут-

верждение о существовании алгоритма для решения задач данного типа сопровождалось фактическим его описанием.

Парадоксы, обнаруженные в основаниях математики в начале XX в., вызвали к жизни различные концепции и течения, призванные эти парадоксы устранить. В 1920-е гг. вплотную встали вопросы о том, что же такое строгая выводимость и эффективное вычисление. Понятие алгоритма само должно было стать объектом математического исследования и поэтому нуждалось в строгом определении. Кроме того, к этому вынуждало развитие физики и техники, быстро приближавшее начало века электронно-вычислительных машин.

Далее, у математиков начали возникать подозрения в том, что некоторые массовые задачи, по-видимому, не имеют алгоритмического решения. Для точного доказательства несуществования какого-то объекта необходимо иметь его точное математическое определение. Совершенно аналогичная ситуация сложилась в свое время в математике, когда назрела необходимость уточнения таких понятий, как непрерывность, кривая, поверхность, длина, площадь, объем и т.п.

Первые работы по уточнению понятия алгоритма и его изучению, т.е. по теории алгоритмов, были выполнены в 1936—1937 гг. математиками А. Тьюрингом, Э. Постом, Ж. Эрбраном, К. Гёделем, А.А. Марковым, А. Чёрчем. Было выработано несколько определений понятия алгоритма, но впоследствии выяснилось, что все они равносильны между собой, т.е. определяют одно и то же понятие.

§ 32. Машины Тьюринга

Введение понятия машины Тьюринга явилось одной из первых и весьма удачных попыток дать точный математический эквивалент для общего интуитивного представления об алгоритме. Это понятие названо по имени английского математика, сформулировавшего его в 1937 г., за 9 лет до появления первой электронно-вычислительной машины.

Определение машины Тьюринга. Машина Тьюринга есть математическая (воображаемая) машина, а не машина физическая. Она есть такой же математический объект, как функция, производная, интеграл, группа и т.д. И так же как и другие математические понятия, понятие машины Тьюринга отражает объективную реальность, моделирует некие реальные процессы. Именно Тьюринг предпринял попытку смоделировать действия математика (или другого человека), осуществляющего некую умственную созидательную деятельность. Такой человек, находясь в определенном «умонастроении» («состоянии»), просматривает некоторый текст. Затем он вносит в этот текст какие-то изменения, проникается

новым «умонастроением» и переходит к просмотру последующих записей.

Машина Тьюринга действует примерно так же. Ее удобно представлять в виде автоматически работающего устройства. В каждый дискретный момент времени устройство, находясь в некотором состоянии, обозревает содержимое одной ячейки протягиваемой через устройство ленты и делает шаг, заключающийся в том, что устройство переходит в новое состояние, изменяет (или оставляет без изменения) содержимое обозреваемой ячейки и переходит к обозрению следующей ячейки — справа или слева. Причем шаг осуществляется на основании предписанной команды. Совокупность всех команд представляет собой программу машины Тьюринга.

Опишем теперь машину Тьюринга Θ более тщательно. Машина Θ располагает конечным числом знаков (символов, букв), образующих так называемый *внешний алфавит* $A = \{a_0, a_1, \dots, a_n\}$. В каждую ячейку обозреваемой ленты в каждый дискретный момент времени может быть записан только один символ из алфавита A . Ради единообразия удобно считать, что среди букв внешнего алфавита A имеется «пустая буква», и именно она записана в пустую ячейку ленты. Условимся, что «пустой буквой» или символом пустой ячейки является буква a_0 . Лента предполагается неограниченной в обе стороны, но в каждый момент времени на ней записано конечное число непустых букв.

Далее, в каждый момент времени машина Θ способна находиться в одном *состоянии* из конечного числа внутренних состояний, совокупность которых $Q = \{q_0, q_1, \dots, q_m\}$. Среди состояний выделяются два — *начальное* q_1 и *заключительное* (или *состояние остановки*) q_0 . Находясь в состоянии q_1 , машина начинает работать. Попад в состояние q_0 , машина останавливается.

Работа машины Θ определяется *программой* (*функциональной схемой*). Программа состоит из команд. Каждая команда $T(i, j)$ ($i = 1, 2, \dots, m; j = 0, 1, \dots, n$) представляет собой выражение одного из следующих видов:

$$q_i a_j \rightarrow q_k a_l \text{ С}; \quad q_i a_j \rightarrow q_k a_l \text{ П}; \quad q_i a_j \rightarrow q_k a_l \text{ Л}, \quad (32.1)$$

где $0 \leq k \leq m; 0 \leq l \leq n$. В выражениях первого вида символ С будем часто опускать.

Как же работает машина Тьюринга? Находясь в какой-либо момент времени в незаключительном состоянии (т.е. в состоянии, отличном от q_0), машина совершает шаг, который полностью определяется ее текущим состоянием q_i и символом a_j , воспринимаемым ею в данный момент на ленте. При этом содержание шага регламентировано соответствующей командой $T(i, j): q_i a_j \rightarrow q_k a_l X$, где $X \in \{С, П, Л\}$. Шаг заключается в том, что: 1) содержимое a_j обозреваемой на ленте ячейки стирается и на его место записывается символ a_l (который может совпадать с a_j); 2) машина пере-

ходит в новое состояние q_k (оно также может совпадать с предыдущим состоянием q_i); 3) машина переходит к обозрению следующей правой ячейки от той, которая обозревалась только что, если $X = \Pi$, или к обозрению следующей левой ячейки, если $X = \Pi$, или же продолжает обозревать ту же ячейку ленты, если $X = C$.

В следующий момент времени (если $q_k \neq q_0$) машина делает шаг, регламентированный командой $T(k, l)$: $q_k a_l \rightarrow q_r a_s X$ и т.д.

Поскольку работа машины, по условию, полностью определяется ее состоянием q_i в данный момент и содержимым a_j обозреваемой в этот момент ячейки, то для каждого q_i и a_j ($i = 1, 2, \dots, m$; $j = 0, 1, \dots, n$) программа машины должна содержать одну и только одну команду, начинающуюся символами $q_i a_j$. Поэтому программа машины Тьюринга с внешним алфавитом $A = \{a_0, a_1, \dots, a_n\}$ и алфавитом внутренних состояний $Q = \{q_0, q_1, \dots, q_m\}$ содержит $m(n+1)$ команд.

Словом в алфавите A или в алфавите Q , или в алфавите $A \cup Q$ называется любая последовательность букв соответствующего алфавита. Под k -й *конфигурацией* будем понимать изображение ленты машины с информацией, сложившейся на ней к началу k -го шага (или слово в алфавите A , записанное на ленту к началу k -го шага), с указанием того, какая ячейка обозревается в этот шаг и в каком состоянии находится машина. Имеют смысл лишь конечные конфигурации, т.е. такие, в которых все ячейки ленты, за исключением, быть может, конечного числа, пусты. Конфигурация называется *заключительной*, если состояние, в котором при этом находится машина, *заключительное*.

Если выбрать какую-либо *незаклучительную* конфигурацию машины Тьюринга в качестве исходной, то работа машины будет состоять в том, чтобы последовательно (шаг за шагом) преобразовывать исходную конфигурацию в соответствии с программой машины до тех пор, пока не будет достигнута *заклучительная* конфигурация. После этого работа машины Тьюринга считается закончившейся, а результатом работы считается достигнутая *заклучительная* конфигурация.

Будем говорить, что непустое слово α в алфавите $A \setminus \{a_0\} = \{a_1, \dots, a_n\}$ воспринимается машиной в *стандартном положении*, если оно записано в последовательных ячейках ленты, все другие ячейки пусты, и машина обозревает крайнюю справа ячейку из тех, в которых записано слово α . Стандартное положение называется *начальным (заклучительным)*, если машина, воспринимающая слово в стандартном положении, находится в начальном состоянии q_1 (соответственно в состоянии остановки q_0). Наконец, будем говорить, что слово α *перерабатывается машиной в слово β* , если от слова α , воспринимаемого в начальном стандартном положении, машина после выполнения конечного числа команд приходит к слову β , воспринимаемому в положении остановки.

Применение машин Тьюринга к словам. Проиллюстрируем на примерах все введенные понятия, связанные с машинами Тьюринга.

Пример 32.1. Дана машина Тьюринга с внешним алфавитом $A = \{0, 1\}$ (здесь 0 — символ пустой ячейки), алфавитом внутренних состояний $Q = \{q_0, q_1, q_2\}$ и со следующей функциональной схемой (программой):

$$q_1 0 \rightarrow q_2 0 \text{П}; q_2 0 \rightarrow q_0 1; q_1 1 \rightarrow q_1 1 \text{П}; q_2 1 \rightarrow q_2 1 \text{П}.$$

Посмотрим, в какое слово переработает эта машина слово 101, исходя из стандартного начального положения. Будем последовательно выписывать конфигурации машины при переработке ею этого слова. Имеем стандартное начальное положение:

$$(1) \quad \begin{array}{c} q_1 \\ \hline \square \quad \square \quad 1 \quad 0 \quad 1 \quad \square \quad \square \quad \square \end{array}$$

На первом шаге действует команда: $q_1 1 \rightarrow q_1 1 \text{П}$. В результате на машине создается следующая конфигурация:

$$(2) \quad \begin{array}{c} q_1 \\ \hline \square \quad \square \quad 1 \quad 0 \quad 1 \quad 0 \quad \square \quad \square \end{array}$$

На втором шаге действует команда: $q_1 0 \rightarrow q_2 0 \text{П}$ и на машине создается конфигурация:

$$(3) \quad \begin{array}{c} q_2 \\ \hline \square \quad \square \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad \square \end{array}$$

Наконец, третий шаг обусловлен командой: $q_2 0 \rightarrow q_0 1$. В результате него создается конфигурация:

$$(4) \quad \begin{array}{c} q_0 \\ \hline \square \quad \square \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad \square \end{array}$$

Эта конфигурация является заключительной, потому что машина оказалась в состоянии остановки q_0 .

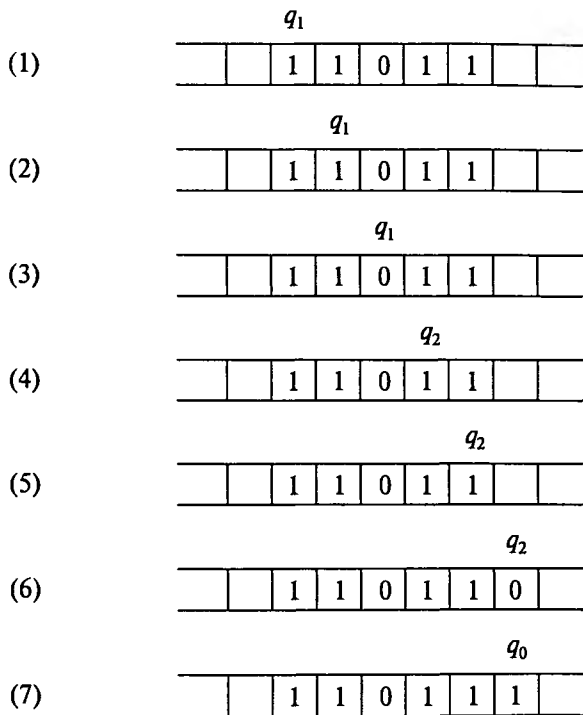
Таким образом, исходное слово 101 переработано машиной в слово 10101.

Полученную последовательность конфигураций можно записать более коротким способом. Конфигурация (1) записывается в виде следующего слова в алфавите $A \cup Q$: 10 q_1 1 (содержимое обозреваемой ячейки записано справа от состояния, в котором находится в данный момент машина). Далее, конфигурация (2) за-

писывается так: $101q_10$, конфигурация (3) — $1010q_20$ и, наконец, (4) — $1010q_01$. Вся последовательность записывается так:

$$10q_11 \Rightarrow 101q_10 \Rightarrow 1010q_20 \Rightarrow 1010q_01.$$

Приведем последовательность конфигураций при переработке этой машиной слова 11011 , исходя из начального положения, при котором в состоянии q_1 обзревается крайняя левая ячейка, в которой содержится символ этого слова (самостоятельно проанализируйте каждый шаг работы машины, указывая, какая команда обусловила его):



Более короткая запись этой последовательности конфигураций, т.е. процесса работы машины, будет $q_111011 \Rightarrow 1q_11011 \Rightarrow 11q_1011 \Rightarrow 110q_211 \Rightarrow 1101q_21 \Rightarrow 11011q_20 \Rightarrow 11011q_01$.

Таким образом, слово 11011 переработано машиной в слово 110111 .

Пример 32.2. Машина Тьюринга задается внешним алфавитом $A = \{0, 1, *\}$ (как и в предыдущем примере 0 — символ пустой ячейки), алфавитом внутренних состояний $Q = \{q_0, q_1, q_2, q_3\}$ и программой: $q_10 \rightarrow q_10Л$, $q_20 \rightarrow q_31П$, $q_30 \rightarrow q_10Л$, $q_11 \rightarrow q_20Л$, $q_21 \rightarrow q_21Л$, $q_31 \rightarrow q_31П$, $q_1* \rightarrow q_00$, $q_2* \rightarrow q_2*Л$, $q_3* \rightarrow q_3*П$.

Посмотрим, как эта машина перерабатывает некоторые слова, и постараемся обнаружить закономерность в ее работе.

Предварительно заметим, что программа машины может быть записана также в виде следующей таблицы:

$A \backslash Q$	q_1	q_2	q_3
0	$q_1 0Л$	$q_3 1П$	$q_1 0Л$
1	$q_2 0Л$	$q_2 1Л$	$q_3 1П$
*	$q_0 0$	$q_2 *Л$	$q_3 *П$

Чтобы определить по таблице, что будет делать машина, находясь, например, в состоянии q_2 и наблюдая в обозреваемой ячейке символ 1, нужно найти в таблице клетку, находящуюся на пересечении столбца q_2 и строки, содержащей 1. В этой клетке записано $q_2 1Л$. Это означает, что на следующем шаге машина останется в прежнем состоянии q_2 , сохранит содержимое обозреваемой ячейки 1 и перейдет к обозрению следующей левой ячейки на ленте.

Применим эту машину к слову $11 * 11$. Вот последовательность конфигураций, возникающих в процессе работы машины (исходная конфигурация — стандартная начальная):

$11 * 1q_1 1 \Rightarrow 11 * q_2 10 \Rightarrow 11q_2 * 10 \Rightarrow 1q_2 1 * 10 \Rightarrow q_2 11 * 10 \Rightarrow q_2 011 * 10 \Rightarrow q_3 11 * 10 \Rightarrow 11q_3 1 * 10 \Rightarrow 111q_3 * 10 \Rightarrow 111 * q_3 10 \Rightarrow 111 * 1q_3 0 \Rightarrow 111 * q_1 10 \Rightarrow 111q_2 * 00 \Rightarrow 11q_2 1 * 0 \Rightarrow 1q_2 11 * 0 \Rightarrow q_2 111 * 0 \Rightarrow q_2 0111 * 0 \Rightarrow 1q_3 111 * 0 \Rightarrow 11q_3 11 * 0 \Rightarrow 111q_3 1 * 0 \Rightarrow 1111q_3 * 0 \Rightarrow 1111 * q_3 0 \Rightarrow 1111q_1 * 0 \Rightarrow 1111q_0 0$.

Предлагается проверить самостоятельно, что данная машина Тьюринга осуществляет следующие преобразования конфигураций: $11 * q_1 1 \Rightarrow 111q_0 0$; $1 * 111q_1 1 \Rightarrow 11111q_0 0$; $11 * 11q_1 1 \Rightarrow 111111q_0 0$; $11111 * 1q_1 1 \Rightarrow 11111111q_0 0$.

Нетрудно заметить, что данная машина Тьюринга реализует операцию сложения: в результате ее работы на ленте записано подряд столько единиц, сколько их было всего записано по обе стороны от звездочки перед началом работы машины.

Этот маленький опыт работы с машинами Тьюринга позволяет сделать некоторые выводы. Так тщательно описанное устройство этой машины (разбитая на ячейки лента, считывающая головка) по существу не имеет никакого значения. Машина Тьюринга — не что иное, как некоторое правило (алгоритм) для преобразования слов алфавита $A \cup Q$, т. е. конфигураций. Таким образом, для определения машины Тьюринга нужно задать ее внешний и внутренний алфавиты, программу и указать, какие из символов обозначают пустую ячейку и заключительное состояние.

Конструирование машин Тьюринга. Создание (синтез) машин Тьюринга (т. е. написание соответствующих программ) является

задачей значительно более сложной, нежели процесс применения данной машины к данным словам.

Пример 32.3. Попытаемся построить такую машину Тьюринга, которая из n записанных подряд единиц оставляла бы на ленте $n-2$ единицы, также записанные подряд, если $n \geq 2$, и работала бы вечно, если $n = 0$ или $n = 1$.

В качестве внешнего алфавита возьмем двухэлементное множество $A = \{0, 1\}$. Количество необходимых внутренних состояний будет определено в процессе составления программы. Считаем, что машина начинает работать из стандартного начального положения, т. е. когда в состоянии q_1 обозревается крайняя правая единица из n записанных на ленте.

Начнем с того, что сотрем первую единицу, если она имеется, перейдем к обозрению следующей левой ячейки и сотрем там единицу, если она в этой ячейке записана. На каждом таком переходе машина должна переходить в новое внутреннее состояние, ибо в противном случае будут стерты вообще все единицы, записанные подряд. Вот команды, осуществляющие описанные действия:

$$q_1 1 \rightarrow q_2 0Л; q_2 1 \rightarrow q_3 0Л.$$

Машина находится в состоянии q_3 и обозревает третью справа ячейку из тех, в которых записано данное слово (n единиц). Не меняя содержимого обозреваемой ячейки, машина должна остановиться, т. е. перейти в заключительное состояние q_0 , независимо от содержимого ячейки. Вот эти команды:

$$q_3 0 \rightarrow q_0 0; q_3 1 \rightarrow q_0 1.$$

Теперь остается рассмотреть ситуации, когда на ленте записана всего одна единица или не записано ни одной. Если на ленте записана одна единица, то после первого шага (выполнив команду $q_1 1 \rightarrow q_2 0Л$) машина будет находиться в состоянии q_2 и будет обозревать вторую справа ячейку, в которой записан 0. По условию, в таком случае машина должна работать вечно. Это можно обеспечить, например, такой командой:

$$q_2 0 \rightarrow q_2 0П,$$

выполняя которую шаг за шагом, машина будет двигаться по ленте неограниченно вправо (или протягивать ленту через считывающую головку справа налево). Наконец, если на ленте не записано ни одной единицы, то машина, по условию, также должна работать вечно. В этом случае в начальном состоянии q_1 обозревается ячейка с содержимым 0, и вечная работа машины обеспечивается следующей командой:

$$q_1 0 \rightarrow q_1 0П.$$

Запишем составленную программу (функциональную схему) построенной машины Тьюринга в виде таблицы:

$A \backslash Q$	q_1	q_2	q_3
0	$q_1 0П$	$q_2 0П$	$q_0 0$
1	$q_0 0Л$	$q_2 0Л$	$q_0 1$

В заключение отметим следующее. Созданная нами машина Тьюринга может применяться не только к словам в алфавите $A = \{0, 1\}$, представляющим собой записанные подряд n единиц ($n \geq 2$). Она применима и ко многим другим словам в этом алфавите, например (проверьте самостоятельно) к словам: 1011, 10011, 111011, 11011, 1100111, 1001111, 10111, 10110111, 10010111 и т.д. (исходя из стандартного начального положения). С другой стороны, построенная машина не применима (т.е. при подаче этих слов на вход машины она работает вечно) не только к слову «1» или к слову, состоящему из одних нулей. Она не применима и к следующим словам (проверьте самостоятельно): 101, 1001, 11101, 101101, 1100101101 и т.д.

Вычислимые по Тьюрингу функции. *Определение 32.4.* Функция называется *вычислимой по Тьюрингу*, если существует машина Тьюринга, вычисляющая ее, т.е. такая машина Тьюринга, которая вычисляет ее значения для тех наборов значений аргументов, для которых функция определена, и работающая вечно, если функция для данного набора значений аргументов не определена.

Остается договориться о некоторых условностях для того, чтобы это определение стало до конца точным. Во-первых, напомним, что речь идет о функциях (или возможно о частичных функциях, т.е. не всюду определенных), заданных на множестве натуральных чисел и принимающих также натуральные значения. Во-вторых, нужно условиться, как записывать на ленте машины Тьюринга значения $x_1, x_2, \dots, x_n$ аргументов функции $f(x_1, x_2, \dots, x_n)$, из какого положения начинать переработку исходного слова и, наконец, в каком положении получать значение функции. Это можно делать, например, следующим образом. Значения $x_1, x_2, \dots, x_n$ аргументов будем располагать на ленте в виде следующего слова:

$$0 \underbrace{1 \dots 1}_{x_1} 0 \underbrace{1 \dots 1}_{x_2} 0 \dots 0 \underbrace{1 \dots 1}_{x_n} 0.$$

Здесь полезно ввести следующие обозначения. Для натурального x обозначаем:

$$1^x = \underbrace{1 \dots 1}_x, \quad 0^x = \underbrace{0 \dots 0}_x.$$

Дополнительно полагаем $0^0 = 1^0 = \Lambda$ — пустое слово. Так что на слова $1^0 = \Lambda$, $1^1 = 1$, $1^2 = 11$, $1^3 = 111$, ... будем смотреть как на «изображения» натуральных чисел 0, 1, 2, 3, ... соответственно.

Таким образом, предыдущее слово можно представить следующим образом: $01^*01^*0 \dots 01^*0$. Далее, начинать переработку данного слова будем из стандартного начального положения, т.е. из положения, при котором в состоянии q_1 обозревается крайняя правая единица записанного слова. Если функция $f(x_1, x_2, \dots, x_n)$ определена на данном наборе значений аргументов, то в результате на ленте должно быть записано подряд $f(x_1, x_2, \dots, x_n)$ единиц; в противном случае машина должна работать бесконечно. При выполнении всех перечисленных условий будем говорить, что *машина Тьюринга вычисляет данную функцию*. Таким образом, сформулированное определение 35.4 становится абсолютно строгим.

Обратимся к примерам. Нетрудно понять, что машина Тьюринга из примера 32.2 по существу вычисляет функцию $f(x) = x + 1$, а машина Тьюринга из примера 32.3 вычисляет функцию $f(x) = x - 2$.

Пример 32.5. Построим машину Тьюринга, вычисляющую функцию $f(x) = x/2$. Эта функция не всюду определена: областью ее определения является лишь множество всех четных чисел. Поэтому, учитывая определение 32.4, нужно сконструировать такую машину Тьюринга, которая при подаче на ее вход четного числа давала бы на выходе половину этого числа, а при подаче нечетного — работала бы неограниченно долго.

Сконструировать машину Тьюринга — значит написать (составить) ее программу. В этом процессе два этапа: сначала *создается алгоритм вычисления значений функции*, а затем *он записывается на языке машины Тьюринга (программируется)*.

В качестве внешнего алфавита возьмем двухэлементное множество $A = \{0, 1\}$. В этом алфавите натуральное число x изображается словом $11 \dots 1$, состоящим из x единиц, которое на ленте машины Тьюринга записывается в виде x единиц, стоящих в ячейках подряд. Работа машины начинается из стандартного начального положения: $01 \dots 1q_110$ (число единиц равно x).

Сделаем начало вычислительного процесса таким: машина обозревает ячейки, двигаясь справа налево, и каждую вторую единицу превращает в 0. Такое начало обеспечивается следующими командами:

- (1): $q_11 \rightarrow q_21L$;
- (2): $q_21 \rightarrow q_10L$;
- (3): $q_20 \rightarrow q_20L$.

Если число x единиц нечетно, то машина продолжит движение по ленте влево неограниченно, т.е. будет работать бесконечно. Если же число x единиц четно, то в результате выполнения команд создается конфигурация $q_10010101 \dots 01010$, в которой число единиц равно $x/2$. Остается сдвинуть единицы так, чтобы между ними не стояли нули. Для осуществления этой процедуры предлагается следующий алгоритм. Будем двигаться по ленте вправо, ничего на ней

не меняя, до первой единицы и перейдем за единицу. Передвижение осуществляется с помощью следующих команд:

(4): $q_10 \rightarrow q_30П$;

(5): $q_30 \rightarrow q_30П$;

(6): $q_31 \rightarrow q_41П$.

В результате их выполнения получим конфигурацию

$001q_4010101 \dots 010100$. (*)

Заменяем 0, перед которым остановились, на 1 и продвинемся вправо до ближайшего 0:

(7): $q_40 \rightarrow q_51П$;

(8): $q_51 \rightarrow q_51П$.

Получим конфигурацию $00111q_50101 \dots 010100$, в которой правее обозреваемой ячейки записаны «пары» 01, ..., 01. Кроме того, на ленте одна единица записана лишняя. Продвинемся по ленте вправо до последней «пары» 01. Это можно сделать с помощью своеобразного цикла:

(9): $q_50 \rightarrow q_60П$;

(10): $q_61 \rightarrow q_51П$.

Получим конфигурацию $001110101 \dots 01010q_600$. Двигаться дальше вправо бессмысленно. Вернемся на две ячейки назад и заменим единицу из последней «пары» 01 на ноль:

(11): $q_60 \rightarrow q_70Л$;

(12): $q_70 \rightarrow q_70Л$;

(13): $q_71 \rightarrow q_80Л$.

Получим конфигурацию $001110101 \dots 01q_800$. Число единиц на ленте снова равно $x/2$. Продвинемся влево на одну ячейку с помощью команды

(14): $q_80 \rightarrow q_90Л$.

В результате чего получим конфигурацию $001110101 \dots 010q_9100$. Теперь уничтожим самую правую единицу и продвинемся по ленте влево до следующей единицы:

(15): $q_91 \rightarrow q_{10}0Л$;

(16): $q_{10}0 \rightarrow q_{10}0Л$.

Получим конфигурацию

$001110101 \dots 0q_{10}100$, (**)

в которой левее обозреваемой ячейки записана серия пар 10, 10, ..., 10 (если читать справа налево). Теперь на ленте недостает одной единицы, т.е. число единиц равно $(x/2) - 1$. Продвинемся по ленте влево до последней «пары» 10. Это можно сделать с помощью цикла

(17): $q_{10}1 \rightarrow q_{11}1Л$;

(18): $q_{11}0 \rightarrow q_{10}0Л$,

выполнив который, придем к следующей конфигурации: $001q_{11}110101 \dots 0100$. Вернемся вправо к ближайшему нулю и превратим его в единицу:

(19): $q_{11}1 \rightarrow q_{12}1П$;

(20): $q_{12}1 \rightarrow q_{12}1П$;

(21): $q_{12}0 \rightarrow q_{13}1П$.

Получим конфигурацию $001111q_{13}101 \dots 0100$, в которой число единиц снова равно $x/2$.

Если теперь перешагнем вправо по ленте через обозреваемую единицу и переведем машину в состояние q_4 с помощью команды

(22): $q_{13}1 \rightarrow q_41П$,

то придем к следующей конфигурации: $0011111q_401 \dots 0100$, которая по существу аналогична конфигурации (*). В результате программа закичивается (становится циклической): снова ближайший 0 превращается в 1, а самая правая 1 — в 0, затем машина возвращается к самому левому нулю, оказываясь в начале следующего цикла, и т.д.

Как же завершается работа программы? В некоторый момент конфигурация будет иметь вид $00111 \dots 1110q_{10}100$. Выполнив команды (17), (18), придем к конфигурации $00111 \dots 1q_{11}110100$. Далее выполняются команды (19), (20), (21), что приводит к конфигурации: $00111 \dots 111111q_{13}00$. Остается остановить машину. Это делается с помощью команды

(23): $q_{13}0 \rightarrow q_00Л$.

Заключительная конфигурация имеет вид: $00111 \dots 1111q_0100$.

Запишем программу машины Тьюринга в табличной форме:

$Q \backslash A$	0	1
q_1	$q_30П$	$q_21Л$
q_2	$q_20Л$	$q_10Л$
q_3	$q_30П$	$q_41П$
q_4	$q_51П$	
q_5	$q_60П$	$q_51П$
q_6	$q_70Л$	$q_51П$
q_7	$q_70Л$	$q_80Л$
q_8	$q_90Л$	$q_71Л$
q_9		$q_{10}0Л$
q_{10}	$q_{10}0Л$	$q_{11}1Л$
q_{11}	$q_{10}0Л$	$q_{12}1П$
q_{12}	$q_{13}1П$	$q_{13}1П$
q_{13}	$q_00Л$	$q_41П$

Предлагается самостоятельно проследить за работой этой машины Тьюринга, взяв в качестве исходных конкретные слова: 111, 1111, 111111, 1111111111.

Правильная вычислимость функций на машине Тьюринга. В предыдущем пункте мы рассмотрели вопрос о том, что значит и каким образом «данная машина Тьюринга вычисляет функцию

$f(x_1, x_2, \dots, x_n)$ ». Для этого нужно, чтобы каждое из чисел $x_1, x_2, \dots, x_n$ было записано на ленту машины непрерывным массивом из соответствующего числа единиц, а сами массивы были разделены символом 0. Если функция $f(x_1, x_2, \dots, x_n)$ определена на данном наборе значений аргументов, то в результате на ленте должно быть записано подряд $f(x_1, x_2, \dots, x_n)$ единиц. При этом мы не очень строго относимся к тому, в каком начальном положении машина начинает работать (часто это было стандартное начальное положение), в каком завершает работу и как эта работа протекает.

В дальнейшем нам понадобится более сильное понятие вычислимости функции на машине Тьюринга — понятие правильной вычислимости.

Определение 32.6. Будем говорить, что машина Тьюринга *правильно вычисляет* функцию $f(x_1, x_2, \dots, x_n)$, если начальное слово $q_1 0 1^{x_1} 0 1^{x_2} 0 \dots 0 1^{x_n} 0$ она переводит в слово $q_0 0 1^{f(x_1, x_2, \dots, x_n)} 0 \dots 0$ и при этом в процессе работы не пристраивает к начальному слову новых ячеек на ленте ни слева, ни справа. Если же функция f не определена на данном наборе значений аргументов, то, начав работать из указанного положения, она никогда в процессе работы не будет надстраивать ленту слева.

Пример 32.7. Приведем программы машин Тьюринга, правильно вычисляющих функции $S(x) = x + 1$ и $O(x) = 0$. Функция $S(x) = x + 1$ осуществляет перевод: $q_1 0 1^x 0 \Rightarrow q_0 0 1^{x+1}$. Ее программа: $q_1 0 \rightarrow q_2 \Pi$, $q_2 1 \rightarrow q_2 \Pi$, $q_2 0 \rightarrow q_3 1$, $q_3 1 \rightarrow q_3 \Pi$, $q_3 0 \rightarrow q_0 0$. Функция $O(x) = 0$ осуществляет перевод: $q_1 0 1^x 0 \Rightarrow q_0 0 0^{x+1}$. Ее программа: $q_1 0 \rightarrow q_2 0 \Pi$, $q_2 1 \rightarrow q_2 \Pi$, $q_2 0 \rightarrow q_3 0 \Pi$, $q_3 1 \rightarrow q_4 0$, $q_4 0 \rightarrow q_3 0 \Pi$, $q_3 0 \rightarrow q_0 0$. Соответствующую машину Тьюринга обозначили O .

В Задачнике (№ 12.24) разобрана работа машины A , называемой «перенос нуля», которая осуществляет перевод слова $0 0 1^x 0$ в слово $0 1^x 0 0$. Причем как в начальном, так и в заключительном состоянии обозревается первая левая ячейка с нулем.

Пример 32.8. Построить две машины «левый сдвиг» B^- и «правый сдвиг» B^+ . Первая из начального стандартного положения перерабатывает слово $0 1^x 0$ в то же самое слово и останавливается, обозревая самую левую ячейку с нулем. Вторая машина из начального состояния, в котором обозревается левая ячейка с нулем, слово $0 1^x 0$ перерабатывает в то же самое слово и останавливается, обозревая самую правую ячейку с нулем.

Программа машины B^- : $q_1 0 \rightarrow q_2 0 \Pi$, $q_2 1 \rightarrow q_2 \Pi$, $q_2 0 \rightarrow q_0 0$. Ясно, что программа машины B^+ получается из программы предыдущей машины заменой символа « Π » символом « Π ».

В задаче № 12.27 Задачника требуется построить машину (называемую «транспозицией» и обозначаемую B), осуществляющую переход $0 1^x q_1 0 1^y 0 \Rightarrow 0 1^y q_0 1^x 0$.

Композиция машин Тьюринга. Определение 32.9. Пусть заданы машины Тьюринга Θ_1 и Θ_2 , имеющие общий внешний алфавит $\{a_0, a_1, \dots, a_m\}$ и алфавиты внутренних состояний $\{q_0, q_1, \dots, q_n\}$ и $\{q_0, q'_1, \dots, q'_t\}$ соответственно. *Композицией* (или *произведением*) машины Θ_1 на машину Θ_2 называется новая машина Θ с тем же внешним алфавитом $\{a_0, a_1, \dots, a_m\}$, внутренним алфавитом $\{q_0, q_1, \dots, q_n, q_{n+1}, \dots, q_{n+t}\}$ и программой, получающейся следующим образом. Во всех командах из Θ_1 , содержащих символ остановки q_0 , заменяем последний на q_{n+1} . Все остальные символы в командах из Θ_1 остаются неизменными. В командах из Θ_2 символ q_0 оставляем неизменным, а все остальные состояния $q'_i (i = 1, \dots, t)$ заменяем соответственно на q_{n+i} . Совокупность всех так полученных команд образует программу машины-композиции Θ .

Введенное понятие является удобным инструментом для конструирования машин Тьюринга. Покажем это на примере.

Пример 32.10. Сконструируем машины Тьюринга, правильно вычисляющие функции-проекторы $I_m^n(x_1, x_2, \dots, x_n) = x_m (1 \leq m \leq n)$.

Рассмотрим сначала конкретный случай $n = 3, m = 2$, т.е. функцию $I_2^3(x_1, x_2, x_3) = x_2$. Мы должны переработать слово $q_1 01^x 01^x 01^x 0$ в слово $q_0 01^x 0$. Будем применять к начальной конфигурации последовательно сконструированные ранее машины Тьюринга B^+, B, B^- , О:

	$q_1 01^x 01^x 01^x 0;$
$B^+:$	$01^x q 01^x 01^x 0;$
$B:$	$01^x q 01^x 01^x 0;$
$B^+:$	$01^x 01^x q 01^x 0;$
$O:$	$01^x 01^x q 00^x 0;$
$B^-:$	$01^x q 01^x 00^x 0;$
$O:$	$01^x q 00^x 00^x 0;$
$B^-:$	$q 01^x 00^x 00^x 0.$

Таким образом, функция $I_2^3(x_1, x_2, x_3) = x_2$ вычисляется следующей композицией машин: $B^+ B B^+ O B^- O B^- = B^+ B B^+ (O B^-)^2$.

Проверьте самостоятельно, что функция $I_2^2(x_1, x_2) = x_2$ вычисляется композицией $B^+ B O B^-$.

Теперь мы можем представить себе алгоритм построения композиции машин B^+, B, B^-, O для вычисления любой функции вида $I_m^n(x_1, x_2, \dots, x_n) = x_m$. С помощью правого сдвига B^+ , применив его $m-1$ раз, нужно сначала достичь массива $01^x m$:

$(B^+)^{m-1}: \quad 01^x 0 \dots q 01^x 0 \dots 01^x 0.$

Затем, двигаясь влево, транспонировать (с помощью B) массив $01^x m$ с каждым соседним слева массивом, пока массив $01^x m$ не выйдет на первое место:

$(B \cdot B^-)^{m-1}: \quad q 01^x 0 01^x 0 \dots 01^x m-1 01^x m+1 0 \dots 01^x 0.$

Теперь нужно дойти до крайнего правого массива с помощью $(n-1)$ -кратного применения правого сдвига B^+ :

$$(B^+)^{n-1}: \quad 01^{x_n}01^{x_1}0 \dots 01^{x_{n-1}}01^{x_{n+1}}0 \dots q01^{x_n}0.$$

Наконец, нужно стирать последовательно справа налево все массивы единиц, кроме первого:

$$(OB^-)^{n-1}: \quad q01^{x_n}00^{x_1}0 \dots 00^{x_{n-1}}00^{x_{n+1}}0 \dots 00^{x_n}0.$$

Итак, данную функцию (правильно) вычисляет следующая машина Тьюринга: $(B^+)^{m-1}(B^- \cdot B^-)^{m-1}(B^+)^{n-1}(O^- \cdot B^-)^{n-1}$.

При $n = 3$, $m = 2$ эта машина имеет вид:

$$B^+BB^-(B^+)^2(OB^-)^2 = B^+BB^+(OB^-)^2,$$

т.е. совпадает с построенной выше машиной. При $n = 2$, $m = 2$ эта машина имеет вид: $B^+(BB^-)B^+(OB^-) = B^+VOB^-$, т.е. также совпадает с соответствующей рассмотренной выше машиной Тьюринга.

В задаче № 12.29 Задачника подробно разобрана работа машины Тьюринга, являющейся композицией машин BB^-B , рассмотренных ранее. Эта машина называется «циклический сдвиг» и обозначается Ц. Слово $01^x01^yq_101^z0$ она переводит в слово $01^zq_001^x01^y0$. При этом нужно помнить, что машины в композиции BB^-B работают в очередности справа налево: сначала правая B , затем B^- и, наконец, левая B .

В задаче № 17.30 Задачника предлагается проверить, что машина Тьюринга, являющаяся следующей композицией $K_2 = B^+GBB^+BBB^+BB^-B^-BB^+$ (называется «копирование»), перерабатывает слово $q_101^x01^y$ в слово $01^x01^yq_001^x01^y$. (G — машина удвоения, см. задачу № 12.28 в Задачнике.)

Тезис Тьюринга (основная гипотеза теории алгоритмов). Вернемся к интуитивному представлению об алгоритмах (см. § 31). Напомним, одно из свойств алгоритма заключается в том, что он представляет собой единый способ, позволяющий для каждой задачи из некоего бесконечного множества задач за конечное число шагов найти ее решение.

На понятие алгоритма можно взглянуть и с несколько иной точки зрения. Каждую задачу из бесконечного множества задач можно выразить (закодировать) некоторым словом некоторого алфавита, а решение задачи — каким-то другим словом того же алфавита. В результате получим функцию, заданную на некотором подмножестве множества всех слов выбранного алфавита и принимающую значения в множестве всех слов того же алфавита. Решить какую-либо задачу — значит найти значение этой функции на слове, кодирующем данную задачу. А иметь алгоритм для решения всех задач данного класса — значит иметь единый способ, позволяющий в конечное число шагов «вычислять» значения построенной функ-

ции для любых значений аргумента из ее области определения. Таким образом, алгоритмическая проблема — по существу, проблема о вычислении значений функции, заданной в некотором алфавите.

Остается уточнить, что значит уметь вычислять значения функции. Это значит вычислять значения функции с помощью подходящей машины Тьюринга. Для каких же функций возможно их тьюрингово вычисление? Многочисленные исследования ученых, обширный опыт показали, что такой класс функций чрезвычайно широк. Каждая функция, для вычисления значений которой существует какой-нибудь алгоритм, оказывалась вычислимой посредством некоторой машины Тьюринга. Это дало повод Тьюрингу высказать следующую гипотезу, называемую основной гипотезой теории алгоритмов, или **тезисом Тьюринга**:

Для нахождения значений функции, заданной в некотором алфавите, тогда и только тогда существует какой-нибудь алгоритм, когда функция является вычислимой по Тьюрингу, т. е. когда она может вычисляться на подходящей машине Тьюринга.

Это означает, что строго математическое понятие вычислимой (по Тьюрингу) функции является по существу идеальной моделью взятого из опыта понятия алгоритма. Данный тезис есть не что иное, как аксиома, постулат, выдвигаемый нами, о взаимосвязях нашего опыта с той математической теорией, которую мы под этот опыт хотим подвести. Конечно же данный тезис в принципе не может быть доказан методами математики, потому что он не имеет внутриматематического характера (одна сторона в тезисе — понятие алгоритма — не является точным математическим понятием). Он выдвинут исходя из опыта, и именно опыт подтверждает его состоятельность. Точно так же, например, не могут быть доказаны и математические законы механики; они открыты Ньютоном и многократно подтверждены опытом.

Впрочем, не исключается принципиальная возможность того, что тезис Тьюринга будет опровергнут. Для этого должна быть указана функция, которая вычислима с помощью какого-нибудь алгоритма, но невычислима ни на какой машине Тьюринга. Но такая возможность представляется маловероятной (в этом одно из значений гипотезы): всякий алгоритм, который будет открыт, может быть реализован на машине Тьюринга.

Дополнительные косвенные доводы в подтверждение этой гипотезы будут приведены в двух последующих параграфах, где рассматриваются другие формализации интуитивного понятия алгоритма и доказываются их равносильность с понятием машины Тьюринга.

Машины Тьюринга и современные электронно-вычислительные машины. Изучение машин Тьюринга и практика составления программ для них закладывают фундамент алгоритмического мышления, сущность которого состоит в том, что нужно уметь разделять тот или иной процесс вычисления или какой-либо другой дея-

тельности на простые составляющие шаги. В машине Тьюринга расчленение (анализ) вычислительного процесса на простейшие операции доведено до предельной возможности: распознавание единичного рассмотренного вхождения символа, перемещение точки наблюдения данного ряда символов в соседнюю точку и изменение имеющейся в памяти информации. Конечно, такое мелкое дробление вычислительного процесса, реализуемого в машине Тьюринга, значительно его удлинит. Но вместе с тем логическая структура процесса, расчлененного, образно выражаясь, до атомарного состояния, значительно упрощается и предстает в некотором стандартном виде, весьма удобном для теоретических исследований. (Именно такое расчленение на простейшие составляющие вычислительного процесса на машине Тьюринга дает еще один косвенный аргумент в пользу тезиса Тьюринга, обсуждавшегося в предыдущем пункте: всякая функция, вычисляемая с помощью какого-либо алгоритма, может быть вычислена на машине Тьюринга, потому что каждый шаг данного алгоритма можно расчленить на еще более мелкие операции, которые реализуются в машине Тьюринга.) Таким образом, понятие машины Тьюринга есть теоретический инструмент анализа алгоритмического процесса, а значит, анализа существа алгоритмического мышления.

В современных ЭВМ алгоритмический процесс расчленен не на столь мелкие составляющие, как в машинах Тьюринга. Наоборот, создатели ЭВМ стремятся к известному укрупнению выполняемых машиной процедур (на этом пути, конечно, есть свои ограничения). Так, для выполнения операции сложения на машине Тьюринга составляется целая программа, а в современной ЭВМ такая операция является простейшей.

Далее, машина Тьюринга обладает бесконечной внешней памятью (неограниченная в обе стороны лента, разбитая на ячейки). Но ни в одной реально существующей машине бесконечной памяти быть не может. Это говорит о том, что машины Тьюринга отображают потенциальную возможность неограниченного увеличения объема памяти современных ЭВМ.

Наконец, можно провести более подробный сравнительный анализ работы современной ЭВМ и машины Тьюринга. В большинстве ЭВМ принята трехадресная система команд, обусловленная необходимостью выполнения бинарных операций, в которых участвует содержимое сразу трех ячеек памяти. Например, число из ячейки a умножается на число из ячейки b , и результат отправляется в ячейку c . Существуют ЭВМ двухадресные и одноадресные. Так, одноадресная ЭВМ работает следующим образом: вызывается (в сумматор) число из ячейки a ; в сумматоре происходит, например, умножение этого числа на число из ячейки b ; результат отправляется из сумматора в ячейку c . Машину Тьюрин-

га можно считать одноадресной машиной, в которой система одноадресных команд упрощена еще больше: на каждом шаге работы машины команда предписывает замену лишь единственного знака, хранящегося в обозреваемой ячейке, а адрес обозреваемой ячейки при переходе к следующему такту может меняться лишь на единицу (обозрение соседней справа или слева ячейки ленты) или не меняться вовсе. Это удлиняет процесс, но в то же время резко унифицирует его, делает стандартным.

Подводя итоги, можно сказать, что современные ЭВМ есть некие реальные физические модели машин Тьюринга, огрубленные с точки зрения теории, но созданные в целях реализации конкретных вычислительных процессов. В свою очередь, понятие машины Тьюринга и теория таких машин есть теоретический фундамент и обоснование современных ЭВМ.

§ 33. Рекурсивные функции

Понятие машины Тьюринга — не единственный известный путь уточнения понятия алгоритма. В настоящем и следующем параграфах будут рассмотрены еще два способа такого уточнения: рекурсивные функции и нормальные алгоритмы Маркова.

Происхождение рекурсивных функций. Всякий алгоритм однозначно сопоставляет допустимым начальным данным результат. Это означает, что с каждым алгоритмом однозначно связана функция, которую он вычисляет. В предыдущем параграфе были рассмотрены примеры функций, которые вычисляются с помощью алгоритма, названного машиной Тьюринга. Возникает естественный вопрос, для всякой ли функции существует вычисляющий ее алгоритм. Учитывая сформулированный в § 32 тезис Тьюринга, утверждающий, что функция вычислима с помощью какого-нибудь алгоритма тогда и только тогда, когда она вычислима с помощью машины Тьюринга, данный вопрос трансформируется в следующий. Для всякой ли функции можно указать вычисляющую ее машину Тьюринга? Если нет, то для каких функций существует вычисляющий их алгоритм (машина Тьюринга), как описать такие, как говорят, алгоритмически или эффективно вычисляемые функции?

Исследование этих вопросов привело к созданию в 1930-х гг. теории рекурсивных функций. При этом класс вычислимых функций (названных здесь рекурсивными) получил такое описание, которое весьма напомнило процесс построения аксиоматической теории на базе некоторой системы аксиом. Сначала были выбраны простейшие функции, эффективная вычисляемость которых была очевидна (своего рода «аксиомы»). Затем сформулированы некоторые правила (названные операторами), на основе которых можно строить новые функции из уже имеющихся (своего рода

«правила вывода»). Тогда требуемым классом функций будет совокупность всех функций, получающихся из простейших с помощью выбранных операторов. Наша цель будет состоять в том, чтобы доказать, что этот класс функций совпадает с классом функций, вычислимых с помощью машин Тьюринга.

Идея доказательства этого утверждения в одну сторону проста: сначала доказать вычислимость по Тьюрингу простейших функций, а затем вычислимость по Тьюрингу функций, получающихся из вычислимых по Тьюрингу функций с помощью выбранных операторов.

Основные понятия теории рекурсивных функций и тезис Чёрча. Приступим к построению класса рекурсивных функций в соответствии с изложенными принципами. Напомним, что рассматриваются функции, заданные на множестве натуральных чисел и принимающие натуральные значения. Функции предполагается брать частичные, т.е. определенные, вообще говоря, не для всех значений аргументов. В качестве исходных простейших функций выберем следующие:

$S(x) = x + 1$ (функция следования);

$O(x) = 0$ (нуль-функция);

$I_m^n(x_1, x_2, \dots, x_n) = x_m$ (функции-проекторы, $1 \leq m \leq n$).

Вычислимость (более того, правильная вычислимость) этих функций с помощью машины Тьюринга установлена в примерах 32.7 и 32.10.

Далее, в качестве операторов, с помощью которых будут строиться новые функции, выберем следующие три: операторы суперпозиции, примитивной рекурсии и минимизации.

Определение 33.1 (оператор суперпозиции). Будем говорить, что n -местная функция φ получена из m -местной функции f и n -местных функций $g_1, \dots, g_m$ с помощью *оператора суперпозиции*, если для всех $x_1, \dots, x_n$ справедливо равенство:

$$\varphi(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)).$$

Понятие суперпозиции функций и сложной функции хорошо известно, но нас сейчас этот оператор интересует с точки зрения его взаимоотношений с процессом вычислимости функций с помощью машин Тьюринга.

Теорема 33.2. Если функции $f(x_1, \dots, x_m), g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)$ правильно вычислимы по Тьюрингу, то правильно вычислима и сложная функция (суперпозиция функций):

$$\varphi(x_1, \dots, x_n) = f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)).$$

Доказательство. Руководствуясь определением 32.9 композиции машин Тьюринга, нетрудно понять, что если машина F правильно вычисляет функцию $f(y)$, а машина G правильно вы-

числяет функцию $g(x)$, то композиция этих машин $F \cdot G$ правильно вычисляет суперпозицию этих функций $f(g(x))$:

$$\begin{aligned} G: & q_1 0 1^x; \\ & q 0 1^{g(x)}; \\ F: & q 0 1^{f(g(x))}. \end{aligned}$$

Рассмотрим более сложную суперпозицию вычислимых функций: $\varphi(x, y) = f(g_1(x, y), g_2(x, y))$. Пусть машины F, G_1, G_2 правильно вычисляют функции f, g_1, g_2 соответственно. Сконструируем машину Тьюринга, правильно вычисляющую сложную функцию $\varphi(x, y)$, пользуясь введенными в § 32 машинами сдвига, транспозиции, копирования и нулевой функции:

$$\begin{aligned} K_2: & q_1 0 1^x 0 1^y; \\ G_1: & 0 1^x 0 1^y q 0 1^{g_1(x, y)}; \\ Ц: & 0 1^{g_1(x, y)} q 0 1^x 0 1^y; \\ G_2: & 0 1^{g_1(x, y)} q 0 1^{g_2(x, y)}; \\ Б^-: & q 0 1^{g_1(x, y)} 0 1^{g_2(x, y)}; \\ F: & q 0 1^{f(g_1(x, y), g_2(x, y))}; \\ q 0 \rightarrow q_0: & q_0 0 1^{f(g_1, g_2)}. \end{aligned}$$

Сконструируйте самостоятельно композицию машин, правильно вычисляющих функцию $\varphi(x, y) = f(g_1(x, y), g_2(x, y), g_3(x, y))$.

Подстановки указанного вида достаточно специфичны (все функции g имеют одно и то же число аргументов) и не исчерпывают всевозможных подстановок, которые можно производить над функциями. Но благодаря функциям-проекторам I_m^n этот недостаток легко устраняется: любая суперпозиция функций в функции может быть выражена через суперпозиции указанного вида и функции-проекторы. В самом деле, например, суперпозиция $f(g_1(x_1, x_2), g_2(x_1))$ может быть в требуемом виде представлена так: $f(g_1(x_1, x_2), I_1^2(g_2(x_1), g_3(x_1)))$, где $g_3(x_1)$ — любая функция от x_1 . В свою очередь, используя подстановку и функции-проекторы, можно переставлять аргументы в функции:

$$\begin{aligned} f(x_2, x_1, x_3, \dots, x_n) &= f(I_2^2(x_1, x_2), I_1^2(x_1, x_2), x_3, \dots, x_n); \\ f(x_1, x_1, x_3, \dots, x_n) &= f(I_1^2(x_1, x_2), I_1^2(x_1, x_2), x_3, \dots, x_n). \end{aligned}$$

Поэтому можно считать, что теорема полностью доказана. $\square$

Определение 33.3. Говорят, что $(n+1)$ -местная функция φ получена из n -местной функции f и $(n+2)$ -местной функции g с помощью оператора примитивной рекурсии, если для любых $x_1, \dots, x_n, y$ справедливы равенства:

$$\begin{aligned} \varphi(x_1, \dots, x_n, 0) &= f(x_1, \dots, x_n); \\ \varphi(x_1, \dots, x_n, y+1) &= g(x_1, \dots, x_n, y, \varphi(x_1, \dots, x_n, y)). \end{aligned}$$

Пара этих равенств называется *схемой примитивной рекурсии*.

Здесь важно отметить то, что, независимо от числа аргументов в φ , рекурсия ведется только по одной переменной y ; остальные n переменных $x_1, \dots, x_n$ на момент применения схемы примитивной рекурсии зафиксированы и играют роль параметров. Кроме того, схема примитивной рекурсии выражает каждое значение определяемой функции φ не только через данные функции f и g , но и через так называемые предыдущие значения определяемой функции φ : прежде чем получить значение $\varphi(x_1, \dots, x_n, k)$, придется проделать $k + 1$ вычисление по указанной схеме — для $y = 0, 1, \dots, k$.

Определение 33.4. Функция называется *примитивно рекурсивной*, если она может быть получена из простейших функций O, S, I_m^n с помощью конечного числа применений операторов суперпозиции и примитивной рекурсии.

Наконец, введем заключительный, третий, оператор.

Определение 33.5 (оператор минимизации). Будем говорить, что n -местная функция φ получается из $(n + 1)$ -местных функций f_1 и f_2 с помощью *оператора минимизации*, или оператора наименьшего числа, если для любых $x_1, \dots, x_n, y$ равенство $\varphi(x_1, \dots, x_n) = y$ выполнено тогда и только тогда, когда значения $f_i(x_1, \dots, x_n, 0), \dots, f_i(x_1, \dots, x_n, y - 1)$ ($i = 1, 2$) определены и попарно неравны: $f_1(x_1, \dots, x_n, 0) \neq f_2(x_1, \dots, x_n, 0), \dots, f_1(x_1, \dots, x_n, y - 1) \neq f_2(x_1, \dots, x_n, y - 1)$, а $f_1(x_1, \dots, x_n, y) = f_2(x_1, \dots, x_n, y)$.

Коротко говоря, величина $\varphi(x_1, \dots, x_n)$ равна наименьшему значению аргумента y , при котором выполняется последнее равенство. Используется следующее обозначение:

$$\varphi(x_1, \dots, x_n) = \mu y [f_1(x_1, \dots, x_n, y) = f_2(x_1, \dots, x_n, y)].$$

В частном случае может быть $f_2 = 0$. Тогда

$$\varphi(x_1, \dots, x_n) = \mu y [f(x_1, \dots, x_n, y) = 0].$$

Оператор минимизации называется также μ -оператором.

Этот оператор предназначен для порождения следующего важного класса рекурсивных функций.

Определение 33.6. Функция называется *частично рекурсивной*, если она может быть получена из простейших функций O, S, I_m^n с помощью конечного числа применений суперпозиции, примитивной рекурсии и μ -оператора. Если функция всюду определена и частично рекурсивна, то она называется *общерекурсивной*.

(Отметим, что не всегда частично рекурсивную функцию можно эффективно доопределить до общерекурсивной.)

Ясно, что всякая примитивно рекурсивная функция будет и частично рекурсивной (и даже общерекурсивной, так как каждая примитивно рекурсивная функция всюду определена), поскольку для построения частично рекурсивных функций из простейших

используется больше средств, чем для построения примитивно рекурсивных функций. В то же время класс частично рекурсивных функций шире класса примитивно рекурсивных функций, так как все примитивно рекурсивные функции всюду определены, а среди частично рекурсивных функций встречаются и функции не всюду определенные.

Понятие частично рекурсивной функции оказалось исчерпывающей формализацией понятия вычислимой функции. При построении аксиоматической теории высказываний (см. гл. III) исходные формулы (аксиомы) и правила вывода выбирались так, чтобы полученные в теории формулы исчерпали бы все тавтологии алгебры высказываний. К чему же стремимся мы в теории рекурсивных функций, почему именно так выбрали простейшие функции и операторы для получения новых функций? Рекурсивными функциями мы стремимся исчерпать все мыслимые функции, поддающиеся вычислению с помощью какой-нибудь определенной процедуры механического характера. Подобно тезису Тьюринга, в теории рекурсивных функций выдвигается соответствующая естественно-научная гипотеза, носящая название *тезиса Чёрча*:

Числовая функция тогда и только тогда алгоритмически (или машинно) вычислима, когда она частично рекурсивна.

И эта гипотеза не может быть доказана строго математически, она подтверждается практикой, опытом, ибо призвана увязать практику и теорию. Все рассматривавшиеся в математике конкретные функции, признаваемые вычислимыми в интуитивном смысле, оказывались частично рекурсивными.

Теперь мы рассмотрим более подробно классы примитивно рекурсивных функций и частично рекурсивных функций и докажем, что все функции из каждого из этих классов вычислимы на подходящих машинах Тьюринга.

Примитивно рекурсивные функции. Итак, функция примитивно рекурсивна, если она может быть получена из простейших функций O , S , I_m^n с помощью конечного числа применений операторов суперпозиции и примитивной рекурсии. Рассмотрим ряд примеров примитивно рекурсивных функций.

Пример 33.7. Покажем, как, исходя из простейших функций, с помощью оператора примитивной рекурсии получить следующую функцию, называемую усеченной разностью:

$$x \dot{-} y = \begin{cases} x - y, & \text{если } x \geq y, \\ 0, & \text{если } x < y. \end{cases}$$

Во-первых, отметим, что функция $x \dot{-} 1$, получающаяся из функции $x \dot{-} y$ фиксированием второго аргумента, удовлетворяет следующим соотношениям:

$$0 \div 1 = 0 = O(x);$$

$$(x + 1) \div 1 = x = I_1^2(x, y),$$

т.е. получена из простейших функций $O(x)$ и $I_1^2(x, y)$ с помощью оператора примитивной рекурсии. Во-вторых, нетрудно понять, исходя из определения усеченной разности, что эта функция удовлетворяет также равенствам:

$$x \div 0 = x = I_1^2(x, y);$$

$$x \div (y + 1) = (x \div y) \div 1 = h(x, y, x \div y)$$

для любых x и y . Тождества показывают, что двухместная функция $x \div y$ получена с помощью оператора примитивной рекурсии из простейшей функции $I_1^2(x, y)$ и функции $h(x, y, z) = z \div 1$.

Пример 33.8. Покажем, что функция $s(x, y) = x + y$ может быть получена из простейших с помощью оператора примитивной рекурсии. Для функции верны следующие тождества:

$$x + 0 = x;$$

$$x + (y + 1) = (x + y) + 1,$$

которые можно записать в виде

$$s(x, 0) = x;$$

$$s(x, y + 1) = s(x, y) + 1$$

или

$$s(x, 0) = I_1^1(x);$$

$$s(x, y + 1) = S(s(x, y)),$$

а это и есть схема примитивной рекурсии, основывающаяся на простейших функциях I_1^1 и S .

Пример 33.9. Аналогично операции сложения, очевидные соотношения для операции умножения $p(x, 0) = x \cdot 0 = 0 = O(x)$, $p(x, y + 1) = x \cdot y + x = p(x, y) + x = x + p(x, y) = s(x, p(x, y))$ говорят о том, что функция $p(x, y) = x \cdot y$ получена из простейшей функции $O(x)$ и функции $s(x, y) = x + y$ с помощью оператора примитивной рекурсии.

Теорема 33.10. *Функция, полученная суперпозицией примитивно рекурсивных функций, сама примитивно рекурсивна.*

Доказательство. В самом деле, компоненты этой функции получены из простейших функций O, S, I_m^n с помощью конечного числа применений операторов суперпозиции и примитивной рекурсии. Чтобы получить рассматриваемую функцию, нужно добавить еще одну суперпозицию. В итоге эта функция также получается из простейших функций в результате конечного числа применений операторов суперпозиции и примитивной рекурсии, т.е. является примитивно рекурсивной. $\square$

С использованием этой теоремы в Задачнике доказывается примитивная рекурсивность еще ряда функций (см. задачи № 13.3, 13.5, 13.6), среди которых содержатся и все булевы функции (см. задачу № 13.7).

Примитивная рекурсивность предикатов. Определив в самом начале § 18 понятие предиката, мы отметили, что к этому понятию возможен и еще один подход. Предикат $P(x_1, \dots, x_n)$, заданный над множествами $M_1, \dots, M_n$, есть функция, заданная на указанных множествах и принимающая значения в двухэлементном множестве $\{0, 1\}$. В теории алгоритмов принято различать предикат P и функцию, связанную с ним, а саму функцию называют характеристической функцией предиката P и обозначают χ_P . Таким образом,

$$\chi_P(x_1, \dots, x_n) = \begin{cases} 0, & \text{если высказывание } P(x_1, \dots, x_n) \text{ — истинно,} \\ 1, & \text{если высказывание } P(x_1, \dots, x_n) \text{ — ложно.} \end{cases}$$

Если $M_1 = \dots = M_n = N$, то χ_P — функция, входящая в круг наших рассмотрений, и имеет смысл поставить вопрос о ее примитивной рекурсивности.

Определение 33.11. Предикат P называется *примитивно рекурсивным*, если его характеристическая функция χ_P примитивно рекурсивна.

В Задачнике рассматриваются примеры примитивно рекурсивных предикатов (см. № 13.11—13.14).

Отметим еще одно важное свойство, связанное с примитивной рекурсивностью функций. Мы используем его в последующих рассмотрениях. Одним из часто встречающихся, особенно в теории алгоритмов, способов задания функций является их задание с помощью так называемого *оператора условного перехода*. Этот оператор по функциям $f_1(x_1, \dots, x_n)$, $f_2(x_1, \dots, x_n)$ и предикату $P(x_1, \dots, x_n)$ строит функцию ϕ :

$$\phi(x_1, \dots, x_n) = \begin{cases} f_1(x_1, \dots, x_n), & \text{если } P(x_1, \dots, x_n) \text{ — истинно,} \\ f_2(x_1, \dots, x_n), & \text{если } P(x_1, \dots, x_n) \text{ — ложно.} \end{cases}$$

Нетрудно понять, что с помощью характеристических функций предиката P и его отрицания $\neg P$ функцию ϕ можно выразить следующим образом:

$$\phi(x_1, \dots, x_n) = f_1(x_1, \dots, x_n) \cdot \chi_P(x_1, \dots, x_n) + f_2(x_1, \dots, x_n) \cdot \chi_{\neg P}(x_1, \dots, x_n).$$

Из этого выражения вытекает следующее утверждение.

Теорема 33.12. Если функции f_1, f_2 и предикат P примитивно рекурсивны, то и функция ϕ , построенная из f_1, f_2, P с помощью оператора условного перехода, примитивно рекурсивна. Этот факт выражают также говоря, что оператор условного перехода примитивно рекурсивен.

Оператор условного перехода может иметь и более общую форму, когда переход носит не двужначный, а многозначный характер и определяется конечным числом предикатов $P_1, \dots, P_k$, из которых истинен всегда один и только один предикат. Ясно, что и в такой форме оператор условного перехода примитивно рекурсивен, так как и в этом случае производимую им функцию можно представить в аналогичном виде:

$$\varphi(x_1, \dots, x_n) = f_1 \cdot \chi_{P_1} + \dots + f_k \cdot \chi_{P_k}.$$

Заметим, что это соотношение определяет φ и в том случае, когда ни один из $P_1, \dots, P_k$ не истинен: в этом случае φ равно нулю.

Последнее замечание позволяет доказать примитивную рекурсивность функций, заданных на конечных множествах, ибо все их можно задать с помощью оператора условного перехода. Правда, при этом их придется доопределить с помощью какой-либо константы на всех остальных натуральных числах, на которых она не определена. Например, функцию φ , определенную на множестве $\{1, 3, 9, 17\}$ равенствами $\varphi(1) = 8$, $\varphi(3) = 0$, $\varphi(9) = 4$, $\varphi(17) = 6$, с помощью оператора условного перехода можно описать так:

$$\varphi(x) = \begin{cases} 8, & \text{если } x = 1, \\ 0, & \text{если } x = 3, \\ 8, & \text{если } x = 9, \\ 6 & \text{— в остальных случаях.} \end{cases}$$

Таким образом, $\varphi(x) = 6$ вне исходной области задания.

В заключение обсуждения примитивно рекурсивных функций сделаем два важных замечания.

Во-первых, все примитивно рекурсивные функции всюду определены. Это следует из того, что всюду определены простейшие функции, а операторы суперпозиции и примитивной рекурсии это свойство сохраняют.

Во-вторых, строго говоря, мы имеем дело не с функциями, а с их примитивно рекурсивными описаниями. Различие здесь точно такое же, как и различие между булевыми функциями и их представлениями в виде формул. Примитивно рекурсивные описания также разбиваются на классы эквивалентности: в один класс входят все описания, задающие одну и ту же функцию. Но задача распознавания эквивалентности примитивно рекурсивных описаний являет собой еще один пример алгоритмически неразрешимой задачи (см. также § 36).

Вычислимость по Тьюрингу примитивно рекурсивных функций. Теперь мы готовы к тому, чтобы сделать еще один шаг на пути (в каком-то смысле аксиоматического) описания всех функций,

вычислимых с помощью машины Тьюринга. Мы докажем, что всякая примитивно рекурсивная функция вычислима с помощью машины Тьюринга. Для этого остается доказать следующую теорему.

Теорема 33.13. Функция φ , возникающая примитивной рекурсией из правильно вычислимых на машине Тьюринга функций f и g , сама правильно вычислима на машине Тьюринга.

Доказательство. Для краткости записей будем считать, что функция φ связана с функциями f и g следующим образом: $\varphi(x, 0) = f(x)$, $\varphi(x, i + 1) = g(x, \varphi(x, i))$. Обозначим F и G — машины Тьюринга, правильно вычисляющие функции f и g соответственно. Пусть x, y — произвольные натуральные числа. Требуется сконструировать машину Тьюринга, вычисляющую значение $\varphi(x, y)$. Как мы уже отмечали, для вычисления $\varphi(x, y)$ предстоит вычислить $y + 1$ значений $\varphi(x, 0), \varphi(x, 1), \dots, \varphi(x, y - 1), \varphi(x, y)$.

Начальная конфигурация такова: $q_101^*01^*0$. Применим к ней следующую последовательность машин Тьюринга: B^*VGBB^*F . В результате получим последовательность конфигураций:

$$\begin{aligned} q_1 01^x 01^y 0 &\stackrel{B^+}{\Rightarrow} 01^x q 01^y 0 \stackrel{B}{\Rightarrow} 01^y q 01^x 0 \stackrel{\Gamma}{\Rightarrow} 01^y q 01^x 01^x 0 \stackrel{B}{\Rightarrow} 01^x q 01^y 01^x 0 \stackrel{B^+}{\Rightarrow} \\ &\stackrel{B^+}{\Rightarrow} 01^x 01^y q 01^x 0 \stackrel{F}{\Rightarrow} 01^x 01^y q_{\alpha} 01^{\varphi(x,0)} 0. \end{aligned}$$

На последнем шаге, применив машину, вычисляющую функцию $f(x)$, к конфигурации $q01^x$, мы получим значение $f(x)$, которое, согласно схеме примитивной рекурсии для φ , есть $\varphi(x, 0)$. (Промежуточным состояниям q мы намеренно не приписывали никаких индексов. Индекс α получило лишь последнее в этой последовательности состояние.)

Теперь мы можем приступить к вычислению $\varphi(x, 1)$, используя второе соотношение схемы примитивной рекурсии: $\varphi(x, 1) = g(x, \varphi(x, 0))$. Для этого применим сначала к последней конфигурации команды: $q_{\alpha}^0 \rightarrow q_{\alpha+1}^0 0$, $q_{\alpha+1} \rightarrow q_{\alpha+2}^0$. В результате получим конфигурацию: $01^*01^{y-1}q_{\alpha+2}^001^{\varphi(x, 0)}0$. Теперь нужно подготовить ленту машины к применению машины G , вычисляющей значение $g(x, \varphi(x, 0))$, т.е. необходимо получить на ленте конфигурацию $q01^*01^{\varphi(x, 0)}$. Для этого применим к конфигурации $01^*01^{y-1}q_{\alpha+2}^001^{\varphi(x, 0)}0$ последовательность машин $AB-BB^+BGBB-BB^+B-BB^-$. Получим последовательность конфигураций:

$$\begin{aligned}
01^x 01^{y-1} q_{\alpha+2} 001^{\varphi(x,0)} 0 &\xRightarrow{A} 01^x 01^{y-1} q 01^{\varphi(x,0)} 00 \xRightarrow{B^-} 01^x q 01^{y-1} 01^{\varphi(x,0)} \xRightarrow{B} \\
&\xRightarrow{B} 01^{y-1} q 01^x 01^{\varphi(x,0)} \xRightarrow{B^+} 01^{y-1} 01^x q 01^{\varphi(x,0)} \xRightarrow{B} 01^{y-1} 01^{\varphi(x,0)} q 01^x \xRightarrow{\Gamma} \\
&\xRightarrow{\Gamma} 01^{y-1} 01^{\varphi(x,0)} q 01^x 01^x \xRightarrow{B} 01^{y-1} 01^x q 01^{\varphi(x,0)} 01^x \xRightarrow{B^-} 01^{y-1} q 01^x 01^{\varphi(x,0)} 01^x \xRightarrow{B} \\
&\xRightarrow{B} 01^x q 01^{y-1} 01^{\varphi(x,0)} 01^x \xRightarrow{B^+} 01^x 01^{y-1} q 01^{\varphi(x,0)} 01^x \xRightarrow{B^+} \\
&\xRightarrow{B^+} 01^x 01^{y-1} 01^{\varphi(x,0)} q 01^x \xRightarrow{B} 01^x 01^{y-1} 01^x q 01^{\varphi(x,0)} \xRightarrow{B^-} 01^x 01^{y-1} q 01^x 01^{\varphi(x,0)}.
\end{aligned}$$

Теперь мы можем применить машину G и вычислить значение $\varphi(x, 1) = g(x, \varphi(x, 0)) : 01^x 01^{y-1} q_\beta 01^{\varphi(x, 0)}$.

Применим к этой конфигурации команду: $q_\beta 0 \rightarrow q_\alpha 0$, закли- вающую программу. Получим конфигурацию: $01^x 01^{y-1} q_\alpha 01^{\varphi(x, 1)}$.

Начинается следующий цикл, осуществляемый командами, идущими после первого появления состояния q_α . Этот цикл пре- образует конфигурацию вида $01^x 01^{y-i} q_\alpha 01^{\varphi(x, i)}$ в конфигурацию $01^x 01^{y-(i+1)} q_\beta 01^{\varphi(x, i+1)}$ при условии, что $y > i$. Команда $q_\beta 0 \rightarrow q_\alpha 0$ закликает программу, и в результате работы цикла параметр $y-i$ будет понижаться до тех пор, пока не получится конфигурация: $01^x 0 q_\alpha 01^{\varphi(x, y)}$, которая в силу команды $q_\alpha 0 \rightarrow q_{\alpha+1} 0$ перейдет в конфигурацию $01^x q_{\alpha+1} 0 01^{\varphi(x, y)}$.

Дополнительные команды $q_{\alpha+1} 0 \rightarrow q_{\beta+1} 0$, А, В, О, В, Б-, А создают на ленте требуемую конфигурацию $q_0 01^{\varphi(x, y)}$, доказыва- щую, что функция $\varphi(x, y)$ правильно вычислена на машине Тью- ринга. $\square$

Следствие 33.14. *Всякая примитивно рекурсивная функция вы- числима по Тьюрингу.*

Доказательство. Утверждение следует (ввиду определения 33.4 примитивно рекурсивной функции) из вычислимости по Тью- рингу простейших функций и свойств сохранения такой вычис- лимости операторами суперпозиции (теорема 33.2) и примитив- ной рекурсии (теорема 33.13). $\square$

Функции Аккермана. Напомним, что мы поставили задачу оха- рактеризовать вычислимые (с помощью какого-либо алгоритма) функции. Учитывая тезис Тьюринга (см. § 32), под алгоритмом достаточно понимать машину Тьюринга. После того как в преды- дущем пункте было доказано, что всякая примитивно рекурсив- ная функция вычислима (по Тьюрингу), возникает обратный воп- рос: исчерпывается ли класс вычислимых (по Тьюрингу) функ- ций примитивно рекурсивными функциями, т.е. всякая ли вы- числимая (по Тьюрингу) функция будет непременно примитив- но рекурсивной?

Применив теоретико-множественное понятие о мощности, до- статочно легко ответить отрицательно на более общий вопрос: исчерпывается ли класс всех функций примитивно рекурсивны- ми функциями, т.е. все ли функции являются примитивно рекур- сивными?

Теорема 33.15. *Существуют функции, не являющиеся примитив- но рекурсивными.*

Доказательство. В самом деле, нетрудно понять, что мно- жество всех примитивно рекурсивных функций счетно. Это объяс- няется тем, что каждая примитивно рекурсивная функция имеет конечное описание, т.е. задается конечным словом в некотором (фиксированном для всех функций) алфавите. Множество всех конечных слов счетно. Поэтому и примитивно рекурсивных функ-

ций имеется не более, чем счетное множество. В то же время множество всех функций даже от одного аргумента из N в N имеет мощность континуума. Тем более, континуально множество функций из N в N от любого конечного числа аргументов. Таким образом, непременно существуют функции, не являющиеся примитивно рекурсивными. $\square$

Отрицательным будет также ответ и на более узкий вопрос, поставленный в предыдущем пункте: все ли вычислимые (а в силу тезиса Тьюринга — вычислимые по Тьюрингу) функции можно описать как примитивно рекурсивные? Чтобы это установить, необходимо привести пример вычислимой функции, не являющейся примитивно рекурсивной. Идея примера состоит в том, чтобы построить такую вычислимую функцию, которая обладала бы свойством, каким не обладает ни одна примитивно рекурсивная функция. Таким свойством может служить скорость роста функции. Итак, необходимо указать такую вычислимую функцию, которая растет быстрее любой примитивно рекурсивной функции и поэтому примитивно рекурсивной не является.

Пример 33.16. Искомая функция конструируется с помощью последовательности вычислимых функций, в которой каждая функция растет существенно быстрее предыдущей.

Начнем с построения такой последовательности. Мы знаем, что произведение растет быстрее суммы, а степень — быстрее произведения. Начнем построение последовательности именно с этих функций, введя для них единообразные обозначения:

$$P_0(a, y) = a + y; \quad P_1(a, y) = a \cdot y; \quad P_2(a, y) = a^y.$$

Эти функции связаны между собой следующими рекурсивными соотношениями:

$$\begin{aligned} P_1(a, y+1) &= a + ay = P_0(a, P_1(a, y)), & P_1(a, 1) &= a; \\ P_2(a, y+1) &= a \cdot a^y = P_1(a, P_2(a, y)), & P_2(a, 1) &= a. \end{aligned}$$

Продолжим эту последовательность, положив по определению для $n = 2, 3, \dots$:

$$\left. \begin{aligned} P_{n+1}(a, 0) &= 1, \\ P_{n+1}(a, 1) &= a, \\ P_{n+1}(a, y+1) &= P_n(a, P_{n+1}(a, y)). \end{aligned} \right\} \quad (1)$$

(Первое из равенств (1) предназначено для того, чтобы функции $P_n(a, y)$ были всюду определены.) Эта схема имеет вид примитивной рекурсии, и, следовательно, все функции $P_n(a, y)$ примитивно рекурсивны. Растут они крайне быстро. Например, $P_3(a, 1) = a$, $P_3(a, 2) = P_2(a, a) = a^a$, ... Значение $P_3(a, k+1)$ получается в результате возведения числа a в степень a k раз.

Зафиксируем теперь значение $a = 2$. Получим последовательность функций от одного аргумента: $P_0(2, y)$, $P_1(2, y)$, ... Введем две новые функции: $B(x, y) = P_x(2, y)$ (она перечисляет последнюю последовательность) и $A(x) = B(x, x)$. Первая из них называется *функцией Аккермана*, а вторая — *диагональной функцией Аккермана*.

Для функции $B(x, y)$ на основании введенных выше обозначений и соотношений (1) вытекают следующие равенства:

$$\left. \begin{aligned} B(0, y) &= 2 + y, \\ B(x + 1, 0) &= \text{sg}(x), \\ B(x + 1, y + 1) &= B(x, B(x + 1, y)), \end{aligned} \right\} \quad (2)$$

которые позволяют вычислять значение функции $B(x, y)$, а следовательно, и значения функции $A(x)$. При этом в процессе вычисления значения функции $B(x, y)$ в некоторой точке используются вычисленные ранее ее значения в неких предыдущих точках. Этим схема (2) похожа на схему примитивной рекурсии. Но примитивная рекурсия ведется по одному аргументу, а в схеме (2) рекурсия ведется сразу по двум аргументам (такая рекурсия называется двойной, двухкратной, или рекурсией второй ступени). При этом существенно усложняется характер упорядочения точек, а следовательно, и понятие предшествующей точки. Это упорядочение не предопределено заранее, как в схеме примитивной рекурсии, где число n всегда предшествует числу $n + 1$, а выясняется в ходе вычислений и для каждой схемы (2), вообще говоря, различно. Например, $B(3, 3) = B(2, B(3, 2))$, а так как $B(3, 2) = P_3(2, 2) = P_2(2, P_3(2, 1)) = P_2(2, 2) = 2^2 = 4$, то вычислению B в точке $(3, 3)$ по схеме (2) должно предшествовать вычисление B в точке $(2, 4)$: $B(3, 3) = B(2, 4) = P_2(2, 4) = 2^4 = 16$. Проверьте самостоятельно, что вычислению B в точке $(3, 4)$ должно предшествовать вычисление в точке $(2, 16)$.

Итак, функция $B(x, y)$, а вместе с ней и функция $A(x)$ вычислимы (по схеме (2)), а значит, в силу гипотезы Тьюринга, вычислимы посредством подходящей машины Тьюринга. Возникает вопрос, можно ли их вычисление свести к вычислению по схеме примитивной рекурсии, т.е. будут ли эти функции примитивно рекурсивными. Именно такова ситуация с функцией Аккермана $A(x)$. Идея доказательства того, что функция $A(x)$ не является примитивно рекурсивной, состоит в доказательстве того, что функция $A(x)$ растет быстрее, чем любая примитивно рекурсивная функция, и поэтому не может быть примитивно рекурсивной. Более точно, для любой примитивно рекурсивной функции $f(x)$ от одного аргумента найдется такое n , что для любого $x \geq n$ будет $A(x) > f(x)$. (Это доказал Аккерман в 1928 г.)

Идея доказательства этого утверждения состоит в следующем. Сначала доказываются два свойства функции $B(x, y)$, которые используются в дальнейшем:

$$B(x, y + 1) > B(x, y) \quad (x, y = 1, 2, \dots);$$

$$B(x + 1, y) \geq B(x, y + 1) \quad (x \geq 1, y \geq 2).$$

Затем вводится понятие B -мажорируемой функции. Функция $f(x_1, \dots, x_n)$ называется B -мажорируемой, если

$$(\exists m \in N)(\forall x_1, \dots, x_n) [\max(x_1, \dots, x_n) > 1 \rightarrow \\ \rightarrow f(x_1, \dots, x_n) < B(m, \max(x_1, \dots, x_n))].$$

Доказывается, что все примитивно рекурсивные функции B -мажорируемы. (Сначала устанавливается B -мажорируемость простейших функций O , $S(x)$, $I_m^n(x)$. Затем доказывается, что оператор суперпозиции, примененный к B -мажорируемым функциям, дает B -мажорируемую функцию. Аналогичным свойством обладает и оператор примитивной рекурсии.)

Наконец, рассмотрим произвольную примитивно рекурсивную функцию $f(x)$. В силу предыдущего утверждения, для некоторого m и любого $x \geq 2$ имеем $f(x) < B(m, x)$. Но тогда $A(m + x) = B(m + x, m + x) > B(m, m + x) > f(m + x)$. (Предпоследнее неравенство получено исходя из двух свойств функции $B(x, y)$, сформулированных вначале.) Это и означает, что $A(x) > f(x)$, начиная по меньшей мере с $x = m + 2$.

Итак, функция Аккермана $A(x)$ не может быть вычислена по схеме примитивной рекурсии, но может быть вычислена по более сложной схеме (2). Следовательно, примитивно рекурсивные функции не исчерпывают класса всех вычислимых функций, а свойство функции быть примитивно рекурсивной не равносильно ее свойству быть вычислимой (в том числе по Тьюрингу). Это говорит о том, что если мы не оставляем затеи породить из простейших функций все вычислимые функции, то мы должны ввести какие-то дополнительные средства (методы) порождения. Таким средством явится оператор минимизации.

Оператор минимизации. Это — оператор наименьшего числа в определении 33.5. В более общем виде его можно определить как оператор, применяемый к произвольному $(n + 1)$ -местному предикату $P(x_1, \dots, x_n, y)$ и дающий в результате n -местную функцию $\varphi(x_1, \dots, x_n)$. Значение $\varphi(a_1, \dots, a_n)$ этой функции на наборе аргументов $a_1, \dots, a_n$ равно наименьшему из таких чисел y , что высказывание $P(a_1, \dots, a_n, y)$ истинно. Оно обозначается $\mu_y P(a_1, \dots, a_n, y)$. Если же наименьшего среди таких чисел не существует, то значение функции $\varphi(x_1, \dots, x_n)$ на этом наборе $a_1, \dots, a_n$ не определено. (Это означает, что оператор минимизации может породить частичную, т.е. не всюду определенную функцию.) Таким образом, $\varphi(x_1, \dots, x_n) = \mu_y P(x_1, \dots, x_n, y)$. Оператор минимизации называется также *оператором наименьшего числа*, или μ -оператором.

Предикат $P(x_1, \dots, x_n, y)$ (заданный над N), к которому применяется оператор минимизации, может быть сконструирован из двух числовых функций следующим образом: « $f_1(x_1, \dots, x_n, y) = f_2(x_1, \dots, x_n, y)$ », или из одной: « $f(x_1, \dots, x_n, y) = 0$ ». Так что оператор минимизации можно рассматривать как оператор, заданный на множестве числовых функций и принимающий значения в нем же.

В этом своем качестве оператор минимизации является удобным средством для построения обратных функций. Действительно, функция $f^{-1}(x) = \mu y[f(y) = x]$ (наименьший y такой, что $f(y) = x$) является обратной для функции $f(x)$. (Поэтому в применении к одноместным функциям оператор минимизации иногда называют *оператором обращения*.)

Рассмотрим примеры действия оператора минимизации для получения обратных функций.

Пример 33.17. Рассмотрим следующую функцию, получающуюся с помощью оператора минимизации:

$$d(x, y) = \mu z[y + z = x] = \mu z[s(I_2^3(x, y, z), I_3^3(x, y, z)) = I_1^3(x, y, z)].$$

Вычислим, например, $d(7, 2)$. Для этого нужно положить $y = 2$ и, придавая переменной z последовательно значения 0, 1, 2, ..., каждый раз вычислять сумму $y + z$. Как только она станет равной 7, то соответствующее значение z принять за значение $d(7, 2)$. Вычисляем:

$$z = 0, 2 + 0 = 2 \neq 7;$$

$$z = 1, 2 + 1 = 3 \neq 7;$$

$$z = 2, 2 + 2 = 4 \neq 7;$$

$$z = 3, 2 + 3 = 5 \neq 7;$$

$$z = 4, 2 + 4 = 6 \neq 7;$$

$$z = 5, 2 + 5 = 7.$$

Таким образом, $d(7, 2) = 5$.

Попытаемся вычислить по этому правилу $d(3, 4)$:

$$z = 0, 4 + 0 = 4 > 3;$$

$$z = 1, 4 + 1 = 5 > 3;$$

$$z = 2, 4 + 2 = 6 > 3;$$

$$\dots\dots\dots$$

Видим, что данный процесс будет продолжаться бесконечно. Следовательно, $d(3, 4)$ не определено.

Пример 33.18. Аналогично, с помощью оператора минимизации можно получить частичную функцию, выражающую частное от деления двух натуральных чисел:

$$x/y = q(x, y) = \mu z[y \cdot z = x] = \mu z[p(I_2^3(x, y, z), I_3^3(x, y, z)) = I_1^3(x, y, z)].$$

Заметим, что обе функции из двух последних примеров не всюду определены, т. е. являются частичными.

В Задачнике рассматриваются и другие функции, получаемые с помощью оператора минимизации (см. № 13.17).

С помощью μ -оператора можно построить некоторые всюду определенные аналоги рассмотренных функций:

$$[x - y] = \mu z[y + z \geq x] = \mu z[y + z + 1 > x];$$

$$[x/y] = \mu z[yz \geq x] = \mu z[y(z + 1) > x].$$

Первая из этих функций равна 0, если $x < y$, и равна $x - y$, если $x \geq y$. Вторая представляет собой целую часть функций x/y .

Заметим, что механизм проявления неопределенности функции в точке при вычислении ее значения с помощью μ -оператора такой же, как и при вычислении ее на машине Тьюринга: в случае неопределенности процесс вычисления не останавливается, а продолжается неограниченно долго.

Общерекурсивные и частично рекурсивные функции. Итак, функция называется *частично рекурсивной* (определение 33.6), если она может быть построена из простейших функций O , S , I_m^n с помощью конечного числа применений суперпозиции, примитивной рекурсии и μ -оператора. Если функция всюду определена и частично рекурсивна, то она называется *общерекурсивной*.

Мы уже отмечали, что класс частично рекурсивных функций шире класса примитивно рекурсивных функций, так как все примитивно рекурсивные функции всюду определены, а среди частично рекурсивных функций встречаются функции, не всюду определенные, например функции $d(x, y)$ и $q(x, y)$, рассмотренные в примерах 33.17, 33.18, а также, например, нигде не определенная функция $f(x) = \mu y[x + 1 + y = 0]$. Примером общерекурсивной, но не примитивно рекурсивной функции может служить и функция Аккермана $A(x)$. (Доказательство ее общерекурсивности можно найти, например, в [11.8], часть III, § 1, № 42, а.)

Продолжим теперь продвижение к поставленной цели — к описанию всех функций, вычислимых на машинах Тьюринга. Следующий шаг — доказательство того, что все частично рекурсивные функции вычислимы по Тьюрингу.

Вычислимость по Тьюрингу частично рекурсивных функций. Теорема 33.19. *Если функция $f(x, y)$ правильно вычислима на машине Тьюринга, то и функция $\phi(x) = \mu y[f(x, y) = 0]$, получающаяся с помощью оператора минимизации из функции $f(x, y)$, также правильно вычислима на машине Тьюринга.*

Доказательство. Обозначим F — машину Тьюринга, правильно вычисляющую функцию $f(x, y)$. Используя ее, сконструируем такую машину Тьюринга, которая для заданного значения x вычисляет последовательно значения $f(x, 0)$, $f(x, 1)$, $f(x, 2)$, ... до тех пор, пока в первый раз получится $f(x, i) = 0$. После этого машина должна выдать на ленту число i , представляющее собой значение функции $\phi(x) = i$. Если же для всех i будет иметь место $f(x, i) > 0$, то

машина должна работать вечно, и это будет означать, что функция φ не определена в точке x . Начальная конфигурация на конструируемой машине такова: $q_1 0^x 0$. Будем мыслить ее следующим образом: $q_1 0^x 0^1 0$ и начнем с применения к ней машины «копирование» K_2 . Получим конфигурацию: $0^1 x 0^1 0^1 q_0 0^1 0^1$. Теперь вычислим значение $f(x, 0)$, применив машину F : $0^1 x 0^1 0^1 q_\alpha 0^1 f(x, 0)$.

Далее подбираем команды, которые при условии $f(x, i) > 0$ преобразовывают конфигурацию $0^1 x 0^1 i q_0 0^1 f(x, i)$ в конфигурацию $0^1 x 0^1 i+1 q_0 0^1 f(x, i+1)$:

$q_\alpha 0 \rightarrow q_{\alpha+1} 0 \text{П:}$	$0^1 x 0^1 0^0 q_{\alpha+1} 1^f(x, 0);$
$q_{\alpha+1} 1 \rightarrow q_{\alpha+2} 0:$	$0^1 x 0^1 0^0 q_{\alpha+2} 0 1^f(x, 0)-1;$
$q_{\alpha+2} 0 \rightarrow q_{\alpha+3} 0 \text{Л:}$	$0^1 x 0^1 0^0 q_{\alpha+3} 0 0 1^f(x, 0)-1;$
$q_{\alpha+3} 0 \rightarrow q_{\alpha+4} 1:$	$0^1 x 0^1 0^0 q_{\alpha+4} 1 0 1^f(x, 0)-1;$
$q_{\alpha+4} 1 \rightarrow q_{\alpha+5} 1 \text{П:}$	$0^1 x 0^1 1^1 q_{\alpha+5} 0 1^f(x, 0)-1;$
О:	$0^1 x 0^1 1^1 q_0;$
Б-Б-:	$q_0 1^x 0^1 1;$
$K_2:$	$0^1 x 0^1 1^1 q_0 1^x 0^1 1;$
$F:$	$0^1 x 0^1 1^1 q_\beta 0^1 f(x, 1);$
$q_\beta 0 \rightarrow q_\alpha 0:$	$0^1 x 0^1 1^1 q_\alpha 0^1 f(x, 1).$

Последняя команда закидывает программу, и машина от конфигурации $0^1 x 0^1 1^1 q_\alpha 0^1 f(x, 1)$ переходит к конфигурации $0^1 x 0^1 1^2 q_\alpha 0^1 f(x, 2)$, затем к конфигурации $0^1 x 0^1 1^3 q_\alpha 0^1 f(x, 3)$ и т.д. Допустим, что по истечении некоторого времени машина достигла конфигурации $0^1 x 0^1 i q_\alpha 0^1 f(x, i)$, при которой $f(x, i) = 0$. Это означает, что $\varphi(x) = i$ и машина должна выдать этот результат. Число i накопленно в «счетчике» $0^1 i$. Поэтому поступаем следующим образом. Уже имеющаяся команда $q_\alpha 0 \rightarrow q_{\alpha+1} 0 \text{П}$ приведет машину к конфигурации $0^1 x 0^1 i q_{\alpha+1} 0$. Следующие команды выдают на ленту необходимую конфигурацию $q_0 0^1 i$, т.е. $q_0 0^1 \varphi(x)$:

$q_{\alpha+1} 0 \rightarrow q_7 0:$	$0^1 x 0^1 i q_7 0;$
Б-Б-:	$0^1 x q_0 1^i;$
В О Б-:	$q_8 0^1 i;$
$q_8 0 \rightarrow q_0 0:$	$q_0 0^1 \varphi(x).$

Теорема доказана. $\square$

Следствие 33.20. *Всякая частично рекурсивная функция вычислима по Тьюрингу.*

Доказательство. Итак, поскольку оператор минимизации сохраняет свойство вычислимости по Тьюрингу (этим же свойством, как было установлено выше, обладают и операторы суперпозиции и примитивной рекурсии), простейшие функции O , S , I_n^n вычислимы по Тьюрингу, а всякая частично рекурсивная функция получается из простейших с помощью применения конечного числа раз трех указанных операторов, то всякая частично рекурсивная функция вычислима по Тьюрингу. $\square$

Частичная рекурсивность функций, вычислимых по Тьюрингу.

Наконец мы расширили класс вычислимых по Тьюрингу функций до таких размеров, что он исчерпывает класс *всех* вычислимых по Тьюрингу функций. Это нам и предстоит доказать. Другими словами, мы намерены доказать, что вычислимы по Тьюрингу лишь частично рекурсивные функции, т.е. *если функция вычислима по Тьюрингу, то она частично рекурсивна*. Еще точнее, по функциональной схеме (программе) машины Тьюринга, вычисляющей функцию $f(x_1, \dots, x_n)$, можно построить рекурсивное описание этой функции. Эта теорема впервые была доказана Тьюрингом.

Теорема 33.21. *Если функция вычислима по Тьюрингу, то она частично рекурсивна.*

Доказательство. Прежде чем приступить к доказательству теоремы, обратим внимание на следующее обстоятельство. Машина Тьюринга, преобразовывающая слова в алфавите $A = \{a_0, a_1, \dots, a_{m-1}\}$, никак не различает природу этого алфавита. В частности, она никак не отличает числа от «нечисел»: работая с числами, машина не считает их в смысле известных арифметических правил, а преобразовывает слова, представляющие собой записи чисел на каком-то языке (в какой-то системе счисления). Правила преобразований задаем мы с помощью соответствующей программы, и мы же даем полученному машиной словесному результату числовую интерпретацию. Именно в этом смысле мы говорили о вычислимости машиной Тьюринга тех или иных числовых функций. Чтобы доказать сформулированную теорему, необходимо идею арифметической (числовой) интерпретации работы машины Тьюринга довести до определенного совершенства и показать, что любое преобразование, осуществляемое машиной Тьюринга, если его интерпретировать как вычисление, является частично рекурсивным.

Разделим доказательство на этапы (их будет пять).

Первый этап. Арифметизация машин Тьюринга начинается с того, что мы вводим в машину своего рода арифметическую систему координат. Эта система координат предназначена для конфигураций машины. Как известно, в каждый момент времени конфигурация на ленте машины Тьюринга имеет вид $\alpha q_i a_j \beta$, где α — слово в алфавите $A = \{a_0, a_1, \dots, a_{m-1}\}$, записанное на ленте левее обозреваемой в данный момент ячейки; q_i — состояние, в котором находится в данный момент машина; a_j — содержимое обозреваемой в данный момент ячейки; β — слово в алфавите A , записанное на ленте правее обозреваемой ячейки. Указанной конфигурации однозначно сопоставляется упорядоченная четверка $(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta})$ чисел, определяемых следующим образом: $\bar{q}_i = i$; $\bar{a}_j = j$; $\bar{\alpha}$ — число, изображаемое цифрами, полученными кодированием символов слова α по следующему правилу: эти символы интерпретируются как m -ичные цифры, т.е. цифры m -ичной системы счисления, т.е.

a_i кодируется цифрой i ; $\bar{\beta}$ аналогично получается из β , но при этом читается справа налево, т.е. крайняя слева ячейка β содержит самый младший разряд, а крайняя справа — самый старший (это сделано для того, чтобы нули справа от β не влияли на значение $\bar{\beta}$).

Завершим кодирование элементов машины Тьюринга. Символу a_0 пустой ячейки сопоставим число 0, сдвигу вправо Π сопоставим 1, сдвигу влево Λ — 2, отсутствию сдвига C сопоставим 0, буквой z закодируем заключительное состояние (состояние остановки) q_0 . В итоге алфавит A закодируется числовым множеством $\bar{A}$, а алфавит Q — числовым множеством $\bar{Q}$.

Тогда, например, если мы имеем машину Тьюринга с внешним алфавитом $A = \{a_0, a_1\}$ и на ее ленте имеется конфигурация $a_1 a_0 a_1 a_1 a_0 q_3 a_1 a_1 a_0 a_1 a_1$, то при нашей кодировке (или координатизации) ей соответствует следующая упорядоченная четверка натуральных чисел: (22, 3, 1, 13). Поясним, как она получилась. В нашей конфигурации $\alpha = a_1 a_0 a_1 a_1 a_0$, $q_i = q_3$, $a_j = a_1$, $\beta = a_1 a_0 a_1 a_1$. Поэтому $\bar{\alpha} = 10110$ — двоичное число, которое следующим образом переводится в десятичное: $[10110]_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 22$. Далее, $\bar{q}_3 = 3$, $\bar{a}_1 = 1$ и, наконец, $\bar{\beta} = [1101]_2 = 13$.

Второй этап. При таком кодировании система команд машины Тьюринга с алфавитом A и множеством состояний Q превращается в тройку числовых функций:

$\varphi_a: \bar{Q} \times \bar{A} \rightarrow \bar{A}$ (функция печатаемого символа);

$\varphi_q: \bar{Q} \times \bar{A} \rightarrow \bar{Q}$ (функция следующего состояния);

$\varphi_d: \bar{Q} \times \bar{A} \rightarrow \{0, 1, 2\}$ (функция сдвига).

Например, если среди команд машины Тьюринга имеется команда $q_i a_j \rightarrow q'_i a'_j X$, то $\varphi_a(\bar{q}_i, \bar{a}_j) = \bar{a}'_j$, $\varphi_q(\bar{q}_i, \bar{a}_j) = \bar{q}'_i$, $\varphi_d(\bar{q}_i, \bar{a}_j) = \bar{\xi}$, где $\bar{\xi} = 0, 1, 2$, если $X = C, \Pi, \Lambda$ соответственно.

Отметим, что все эти функции $\varphi_a, \varphi_q, \varphi_d$ заданы на конечном множестве $\bar{Q} \times \bar{A}$ и потому примитивно рекурсивны.

Третий этап. Выполнив одну команду, машина Тьюринга преобразует имеющуюся на ленте конфигурацию $K = \alpha q_i a_j \beta$ в новую конфигурацию $K' = \alpha' q'_i a'_j \beta'$. При арифметизации это означает, что упорядоченной четверке чисел $(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta})$, соответствующей конфигурации K , однозначно сопоставляется упорядоченная четверка чисел $(\bar{\alpha}', \bar{q}'_i, \bar{a}'_j, \bar{\beta}')$, соответствующая конфигурации K' .

Например, при команде $q_3 a_1 \rightarrow q_4 a_0 \Pi$ ранее приведенная конфигурация перейдет в конфигурацию $K' = a_1 a_0 a_1 a_1 a_0 q_4 a_1 a_0 a_1 a_1$, которой соответствует четверка чисел (44, 4, 1, 6).

Так будет происходить почти со всеми конфигурациями, связанными с алфавитами A, Q . В итоге на множестве таких конфигураций будет задана (вообще говоря, не всюду определенная, т.е. частичная) нечисловая функция $\psi_\theta(K) = K'$, обусловленная данной машиной Тьюринга θ . Назовем ее *функцией следующего шага*.

При введенной арифметизации этой функции соответствует четверка числовых функций следующего шага. Иначе говоря, $\bar{\alpha}'$, $\bar{q}'$, $\bar{a}'$, $\bar{\beta}'$ — это числовые функции, каждая из которых зависит от четырех числовых переменных $\bar{\alpha}$, $\bar{q}$, $\bar{a}$, $\bar{\beta}$. Попытаемся понять, как эти функции связаны с функциями системы команд φ_a , φ_q , φ_d . Во-первых, ясно, что $\bar{q}'_i = \varphi_q$ и функция $\bar{q}'$ фактически не зависит от $\bar{\alpha}$, $\bar{\beta}$, а зависит лишь от $\bar{q}$, $\bar{a}$, т.е. $\bar{q}'(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta}) = \varphi_q(\bar{q}_i, \bar{a}_j)$.

Рассмотрим теперь функцию $\bar{\alpha}'(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta})$. Если при рассматриваемом такте работы машины ее головка осталась на месте, т.е. обозреваемая ячейка не изменилась, т.е. $\varphi_d(\bar{q}_i, \bar{a}_j) = 0$, то ясно, что $\bar{\alpha}' = \bar{\alpha}$. Если головка сдвинулась вправо, т.е. $\varphi_d(\bar{q}_i, \bar{a}_j) = 1$, то это означает, что степень каждого разряда числа $\bar{\alpha}$ повысилась на единицу: нулевой разряд стал первым, первый — вторым и т.д., т.е. число $\bar{\alpha}$ увеличилось в m раз (напомним, что m — число элементов в алфавите A , т.е. основание системы счисления, в которой рассматривается наша арифметизация): $m\bar{\alpha}$. Кроме того, в образовавшийся младший (нулевой) разряд помещается та m -ичная цифра, которая соответствует при кодировании только что вписанному на ленту элементу из A . Эта цифра равна $\varphi_a(\bar{q}_i, \bar{a}_j)$. В итоге получим, что при сдвиге вправо: $\bar{\alpha}'(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta}) = m\bar{\alpha} + \varphi_a(\bar{q}_i, \bar{a}_j)$. Наконец, при сдвиге на данном шаге головки влево, т.е. при $\varphi_d(\bar{q}_i, \bar{a}_j) = 2$, степень каждого разряда числа $\bar{\alpha}$ понизилась на единицу: первый разряд стал нулевым, второй — первым и т.д., т.е. число $\bar{\alpha}$ уменьшилось в m раз: $\bar{\alpha}/m$. Но поскольку самый младший (нулевой) разряд оказался фактически как бы «отрубленным», то в итоге получилось не частное $\bar{\alpha}/m$ (оно могло бы оказаться дробным), а его целая часть: $[\bar{\alpha}/m]$.

Итак, для функции $\bar{\alpha}'$ мы получаем следующее описание с помощью оператора условного перехода:

$$\bar{\alpha}'(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta}) = \begin{cases} \bar{\alpha}, & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 0 \text{ (нет сдвига),} \\ m\bar{\alpha} + \varphi_a(\bar{q}_i, \bar{a}_j), & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 1 \text{ (сдвиг вправо),} \\ \bar{\alpha}/m, & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 2 \text{ (сдвиг влево).} \end{cases}$$

Совершенно аналогичная, но в определенном смысле двойственная картина наблюдается и для функции $\bar{\beta}'$: при сдвиге вправо (влево) она ведет себя так же, как функция $\bar{\alpha}'$ при сдвиге влево (вправо). Так что для нее получаем следующее описание с помощью оператора условного перехода:

$$\bar{\beta}'(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta}) = \begin{cases} \bar{\beta}, & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 0 \text{ (нет сдвига),} \\ \bar{\beta}/m, & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 1 \text{ (сдвиг вправо),} \\ m\bar{\beta} + \varphi_a(\bar{q}_i, \bar{a}_j), & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 2 \text{ (сдвиг влево).} \end{cases}$$

Наконец, рассмотрим функцию $\bar{\alpha}'(\bar{\alpha}, \bar{q}, \bar{a}, \bar{\beta})$. Если сдвига не происходит, то ясно, что $\bar{\alpha}' = \varphi_a(\bar{q}_i, \bar{a}_j)$. Если происходит сдвиг вправо, то машина приходит к обозрению самого левого разряда (напомним, что это есть младший разряд) — числа $\bar{\beta}$: именно он был отброшен при взятии для $\bar{\beta}'$ целой части частного $\bar{\beta}/m$. Он как раз и представляет собой остаток от деления числа $\bar{\beta}$ на m , т. е. в этом случае $\bar{\alpha}' = r(m, \bar{\beta})$. Если же происходит сдвиг влево, то двойственно получаем: $\bar{\alpha}' = r(m, \bar{\alpha})$. Итак, функция $\bar{\alpha}'$ получает следующее описание:

$$\bar{\alpha}'(\bar{\alpha}, \bar{q}_i, \bar{a}_j, \bar{\beta}) = \begin{cases} \varphi_a(\bar{q}_i, \bar{a}_j), & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 0 \text{ (нет сдвига),} \\ r(m, \bar{\beta}), & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 1 \text{ (сдвиг вправо),} \\ r(m, \bar{\alpha}), & \text{если } \varphi_d(\bar{q}_i, \bar{a}_j) = 2 \text{ (сдвиг влево).} \end{cases}$$

Теперь сделаем выводы. В полученных выражениях для функций $\bar{q}', \bar{\alpha}', \bar{\beta}', \bar{a}'$ задействованы только примитивно рекурсивные функции, и указанные функции получены из этих примитивно рекурсивных функций с помощью оператора условного перехода, который, как мы знаем, сохраняет свойство примитивной рекурсивности, т. е. из примитивно рекурсивных функций создает снова примитивно рекурсивную функцию. Следовательно, все функции $\bar{\alpha}', \bar{q}', \bar{a}', \bar{\beta}'$ примитивно рекурсивны.

Итак, мы доказали, что на каждом шаге любая машина Тьюринга осуществляет примитивно рекурсивное вычисление.

Четвертый этап. Рассмотрим теперь с точки зрения введенной арифметизации работу машины Тьюринга в целом.

Пусть задана начальная конфигурация $K(0) = (\bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0)$. Тогда конфигурация $K(t)$, возникающая на такте t работы машины, зависит от величины t и компонент $\bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0$ начальной конфигурации, т. е. она является векторной функцией $K(t) = (K_\alpha(t), K_q(t), K_a(t), K_\beta(t))$, компоненты которой, в свою очередь, являются функциями, зависящими от переменных $t, \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0$. Эти функции определяются следующим образом:

$$\begin{aligned} K_\alpha(0, \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0) &= \bar{\alpha}_0; \\ K_\alpha(t+1, \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0) &= \bar{\alpha}'(K_\alpha(t), \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0), K_q(t, \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0), \\ &\quad K_a(t, \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0), K_\beta(t, \bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0)); \\ K_q(0) &= \bar{q}_0; \\ K_q(t+1) &= \bar{q}'(K_\alpha(t), K_q(t), K_a(t), K_\beta(t)); \\ K_a(0) &= \bar{a}_0; \\ K_a(t+1) &= \bar{a}'(K_\alpha(t), K_q(t), K_a(t), K_\beta(t)); \\ K_\beta(0) &= \bar{\beta}_0, K_\beta(t+1) = \bar{\beta}'(K_\alpha(t), K_q(t), K_a(t), K_\beta(t)). \end{aligned}$$

(В записях для функций K_q, K_a, K_β аргументы $\bar{\alpha}_0, \bar{q}_0, \bar{a}_0, \bar{\beta}_0$ для краткости опущены.)

Эти соотношения представляют собой схемы примитивной рекурсии, определяющие функции $K_\alpha, K_q, K_a, K_\beta$ с помощью функ-

ций $\bar{\alpha}', \bar{q}', \bar{a}', \bar{\beta}'$. При этом рекурсия ведется по переменной t . Прimitивная рекурсивность функций $\bar{\alpha}', \bar{q}', \bar{a}', \bar{\beta}'$ установлена на предыдущем шаге доказательства. Тогда отсюда очевидно следует, что и функции $K_\alpha, K_q, K_a, K_\beta$ также примитивно рекурсивны.

Пятый этап. Наконец, на заключительном шаге доказательства покажем, что результат работы машины Тьюринга (т.е. вычисляемая машиной функция) носит рекурсивный характер. (Обратите внимание: не примитивно рекурсивный, а рекурсивный, т.е. здесь придется использовать оператор минимизации μ .)

Здесь мы докажем утверждение, обратное тому, которое было доказано в предыдущем пункте: *всякая функция, правильно вычисляемая на машине Тьюринга, частично рекурсивна*. Пусть φ — функция, правильно вычисляемая машиной Тьюринга. Такая машина, начав с конфигурации $q_1 a_0 \beta_0$, останавливается в конфигурации вида $q_z a_z \beta_z$, т.е. для такой машины $K_\alpha(0) = 0$, $K_q(0) = 1$, исходное слово на ленте кодируется числом $m\beta_0 + \bar{\alpha}_0$, заключительное слово — числом $m\beta_z + \bar{\alpha}_z$, т.е. вычисляется значение функции $\varphi(m\beta_0 + \bar{\alpha}_0) = m\beta_z + \bar{\alpha}_z$. Заключительное слово — это слово, написанное на ленте в тот момент t_z , когда машина впервые перешла в заключительное состояние q_z , т.е. в момент $t_z = \mu t [K_q(t) = z]$. Поэтому $\bar{\beta}_z = K_\beta(t_z)$, $\bar{\alpha}_z = K_\alpha(t_z)$ и $\varphi(m\beta_0 + \bar{\alpha}_0) = m\bar{\beta}_z + \bar{\alpha}_z = mK_\beta(t_z, 0, 1, \bar{\alpha}_0, \bar{\beta}_0) + K_\alpha(t_z, 0, 1, \bar{\alpha}_0, \bar{\beta}_0)$.

Учитывая, что $\bar{\beta}_0 = [x/m]$, $\bar{\alpha}_0 = r(m, x)$, выражение для результирующего значения $\varphi(x)$ можно со всеми подробностями записать так:

$$\varphi(x) = mK_\beta(\mu t [K_q(t, 0, 1, r(m, x), [x/m]) = z], 0, 1, r(m, x), [x/m]) + K_\alpha(\mu t [K_q(t, 0, 1, r(m, x), [x/m]) = z], 0, 1, r(m, x), [x/m]),$$

где m, z — константы, зависящие от конкретной машины. Отсюда непосредственно видно, что функция $\varphi(x)$, представляющая собой результат работы машины Тьюринга, построена из примитивно рекурсивных функций с помощью оператора минимизации μ и, следовательно, является частично рекурсивной.

Этим и завершается доказательство того, что всякая вычисляемая по Тьюрингу функция частично рекурсивна. $\square$

Соединив вместе следствие 33.20 и теорему 33.21, приходим к следующей теореме.

Теорема 33.22. *Функция вычислима по Тьюрингу тогда и только тогда, когда она частично рекурсивна.* $\square$

Итог рассмотрений настоящего параграфа состоит в том, что мы дали некую альтернативную характеристику вычислимым по Тьюрингу функциям: это те и только те функции, которые частично рекурсивны. Другими словами, класс функций, вычисляемых по Тьюрингу, совпадает с классом частично рекурсивных функций. Совпадение этих двух классов вычисляемых функций, в основе построения которых лежали совершенно разные подходы к формализации

понятия вычислимости функции, говорит о том, что эти подходы оказались весьма состоятельными, и служит косвенным подтверждением того, что как тезис Тьюринга, так и тезис Чёрча не только не безосновательны, но и имеют все права на признание.

§ 34. Нормальные алгоритмы Маркова

Теория нормальных алгоритмов (или алгорифмов, как называл их создатель теории) была разработана советским математиком А. А. Марковым (1903—1979) в конце 1940-х — начале 1950-х гг. XX в. Эти алгоритмы представляют собой некоторые правила по переработке слов в каком-либо алфавите, так что исходные данные и искомые результаты для алгоритмов являются словами в некотором алфавите.

Марковские подстановки. *Алфавитом* (как и прежде) называется любое непустое множество. Его элементы называются *буквами*, а любые последовательности букв — *словами* в данном алфавите. Для удобства рассуждений допускаются пустые слова (они не имеют в своем составе ни одной буквы). *Пустое слово* будем обозначать Λ . Если A и B — два алфавита, причем $A \subseteq B$, то алфавит B называется *расширением* алфавита A .

Слова будем обозначать латинскими буквами: P, Q, R (или теми же буквами с индексами). Одно слово может быть составной частью другого слова. Тогда первое называется *подсловом* второго или вхождением во второе. Например, если A — алфавит русских букв, то можем рассмотреть такие слова: P_1 = параграф, P_2 = граф, P_3 = ра. Слово P_2 является подсловом слова P_1 , а P_3 — подсловом P_1 и P_2 , причем в P_1 оно входит дважды. Особый интерес представляет первое вхождение.

Определение 34.1. *Марковской подстановкой* называется операция над словами, задаваемая с помощью упорядоченной пары слов (P, Q) , состоящая в следующем. В заданном слове R находят первое вхождение слова P (если таковое имеется) и, не изменяя остальных частей слова R , заменяют в нем это вхождение словом Q . Полученное слово называется *результатом* применения марковской подстановки (P, Q) к слову R . Если же первого вхождения P в слово R нет (и, следовательно, вообще нет ни одного вхождения P в R), то считается, что марковская подстановка (P, Q) неприменима к слову R .

Частными случаями марковских подстановок являются подстановки с пустыми словами: (Λ, Q) , (P, Λ) , (Λ, Λ) .

Пример 34.2. Примеры марковских подстановок рассмотрены в таблице, в каждой строке которой сначала дается преобразуемое слово, затем применяемая к нему марковская подстановка и, наконец, получающееся в результате слово:

Преобразуемое слово	Марковская подстановка	Результат
138 578 926 тарарам шрам функция логика книга поляна	(8 578 9, 00) (ара, Λ) (ра, ар) (Λ, ζ-) (ика, Λ) (Λ, Λ) (пор, т)	130 026 трам шарм ζ-функция лог книга [неприменима]

Для обозначения марковской подстановки (P, Q) используется запись $P \rightarrow Q$. Она называется *формулой подстановки* (P, Q) . Некоторые подстановки (P, Q) будем называть *заключительными* (смысл названия станет ясен чуть позже). Для обозначения таких подстановок будем использовать запись $P \rightarrow \cdot Q$, называя ее *формулой заключительной подстановки*. Слово P называется *левой частью*, а Q — *правой частью* в формуле подстановки.

Нормальные алгоритмы и их применение к словам. Упорядоченный конечный список формул подстановок

$$\begin{cases} P_1 \rightarrow (\cdot)Q_1, \\ P_2 \rightarrow (\cdot)Q_2, \\ \dots\dots\dots \\ P_r \rightarrow (\cdot)Q_r \end{cases}$$

в алфавите A называется *схемой* (или *записью*) нормального алгоритма в A . (Запись точки в скобках означает, что она может стоять в этом месте, а может отсутствовать.) Данная схема определяет (детерминирует) алгоритм преобразования слов, называемый нормальным алгоритмом Маркова. Дадим его точное определение.

Определение 34.3. *Нормальным алгоритмом (Маркова) в алфавите A называется следующее правило построения последовательности V_i слов в алфавите A , исходя из данного слова V в этом алфавите. В качестве начального слова V_0 последовательности берется слово V . Пусть для некоторого $i \geq 0$ слово V_i построено и процесс построения рассматриваемой последовательности еще не завершился. Если при этом в схеме нормального алгоритма нет формул, левые части которых входили бы в V_i , то V_{i+1} полагают равным V_i , и процесс построения последовательности считается завершившимся. Если же в схеме имеются формулы с левыми частями, входящими в V_i , то в качестве V_{i+1} берется результат марковской подстановки правой части первой из таких формул вместо первого вхождения ее левой части в слово V_i ; процесс построения последовательности считается *завершившимся*, если на данном шаге была применена формула *заключительной подстановки*, и *продолжающимся* — в противном случае. Если процесс пост-*

роения упомянутой последовательности обрывается, то говорят, что рассматриваемый *нормальный алгоритм* применим к слову V . Последний член W последовательности называется *результатом применения нормального алгоритма к слову V* . Говорят, что *нормальный алгоритм перерабатывает V в W* .

Последовательность V_i будем записывать следующим образом:

$$V_0 \Rightarrow V_1 \Rightarrow V_2 \Rightarrow \dots \Rightarrow V_{m-1} \Rightarrow V_m,$$

где $V_0 = V$ и $V_m = W$.

Мы определили понятие нормального алгоритма в алфавите A . Если же алгоритм задан в некотором расширении алфавита A , то говорят, что он есть *нормальный алгоритм над A* .

Рассмотрим примеры нормальных алгоритмов.

Пример 34.4. Пусть $A = \{a, b\}$ — алфавит. Рассмотрим следующую схему нормального алгоритма в A :

$$\begin{cases} a \rightarrow .\Lambda, \\ b \rightarrow b. \end{cases}$$

Нетрудно понять, как работает определяемый этой схемой нормальный алгоритм. Всякое слово V в алфавите A , содержащее хотя бы одно вхождение буквы a , он перерабатывает в слово, получающееся из V вычеркиванием в нем самого левого (первого) вхождения буквы a . Пустое слово он перерабатывает в пустое. (Алгоритм не применим к таким словам, которые содержат только букву b .) Например, $aabab \Rightarrow abab$, $ab \Rightarrow b$, $aa \Rightarrow a$, $bbab \Rightarrow bbb$, $baba \Rightarrow bba$.

Пример 34.5. Пусть $A = \{a_0, a_1, \dots, a_n\}$ — алфавит. Рассмотрим схему

$$\begin{cases} a_0 \rightarrow \Lambda, \\ a_1 \rightarrow \Lambda, \\ \dots\dots\dots \\ a_n \rightarrow \Lambda, \\ \Lambda \rightarrow .\Lambda. \end{cases}$$

Она определяет нормальный алгоритм, перерабатывающий всякое слово (в алфавите A) в пустое слово. Например, $a_1 a_2 a_1 a_3 a_0 \Rightarrow a_1 a_2 a_1 a_3 \Rightarrow a_2 a_1 a_3 \Rightarrow a_2 a_3 \Rightarrow a_3 \Rightarrow \Lambda$; $a_0 a_2 a_2 a_1 a_3 a_1 \Rightarrow a_2 a_2 a_1 a_3 a_1 \Rightarrow a_2 a_2 a_3 a_1 \Rightarrow a_2 a_2 a_3 \Rightarrow a_2 a_3 \Rightarrow a_3 \Rightarrow \Lambda$.

Нормально вычислимые функции и принцип нормализации Маркова. Как и машины Тьюринга, нормальные алгоритмы не производят собственно вычислений: они лишь производят преобразования слов, заменяя в них одни буквы другими по предписанным им правилам. В свою очередь, мы предписываем им такие правила, результаты применения которых мы можем интерпретировать как вычисления. Рассмотрим два примера.

Пример 34.6. В алфавите $A = \{1\}$ схема $\Lambda \rightarrow .1$ определяет нормальный алгоритм, который к каждому слову в алфавите $A = \{1\}$ (все такие слова суть следующие: $\Lambda, 1, 11, 111, 1111, 11111$ и т.д.) приписывает слева 1. Следовательно, алгоритм реализует (вычисляет) функцию $f(x) = x + 1$.

Пример 34.7. Дана функция

$$\varphi_3(11 \dots 1) = \begin{cases} 1, & \text{если } n \text{ делится на } 3, \\ \Lambda, & \text{если } n \text{ не делится на } 3, \end{cases}$$

где n — число единиц в слове $11 \dots 1$. Рассмотрим нормальный алгоритм в алфавите $A = \{1\}$ со следующей схемой:

$$\begin{cases} 111 \rightarrow \Lambda, \\ 11 \rightarrow .\Lambda, \\ 1 \rightarrow .\Lambda, \\ \Lambda \rightarrow .1. \end{cases}$$

Этот алгоритм работает по такому принципу: пока число букв 1 в слове не меньше 3, алгоритм последовательно стирает по три буквы. Если число букв меньше 3, но больше 0, то оставшиеся буквы 1 или 11 стираются заключительно; если слово пусто, оно заключительно переводится в слово 1. Например:

$$\begin{aligned} 1111111 &\Rightarrow 1111 \Rightarrow 1 \Rightarrow \Lambda; \\ 111111111 &\Rightarrow 111111 \Rightarrow 111 \Rightarrow \Lambda \Rightarrow 1. \end{aligned}$$

Таким образом, рассмотренный алгоритм реализует (или вычисляет) данную функцию.

Сформулируем теперь точное определение такой вычислимости функций.

Определение 34.8. Функция f , заданная на некотором множестве слов алфавита A , называется *нормально вычислимой*, если найдется такое расширение B данного алфавита ($A \subseteq B$) и такой нормальный алгоритм в B , что каждое слово V (в алфавите A) из области определения функции f этот алгоритм перерабатывает в слово $f(V)$.

Таким образом, нормальные алгоритмы примеров 34.6 и 34.7 показывают, что функции $f(x) = x + 1$ и $\varphi_3(x)$ нормально вычислимы. Причем соответствующие нормальные алгоритмы удалось построить в том же самом алфавите A , на словах которого были заданы рассматривавшиеся функции, т.е. расширять алфавит не потребовалось ($B = A$). Следующий пример демонстрирует нормальный алгоритм в расширенном алфавите, вычисляющий данную функцию.

Пример 34.9. Построим нормальный алгоритм для вычисления функции $f(x) = x + 1$ не в одноичной системе (как сделано в при-

мере 34.6), а в десятичной. В качестве алфавита возьмем перечень арабских цифр $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, а нормальный алгоритм будем строить в его расширении $B = A \cup \{a, b\}$. Вот схема этого нормального алгоритма (читается по столбцам):

$0b \rightarrow . 1$	$a0 \rightarrow 0a$	
$1b \rightarrow . 2$	$a1 \rightarrow 1a$	$1a \rightarrow 1b$
$2b \rightarrow . 3$	$a2 \rightarrow 2a$	$2a \rightarrow 2b$
$3b \rightarrow . 4$	$a3 \rightarrow 3a$	$3a \rightarrow 3b$
$4b \rightarrow . 5$	$a4 \rightarrow 4a$	$4a \rightarrow 4b$
$5b \rightarrow . 6$	$a5 \rightarrow 5a$	$5a \rightarrow 5b$
$6b \rightarrow . 7$	$a6 \rightarrow 6a$	$6a \rightarrow 6b$
$7b \rightarrow . 8$	$a7 \rightarrow 7a$	$7a \rightarrow 7b$
$8b \rightarrow . 9$	$a8 \rightarrow 8a$	$8a \rightarrow 8b$
$9b \rightarrow b0$	$a9 \rightarrow 9a$	$9a \rightarrow 9b$
$b \rightarrow . 1$	$0a \rightarrow 0b$	$\Lambda \rightarrow a.$

Попробуем применить алгоритм к пустому слову Λ . Нетрудно понять, что на каждом шаге должна будет применяться самая последняя формула данной схемы. Получается бесконечный процесс:

$$\Lambda \Rightarrow a \Rightarrow aa \Rightarrow aaa \Rightarrow aaaa \Rightarrow \dots$$

Это означает, что к пустому слову данный алгоритм не применим.

Если применить теперь алгоритм к слову 499, получим следующую последовательность слов: $499 \Rightarrow a499$ (применена последняя формула) $\Rightarrow 4a99$ (формула из середины второго столбца) $\Rightarrow \Rightarrow 49a9 \Rightarrow 499b$ (дважды применена формула из конца второго столбца) $\Rightarrow 499b$ (предпоследняя формула) $\Rightarrow 49b0 \Rightarrow 4b00$ (дважды применена предпоследняя формула первого столбца) $\Rightarrow 500$ (применена формула из середины первого столбца).

Таким образом, слово 499 перерабатывается данным нормальным алгоритмом в слово 500. Предлагается проверить, что $328 \Rightarrow \Rightarrow 329, 789 \Rightarrow 790$.

В рассмотренном примере нормальный алгоритм построен в алфавите B , являющемся существенным расширением алфавита A (т.е. $A \subseteq B$ и $A \neq B$), но данный алгоритм слова в алфавите A перерабатывает снова в слова в алфавите A . В таком случае говорят, что алгоритм задан *над* алфавитом A .

Создатель теории нормальных алгоритмов советский математик А. А. Марков выдвинул гипотезу, получившую название «**Принцип нормализации Маркова**». Согласно этому принципу, *для нахождения значений функции, заданной в некотором алфавите, тогда и только тогда существует какой-нибудь алгоритм, когда функция нормально вычислима.*

Сформулированный принцип, как и тезисы Тьюринга и Чёрча, носит внематематический характер и не может быть строго доказан. Он выдвинут на основании математического и практического опыта.

Все, что в предыдущих параграфах было сказано о тезисах Тьюринга и Чёрча, можно с полным правом отнести к принципу нормализации Маркова. Косвенным подтверждением этого принципа служат теоремы следующего пункта, устанавливающие эквивалентность и этой теории алгоритмов теориям машин Тьюринга и рекурсивных функций.

Совпадение класса всех нормально вычислимых функций с классом всех функций, вычислимых по Тьюрингу. Это совпадение будет означать, что понятие нормально вычислимой функции равносильно понятию функции, вычислимой по Тьюрингу, а вместе с ним и понятию частично рекурсивной функции.

Теорема 34.10. *Всякая функция, вычислимая по Тьюрингу, будет также и нормально вычислимой.*

Доказательство. Пусть машина Тьюринга с внешним алфавитом $A = \{a_0, a_1, \dots, a_m\}$ и алфавитом внутренних состояний $Q = \{q_0, q_1, \dots, q_n\}$ вычисляет некоторую функцию f , заданную и принимающую значения в множестве слов алфавита A (словарную функцию на A). Попытаемся представить программу этой машины Тьюринга в виде схемы некоторого нормального алгоритма. Для этого нужно каждую команду машины Тьюринга $q_\alpha a_i \rightarrow q_\beta a_j X$ представить в виде совокупности марковских подстановок. Конфигурации, возникающие в машине Тьюринга в процессе ее работы, представляют собой слова в алфавите $A \cup Q$. Эти слова имеют вид: $a_i \dots a_i q_\alpha a_{i+1} \dots a_i$. Нам понадобится различать начало слова и его конец (или его левый и правый концы). Для этого к алфавиту $A \cup Q$ добавим еще два символа (не входящие ни в A , ни в Q): $A \cup Q \cup \{u, v\}$. Эти символы будем ставить соответственно в начало и конец каждого машинного слова w : $u w v$.

Пусть на данном шаге работы машины Тьюринга к машинному слову w предстоит применить команду $q_\alpha a_i \rightarrow q_\beta a_j X$. Это означает, что машинное слово w (а вместе с ним и слово $u w v$) содержит подслово $q_\alpha a_i$. Посмотрим, какой совокупностью марковских подстановок можно заменить данную команду в каждом из следующих трех случаев:

а) $X = C$, т. е. команда имеет вид: $q_\alpha a_i \rightarrow q_\beta a_j$. Ясно, что в этом случае следующее слово получается из слова $u w v$ с помощью подстановки $q_\alpha a_i \rightarrow q_\beta a_j$, которую мы и будем считать соответствующей команде $q_\alpha a_i \rightarrow q_\beta a_j$;

б) $X = L$, т. е. команда имеет вид: $q_\alpha a_i \rightarrow q_\beta a_j L$. Нетрудно понять, что в этом случае для получения из слова $u w v$ следующего слова надо к слову $u w v$ применить ту подстановку из совокупности

$$\begin{aligned}
a_0 q_\alpha a_i &\rightarrow q_\beta a_0 a_j; \\
a_1 q_\alpha a_i &\rightarrow q_\beta a_1 a_j; \\
&\dots\dots\dots \\
a_m q_\alpha a_i &\rightarrow q_\beta a_m a_j; \\
u q_\alpha a_i &\rightarrow u q_\beta a_0 a_j,
\end{aligned}$$

которая применима к слову uvw . В частности, последняя подстановка применима только тогда, когда q_α — самая левая буква в слове w , т. е. когда надо пристраивать ячейку слева;

в) $X = \Pi$, т. е. команда имеет вид: $q_\alpha a_i \rightarrow q_\beta a_j \Pi$. В этом случае аналогично, чтобы получить из слова uvw следующее слово, нужно к слову uvw применить ту из подстановок совокупности

$$\begin{aligned}
q_\alpha a_i a_0 &\rightarrow a_j q_\beta a_0; \\
q_\alpha a_i a_1 &\rightarrow a_j q_\beta a_1; \\
&\dots\dots\dots \\
q_\alpha a_i a_m &\rightarrow a_j q_\beta a_m; \\
q_\alpha a_i v &\rightarrow a_j q_\beta a_0 v,
\end{aligned}$$

которая применима к слову uvw .

Поскольку слово $q_\alpha a_i$ входит в слово w только один раз, то к слову uvw применима только одна из подстановок, перечисленных в пунктах б, в. Поэтому порядки следования подстановок в этих пунктах безразличны, важны лишь их совокупности.

Заменяем каждую команду из программы машины Тьюринга указанным способом совокупностью марковских подстановок. Мы получим схему некоторого нормального алгоритма. Теперь ясно, что применить к слову w данную машину Тьюринга — это все равно, что применить к слову uvw построенный нормальный алгоритм. Другими словами, действие машины Тьюринга равнозначно действию подходящего нормального алгоритма. Это и означает, что всякая функция, вычислимая по Тьюрингу, нормально вычислима. $\square$

Верно и обратное утверждение.

Теорема 34.11. *Всякая нормально вычислимая функция вычислима по Тьюрингу.*

Доказательство. В [8.6] (теорема 1, с. 246—249) фактически доказано, что всякая нормально вычислимая функция частично рекурсивна (см. также следствие 5.11 в [5.13], с. 248—249). Добавив сюда доказанное в предыдущем параграфе (следствие 33.20) утверждение о том, что всякая частично рекурсивная функция вычислима по Тьюрингу, мы и приходим к справедливости сформулированного утверждения о вычислимости по Тьюрингу всякой нормально вычислимой функции. $\square$

Таким образом, класс нормально вычисляемых функций совпадает с классом функций, вычисляемых по Тьюрингу.

Эквивалентность различных теорий алгоритмов. Итак, в двух последних параграфах мы познакомились с тремя теориями, каждая из которых уточняет понятие алгоритма, и доказали, что все эти теории равносильны между собой. Другими словами, они описывают один и тот же класс функций, т. е. справедлива следующая теорема.

Теорема 34.12. *Следующие классы функций (заданных на натуральных числах и принимающих натуральные значения) совпадают:*

- а) класс всех функций, вычислимых по Тьюрингу;*
- б) класс всех частично рекурсивных функций;*
- в) класс всех нормально вычислимых функций.*

Полезно уяснить смысл и значение этого важного результата. В разное время в разных странах ученые независимо друг от друга, изучая интуитивное понятие алгоритма и алгоритмической вычислимости, создали теории, описывающие данное понятие, которые оказались равносильными. Этот факт служит мощным косвенным подтверждением адекватности этих теорий опыту вычислений, справедливости каждого из тезисов Тьюринга, Чёрча и Маркова. В самом деле, ведь если бы один из этих классов оказался шире какого-либо другого класса, то соответствующий тезис Тьюринга, Чёрча или Маркова был бы опровергнут. Например, если бы класс нормально вычислимых функций оказался шире класса рекурсивных функций, то существовала бы нормально вычислимая, но не рекурсивная функция. В силу ее нормальной вычислимости она была бы алгоритмически вычислима в интуитивном понимании алгоритма, и предположение о ее нерекурсивности опровергало бы тезис Чёрча. Но классы Тьюринга, Чёрча и Маркова совпадают, и таких функций не существует. Это и служит еще одним косвенным подтверждением тезисов Тьюринга, Маркова и Чёрча.

Можно отметить, что существуют еще и другие теории алгоритмов, и для всех них также доказана их равносильность с рассмотренными теориями.

§ 35. Разрешимость и перечислимость множеств

Теперь, когда мы достаточно подробно изучили три различных формализации понятия алгоритма, установили их эквивалентность и сформулировали тезисы Тьюринга, Чёрча и Маркова, можно сделать некоторые общие выводы. Из наших рассмотрений следует, что любые утверждения о существовании или несуществовании алгоритмов, сделанные в одной из трех формализаций, верны и в другой. Это означает, что возможно развитие и изложение теории алгоритмов, инвариантное по отношению к способу формализации понятия «алгоритм». Это своего рода общая теория алгоритмов. Основные ее понятия — алгоритм и вычислимая функция.

При интерпретировании этой общей теории, например, в теории рекурсивных функций понятие алгоритм превращается в рекурсивное описание функции, понятие вычислимая функция — в понятие частично рекурсивная (или общерекурсивная) функция. (При этом следует всегда помнить, что алгоритм и вычисляемая им функция — это не одно и то же. Одна и та же функция может вычисляться с помощью разных алгоритмов.)

Будем рассматривать функции f от одного или нескольких аргументов, заданные на множестве $N = \{0, 1, 2, 3, 4, \dots, n, \dots\}$ всех натуральных чисел или на некоторых его подмножествах (частичные функции) и принимающие значения в множестве N . Таким образом, рассматриваются функции f , являющиеся отображениями декартовой n -й степени N^n в множество N . Область определения Df функции f есть подмножество множества $N^n = N \times \dots \times N$: $Df = \{(x_1, \dots, x_n) : f(x_1, \dots, x_n) \text{ — определено}\}$. Область изменения (значений) f есть подмножество множества N : $If = \{y \in N : (\exists x_1, \dots, x_n) (f(x_1, \dots, x_n) = y)\}$.

Определение 35.1. Функция $f(x_1, \dots, x_n)$ называется *вычислимой*, если существует алгоритм, позволяющий вычислять ее значения для тех наборов аргументов, для которых она определена, и работающий вечно, если функция для данного набора значений аргументов не определена.

Пусть $M \subseteq N^n = N \times \dots \times N$.

Определение 35.2. Множество M называется *разрешимым*, если существует алгоритм A_M , который по любому объекту a дает ответ, принадлежит a множеству M или нет. Алгоритм A_M называется разрешающим алгоритмом для M .

Известно понятие *характеристической функции* множества M . Ею называется функция χ_M , заданная на множестве M , принимающая значения в двухэлементном множестве $\{0, 1\}$ и определяемая следующим образом:

$$\chi_M(x_1, \dots, x_n) = \begin{cases} 0, & \text{если } (x_1, \dots, x_n) \notin M; \\ 1, & \text{если } (x_1, \dots, x_n) \in M. \end{cases}$$

Отсюда ясно, что множество M разрешимо тогда и только тогда, когда его характеристическая функция χ_M вычислима.

Примером разрешимого множества может служить множество всех тавтологий логики высказываний. Разрешающий алгоритм состоит в прямом вычислении значений данной формулы на всевозможных наборах значений ее пропозициональных переменных (составление таблицы истинности формулы).

Пусть теперь $M \subseteq N$.

Определение 35.3. Множество $M \subseteq N$ называется (*рекурсивно*, или *эффективно*, или *алгоритмически*) перечислимым, если M либо пусто, либо есть область значений некоторой вычислимой функ-

ции или, другими словами, если существует алгоритм для последовательного порождения (перечисления) всех его элементов.

Другими словами, M перечислимо, если существует такая вычислимая функция $\psi_M(x)$, что $a \in M \Leftrightarrow (\exists x)(a = \psi_M(x))$. Функция ψ_M называется *перечисляющей* множество M (или для множества M); соответственно алгоритм, вычисляющий ψ_M , называется *перечисляющим* или *порождающим* для M .

Пример 35.4. Рассмотрим множество $M = \{1, 4, 9, 16, 25, 36, \dots\}$ квадратов натуральных чисел. Оно перечислимо: для получения его элементов нужно последовательно брать числа 1, 2, 3, 4, ... и возводить их в квадрат. Другими словами, M есть область значений вычислимой функции $f(x) = x^2$: $M = \{1^2, 2^2, 3^2, 4^2, \dots\}$. Более того, это множество является также и разрешимым: для проверки того, принадлежит или нет некоторое число данному множеству, нужно разложить число на простые множители, что позволит выяснить, является ли оно точным квадратом.

Далее, в теореме 35.6 будет показано, что любое разрешимое множество перечислимо, а в теореме 35.7 — что обратное утверждение неверно.

Важность понятий разрешимости и перечислимости множеств для оснований математики связана с тем, что язык теории множеств является в известном смысле универсальным языком математики. Всякому математическому утверждению можно придать вид утверждения о каких-либо множествах. В связи с этим к способам задания множеств предъявляются повышенные требования. Необходимо точное понимание таких понятий, как «конструктивный способ задания множества» и «множество, заданное эффективно». Это и достигается благодаря понятиям разрешимости и перечислимости множества. Язык разрешимых и перечислимых множеств является универсальным языком для утверждений о существовании (или отсутствии) алгоритмов решения математических проблем.

Теорема 35.5. Если множества M и L перечислимы, то перечислимы множества $M \cup L$ и $M \cap L$.

Доказательство. Если имеются алгоритмы для порождения элементов множеств M и L , то алгоритм для порождения множества $M \cup L$ получается из исходных путем их одновременного применения. Следовательно, множество $M \cup L$ перечислимо.

Пусть теперь алгоритм Ω_M последовательно порождает элементы $m_1, m_2, m_3, \dots$ множества M , а алгоритм Ω_L последовательно порождает элементы $l_1, l_2, l_3, \dots$ множества L . Тогда алгоритм для перечисления элементов множества $M \cap L$ заключается в следующем.

Поочередно с помощью алгоритмов Ω_M и Ω_L порождаются элементы $m_1, l_1, m_2, l_2, m_3, l_3$ и т.д. Каждый вновь порожденный

элемент m_i сравнивается со всеми ранее порожденными элементами l_j . Если m_i совпадает с одним из них, то он включается во множество $M \cap L$. В противном случае надо переходить к порождению элемента l_i и сравнивать его со всеми ранее порожденными элементами m_j , и т.д. Описанная процедура позволяет эффективно перечислить все элементы множества $M \cap L$, что и требовалось доказать. $\square$

Теорема 35.6. Пусть $M \subseteq N$. Множество M разрешимо тогда и только тогда, когда оно само и его дополнение $\bar{M}$ перечислимы.

Доказательство. Необходимость. Пусть M — разрешимое множество. Можем считать, что $M \neq \emptyset$, т.е. имеется элемент $a \in M$. Тогда характеристическая функция χ_M множества M , как было отмечено выше, вычислима, т.е. имеется алгоритм для ее вычисления.

Строим алгоритм для перечисления множества M . Рассмотрим функцию

$$f(x) = \begin{cases} x, & \text{если } \chi_M(x) = 1, \\ a, & \text{если } \chi_M(x) = 0. \end{cases}$$

Отсюда $M = \{f(0), f(1), f(2), f(3), \dots\}$, т.е. M есть множество значений функции f , которая, очевидно, вычислима ввиду вычислимости функции $\chi_M(x)$. Следовательно, множество M перечислимо.

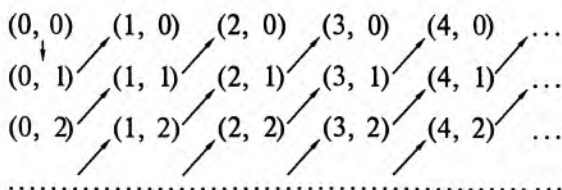
Аналогично, выбрав элемент $b \in \bar{M}$, строим функцию:

$$g(x) = \begin{cases} b, & \text{если } \chi_M(x) = 1, \\ x, & \text{если } \chi_M(x) = 0, \end{cases}$$

которая также вычислима ввиду вычислимости функции $\chi_M(x)$. Кроме того, $\bar{M} = \{g(0), g(1), g(2), g(3), \dots\}$, т.е. $\bar{M}$ есть множество значений вычислимой функции g . Следовательно, множество $\bar{M}$ также перечислимо.

Достаточность. Пусть множества M и $\bar{M}$ перечислимы, т.е. $M = \{f(0), f(1), f(2), f(3), \dots\}$ и $\bar{M} = \{g(0), g(1), g(2), g(3), \dots\}$, где f и g — некоторые вычислимые функции. Тогда алгоритм, выясняющий, принадлежит или нет произвольное число n множеству M , действует следующим образом. Последовательно порождаем элементы $f(0), g(0), f(1), g(1), f(2), g(2), \dots$ и на каждом шаге получаемый элемент сравниваем с n . Поскольку n должно принадлежать либо M , либо $\bar{M}$, то на конечном шаге получим $f(k) = n$ или $g(k) = n$. Если $f(k) = n$, то $n \in M$, а если $g(k) = n$, то $n \in \bar{M}$ и, значит, $n \notin M$. Следовательно, множество M разрешимо. $\square$

Прежде чем переходить к следующей теореме, отметим, что существует эффективное перечисление всех упорядоченных пар натуральных чисел, которое называется *диагональным методом*, или *диагональным процессом*:



Перечисление осуществляется последовательным прохождением по диагоналям, начиная с левого верхнего угла. Первыми парами этого перечисления являются: $(0, 0)$, $(0, 1)$, $(1, 0)$, $(0, 2)$, $(1, 1)$, $(2, 0)$, $(0, 3)$, ... Можно доказать, что в данной последовательности пара (m, n) стоит на месте с номером

$$C(m, n) = \frac{m^2 + 2mn + n^2 + 3m + n + 2}{2}.$$

Теорема 35.7. *Существует перечислимое, но неразрешимое множество натуральных чисел.*

Доказательство. На основании предыдущей теоремы достаточно привести пример такого множества U натуральных чисел, которое само было бы перечислимо, а его дополнение $\bar{U}$ перечислимым не было.

Ясно, что перечислимых множеств натуральных чисел (как и алгоритмов) имеется лишь счетное количество. Следовательно, все перечислимые множества можно расположить в последовательность (перенумеровать): $M_0, M_1, M_2, \dots$ Более того, можно считать, что эта нумерация эффективна, т.е. по номеру множества можно восстановить само это множество. (В начале § 36 будет показано, как можно эффективно перенумеровать все машины Тьюринга, рассматривая их затем как алгоритмы, вычисляющие функции, порождающие перечислимые множества.)

Рассмотрим теперь алгоритм Ω , который последовательно порождает все элементы следующего множества U . На шаге с номером $C(m, n)$ этот алгоритм вычисляет m -й элемент множества M_n , и если элемент совпадает с n , то он относит его в множество U . Таким образом,

$$n \in U \Leftrightarrow n \in M_n.$$

Итак, U порождается алгоритмом Ω , т.е. U перечислимо. Поскольку дополнение $\bar{U}$ множества U состоит из всех таких n , что $n \notin M_n$, то $\bar{U}$ отличается от любого перечислимого множества хотя бы одним элементом. Поэтому $\bar{U}$ не является перечислимым. Следовательно, на основании теоремы 35.6 множество U неразрешимо, что и завершает доказательство. $\square$

Доказанная теорема фактически включает в себя в неявном виде теорему Гёделя о неполноте формальной арифметики, о которой мы подробно будем говорить в заключительном параграфе этой главы.

Подведем некоторые итоги. Итак, эффективно заданное множество — это множество, обладающее разрешающей или перечисляющей функцией (алгоритмом). Объединение и пересечение перечислимых множеств перечислимы. Непустое множество $M \subseteq N$ разрешимо тогда и только тогда, когда оно само и его дополнение перечислимы. В частности, отсюда следует, что всякое непустое разрешимое множество перечислимо. Тем не менее существует перечислимое, но неразрешимое множество натуральных чисел. В теореме 35.7 такое множество описано. Другим примером такого множества является множество $M = \{x : A_x(x) \text{ определен}\}$, т. е. множество номеров самоприменимых алгоритмов.

Таким образом, перечислимость — более слабый вид эффективности, нежели разрешимость. Хотя перечисляющая процедура и задает эффективно список элементов множества M , поиск данного элемента a в этом списке может оказаться неэффективным: это неопределенно долгий процесс, который в конечном счете остановится, если $a \in M$, но не остановится, если $a \notin M$. В случае же перечислимости и дополнения $\overline{M}$ перечисляющая процедура для M становится эффективной и гарантирует разрешимость множества M .

§ 36. Неразрешимые алгоритмические проблемы

Алгоритмическая проблема — это проблема, в которой требуется найти единый метод (алгоритм) для решения бесконечной серии однотипных единичных задач. Такие проблемы называют также *массовыми проблемами*. Они возникали и решались в различных областях математики на протяжении всей ее истории. Примеры таких проблем рассматривались в § 31.

Математики в начале XX в. столкнулись с тем, что для некоторых массовых проблем не удастся подобрать общий алгоритм для их решения. В связи с этим возникла необходимость дать точное определение самому понятию алгоритма. Мы познакомились с несколькими способами такого уточнения, и в настоящем параграфе приведем примеры алгоритмически неразрешимых массовых проблем. Сначала в качестве понятия, уточняющего понятие алгоритма, будем использовать понятие машины Тьюринга. Затем рассмотрим проблему алгоритмической разрешимости в рамках общей теории алгоритмов.

Нумерация алгоритмов. Понятие нумерации алгоритмов — важное средство для их исследования, в частности для доказательств несуществования единого алгоритма для решения той или иной массовой проблемы. Посмотрим сначала на это понятие в рамках нашей общей теории алгоритмов.

Поскольку любой алгоритм можно задать конечным описанием (словом) (например, в конечном алфавите знаков, используемых при наборе математических книг), а множество всех конеч-

ных слов в фиксированном конечном алфавите счетно, то множество всех алгоритмов счетно. Это означает наличие взаимно-однозначного соответствия между множеством N натуральных чисел и множеством всех алгоритмов, рассматриваемым как подмножество множества Al^* всех слов в алфавите Al , выбранном для описания алгоритмов ($\varphi: N \rightarrow Al^*$). Такая функция называется *нумерацией алгоритмов*. Если $\varphi(n) = A$, то число n называется *номером алгоритма A* . Из взаимной однозначности отображения φ следует существование обратной функции φ^{-1} , восстанавливающей по описанию алгоритма A_n его номер в этой нумерации $\varphi^{-1}(A_n) = n$. Очевидно, что различных нумераций много.

Нумерация всех алгоритмов является одновременно и нумерацией всех вычислимых функций в следующем смысле: номер функции f — это номер некоторого алгоритма, вычисляющего f . Ясно, что в любой нумерации всякая функция будет иметь бесконечное множество различных номеров.

Существование нумераций позволяет работать с алгоритмами как с числами. Это особенно удобно при исследовании алгоритмов над алгоритмами. Отсутствие именно таких алгоритмов часто приводит к алгоритмически неразрешимым проблемам.

Нумерация машин Тьюринга. Опишем теперь более конкретный процесс нумерации всех машин Тьюринга, который используем при построении примера невычислимой по Тьюрингу функции. Будем считать, что для обозначения внутренних состояний машин Тьюринга используются буквы бесконечной последовательности: $q_0, q_1, q_2, \dots, q_r, \dots$, а для обозначения букв внешних алфавитов используются буквы последовательности: $a_0, a_1, a_2, \dots, a_s, \dots$

Выразим (или, как говорят, закодируем) все символы этих бесконечных последовательностей словами конечного стандартного алфавита $\{a_0, 1, q, C, П, Л\}$ по следующим правилам:

q_i ($i = 0, 1, \dots$) обозначим (закодируем) словом из $i + 1$ букв q : $qq \dots q$;

a_j ($j = 1, 2, \dots$) обозначим (закодируем) словом из j единиц: $11 \dots 1$.

В стандартном алфавите программу машины Тьюринга можно записать в виде слова, руководствуясь следующим правилом. Сначала все команды программы переводятся на язык стандартного алфавита, для чего в записях этих команд $q_i a_j \rightarrow q_i a_m X$, где $X \in \{C, П, Л\}$, опускается символ « $\rightarrow$ », а буквы q_i, a_j, q_l, a_m заменяются соответствующими словами стандартного алфавита. Затем полученные слова-команды записываются подряд в любом порядке в виде единого слова.

Например, программа машины Тьюринга, рассмотренной в примере 32.1, в этих обозначениях имеет вид: $q_1 a_0 \rightarrow q_2 a_0 П, q_1 a_1 \rightarrow q_1 a_1 П, q_2 a_0 \rightarrow q_0 a_1 C, q_2 a_1 \rightarrow q_2 a_1 П$. Опускаем символ « $\rightarrow$ », заменяем буквы словами стандартного алфавита и в результате полу-

чаем следующие слова в стандартном алфавите, кодирующие соответствующие команды: $qqa_0qqqa_0П$, $qq1qq1П$, $qqqa_0q1С$, $qqq1qqq1П$. Выписываем эти слова подряд и получаем слово, кодирующее программу данной машины Тьюринга:

$qqa_0qqqa_0Пqq1qq1Пqqqa_0q1Сqqq1qqq1П$.

Нетрудно указать алгоритм, позволяющий узнавать, является ли слово в стандартном алфавите программой некоторой машины Тьюринга. Такой алгоритм может, например, состоять в следующем. Нужно анализировать все подслова данного слова, заключенные между всевозможными парами букв из $\{С, П, Л\}$. Эти подслова должны иметь следующую структуру: сначала записаны несколько букв q , затем a_0 или несколько букв 1 , затем снова несколько букв q и, наконец, снова a_0 или несколько единиц.

Таким образом, каждая машина Тьюринга вполне определяет-ся некоторым конечным словом в конечном стандартном алфавите. Поскольку множество всех конечных слов в конечном алфавите счетно, то и всех мыслимых машин Тьюринга (отличающихся друг от друга по существу своей работы) имеется не более чем счетное множество.

Перенумеруем теперь все машины Тьюринга, для чего все слова стандартного алфавита, представляющие собой программы всевозможных машин Тьюринга, расположим в виде фиксированной счетно-бесконечной последовательности, которую составим по такому правилу: сначала выписываются в какой-нибудь фиксированной последовательности все однобуквенные слова: $\alpha_0, \alpha_1, \dots, \alpha_\xi$, представляющие программы машин Тьюринга (множество таких слов конечно, потому что конечен стандартный алфавит, из букв которого строятся слова), затем выписываются все двухбуквенные слова $\alpha_{\xi+1}, \dots, \alpha_\eta$, представляющие программы машин Тьюринга (множество таких слов также конечно, потому что конечен стандартный алфавит), затем выписываются трехбуквенные слова и т. д. Получится последовательность программ $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n, \dots$ всех мыслимых машин Тьюринга. Число k будем называть *номером машины Тьюринга*, если программа этой машины записывается словом α_k .

Существование невычислимых по Тьюрингу функций. Теорема 36.1. *Существует функция, не вычислимая по Тьюрингу, т. е. не вычисляемая ни на одной машине Тьюринга.*

Доказательство. Функции, о которых идет речь, представляют собой функции, заданные и принимающие значения в множестве слов в алфавите $A_1 = \{1\}$. Ясно, что множество слов в алфавите $A_1 = \{1\}$ счетно. Следовательно, рассматривается множество всех функций, заданных на счетном множестве и принимающих значения в счетном же множестве. Как известно, это множество имеет мощность континуума. С другой стороны, поскольку множество всевозможных машин Тьюринга, как мы установили в пре-

дыдущем пункте, перенумеровав их, счетно, это и множество функций, вычислимых по Тьюрингу, также счетно. Континуальная мощность строго больше счетной. Следовательно, существуют функции, не вычислимые по Тьюрингу. $\square$

Доказанная теорема есть чистая теорема существования. Интересно получить пример конкретной функции, не вычислимой по Тьюрингу.

Пример 36.2. Укажем конкретную функцию, которую нельзя вычислить ни на какой машине Тьюринга. На основании тезиса Тьюринга это будет означать, что не существует вообще никакого алгоритма для вычисления значений такой функции.

Рассмотрим следующую функцию $\psi(\alpha)$ на словах в алфавите $A_1 = \{1\}$. Для произвольного слова α длиной n в алфавите $A_1 = \{1\}$ положим: $\psi(\alpha) = \beta_n 1$, если слово α перерабатывается машиной Тьюринга с номером n (см. предыдущий пункт) в слово β_n алфавита $A_1 = \{1\}$; $\psi(\alpha) = 1$ в противном случае. Докажем, что функция $\psi(\alpha)$ не вычислима по Тьюрингу.

Допустим противное. Это означает, что существует машина Тьюринга T со стандартным алфавитом $\{a_0, 1, q, \Pi, \Pi\}$, вычисляющая эту функцию. Пусть k — номер этой машины в нумерации, описанной в предыдущем пункте. Посмотрим, чему равно слово $\psi(1^k)$ (напомним, что $1^k = 11 \dots 1$ — слово из k единиц), являющееся значением функции $\psi(\alpha)$ при $\alpha = 1^k$. Предположим, что машина T перерабатывает слово 1^k в слово β_k в том же алфавите $A_1 = \{1\}$. Тогда по определению вычислимости функции $\psi(\alpha)$ на машине T это означает, что $\psi(1^k) = \beta_k$. Но с другой стороны, по самому определению функции $\psi(\alpha)$ это означает, что $\psi(1^k) = \beta_k 1$. Полученное противоречие доказывает, что машины Тьюринга, вычисляющей функцию $\psi(\alpha)$, не существует. $\square$

Принимая во внимание тезис Тьюринга, заключаем, что не существует вообще никакого алгоритма для вычисления значений функции $\psi(\alpha)$. Это означает, что массовая проблема нахождения значений функции $\psi(\alpha)$ для всевозможных значений аргумента алгоритмически не разрешима.

Проблемы распознавания самоприменимости и применимости. Это еще два примера алгоритмически не разрешимых проблем. Сначала о первой. Предположим, что на ленте машины Тьюринга записана ее собственная функциональная схема в алфавите машины. Если машина применима к такой конфигурации, то будем называть ее самоприменяемой, в противном случае — несамоприменяемой. Возникает массовая проблема распознавания самоприменяемых машин Тьюринга, состоящая в следующем. По заданной функциональной схеме (программе) машины Тьюринга установить, к какому классу относится машина: к классу самоприменимых машин или к классу несамоприменимых машин.

Теорема 36.3. *Проблема распознавания самоприменимых машин Тьюринга алгоритмически не разрешима.*

Доказательство. Допустим противное, т.е. алгоритм для такого распознавания существует. Значит, на основании тезиса Тьюринга, существует машина Тьюринга, реализующая данный алгоритм. Пусть Θ — такая машина. На ее ленту заносится соответствующим образом закодированная программа той или иной машины Тьюринга. При этом, если машина самоприменима, то занесенное слово перерабатывается машиной Θ в какой-то символ σ (имеющий смысл утвердительного ответа на поставленный вопрос о самоприменимости). Если же машина несамоприменима, то занесенное на ленту слово, кодирующее ее программу, перерабатывается машиной Θ в какой-то символ τ (имеющий смысл отрицательного ответа на поставленный вопрос).

Рассмотрим теперь такую машину Тьюринга Θ_1 , которая по-прежнему перерабатывает несамоприменимые коды в τ , а к самоприменимым кодам машина Θ_1 уже не применима. Такая машина получается из машины Θ , если следующим образом слегка изменить ее программу: после появления символа σ вместо остановки машина должна неограниченно его повторять.

Итак, Θ_1 применима ко всякому несамоприменимому коду (вырабатывая символ τ) и не применима к самоприменимым кодам. Это приводит к противоречию, потому что такая машина не может быть ни самоприменимой, ни несамоприменимой. В самом деле, если машина Θ_1 самоприменима, то она не применима к своему коду. Значит, машина несамоприменима. Противоречие. С другой стороны, если машина Θ_1 несамоприменима, то ее код должен перерабатываться самой машиной Θ_1 в символ τ . Значит, Θ_1 применима к собственному коду, т.е. самоприменима. Снова противоречие. Оно и доказывает теорему. $\square$

На основании доказанной теоремы устанавливается алгоритмическая неразрешимость и некоторых других массовых проблем, возникающих в теории машин Тьюринга, например *проблема распознавания применимости для машин Тьюринга*, которая состоит в следующем. Заданы функциональная схема (программа) какой-нибудь машины Тьюринга и конфигурация в ней: узнать, применима ли машина к данной конфигурации или нет.

Теорема 36.4. *Проблема распознавания применимых машин Тьюринга алгоритмически не разрешима.*

Доказательство. Если бы существовал алгоритм для решения этой проблемы, то с его помощью можно было бы узнать, применима ли машина к слову, кодирующему ее собственную программу, т.е. самоприменима ли она. Но на основании предыдущей теоремы известно, что такого алгоритма не существует. $\square$

Алгоритмически неразрешимые проблемы в общей теории алгоритмов. Итак, мы установили алгоритмическую неразрешимость

двух проблем, связанных с машинами Тьюринга: проблема распознавания самоприменимых машин Тьюринга (теорема 36.3) и проблема распознавания применимости для машин Тьюринга (теорема 36.4). Каждое из этих утверждений может быть сформулировано и доказано и в общей теории алгоритмов (в инвариантном виде).

Теорема о неразрешимости проблемы остановки (т.е. проблемы распознавания применимости алгоритма) звучит так. Не существует алгоритма, который по номеру x любого алгоритма (в произвольной, но фиксированной нумерации) и исходным данным y определял бы, остановится алгоритм при этих данных или нет; иначе говоря, не существует алгоритма $B(x, y)$, такого, что для любого алгоритма A_x (с номером $\varphi^{-1}(A) = x$)

$$B(x, y) = \begin{cases} 1, & \text{если } A_x(y) \text{ определен,} \\ 0, & \text{если } A_x(y) \text{ не определен.} \end{cases}$$

Теорему об алгоритмической неразрешимости проблемы самоприменимости алгоритмов можно сформулировать так. Не существует алгоритма $B_1(x)$ такого, что для любого алгоритма A_x

$$B_1(x) = \begin{cases} 1, & \text{если } A_x(x) \text{ определен,} \\ 0, & \text{если } A_x(x) \text{ не определен.} \end{cases}$$

Рассмотрим еще одну алгоритмическую проблему об алгоритмах и докажем ее неразрешимость. Это *проблема определения общерекурсивности алгоритмов (и функций)*, т.е. проблема определения того, *ко всяким ли* допустимым начальным данным применим алгоритм. Прежде докажем лемму.

Лемма 36.5. *Для любого перечисления любого множества Φ всюду определенных вычислимых (т.е. общерекурсивных) функций существует общерекурсивная функция, не входящая в это перечисление.*

Доказательство. Пусть ψ — перечисление множества Φ , порождающее последовательность $A_0, A_1, A_2, \dots$ всюду определенных вычислимых функций. Введем функцию $B(x) = A_x(x) + 1$. Так как A_x общерекурсивна, то и $B(x)$ общерекурсивна. Если предположить, что $B \in \Phi$, то B имеет некоторый номер x_0 и, следовательно, $B(x) = A_{x_0}(x)$. Тогда в точке $x = x_0$ по определению $B(x_0) = A_{x_0}(x_0) + 1$, а в силу последнего соотношения имеем $B(x_0) = A_{x_0}(x_0)$. Получаем противоречие, из которого следует, что B не входит в перечисление, порождаемое ψ .

(Заметим, что если бы в перечислении допускались частичные функции, то такое определение функции B не привело бы к противоречию, а означало бы лишь, что B не определена в точке x_0 .) $\square$

Теорема 36.6. Проблема определения общерекурсивности алгоритмов неразрешима, т. е. не существует алгоритма $B(x)$, такого, что для любого алгоритма A_x

$$B(x) = \begin{cases} 1, & \text{если } A_x \text{ всюду определен,} \\ 0, & \text{если } A_x \text{ не всюду определен.} \end{cases}$$

Доказательство. Допустим противное, т. е. такой алгоритм $B(x)$ существует. Тогда он определяет общерекурсивную функцию $f(x)$. Определим функцию $g(x)$ следующим образом:

$$\begin{aligned} g(0) &= \mu y [f(y) = 1]; \\ g(x+1) &= \mu y [y > g(x) \wedge f(y) = 1]. \end{aligned}$$

Так как номеров всюду определенных функций (и, следовательно, точек y , в которых $f(y) = 1$) бесконечное множество, то функция $g(x)$ всюду определена. Ясно, что функция $g(x)$ принимает значение 1 на каждой всюду определенной вычислимой (т. е. общерекурсивной) функции, т. е. является перечислением множества *всех* общерекурсивных функций. Но, на основании предыдущей леммы, такого перечисления не существует. Противоречие. Следовательно, не существует и алгоритма $B(x)$, определенного в условии теоремы, т. е. проблема определения общерекурсивности алгоритмов неразрешима. $\square$

Раз нельзя указать единого алгоритма, отличающего всюду определенные вычислимые (т. е. общерекурсивные) функции от частично рекурсивных, попытаемся подойти к проблеме частично рекурсивных функций с другой стороны. Может быть, возможно *каждую* частично рекурсивную функцию доопределить на неопределимых точках так, чтобы получилась рекурсивная (т. е. общерекурсивная) функция. Оказывается, и эта задача неразрешима, что следует из теоремы, приведенной ниже.

Теорема 36.7. Существует такая частично рекурсивная функция f , что никакая общерекурсивная функция g не является ее доопределением.

Доказательство. Как и прежде, считаем, что выбрана некоторая вычислимая нумерация $\varphi: N \rightarrow Al^*$ и для каждого алгоритма A_x значение $\varphi^{-1}(A_x) = x$ — его номер в этой нумерации. Рассмотрим следующую частичную функцию:

$$f(x) = \begin{cases} A_x(x) + 1, & \text{если } A_x \text{ определен,} \\ \text{не определена,} & \text{если } A_x \text{ не определен.} \end{cases}$$

Ясно, что функция $f(x)$ вычислима и, значит, частично рекурсивна.

Пусть теперь $g(x)$ — произвольная общерекурсивная функция и x_g — ее номер в нумерации φ , т. е. $\varphi^{-1}(g) = x_g$. Так как g всюду

определена, то $g(x_g) = A_{x_g}(x_g)$ определена и, следовательно, $f(x_g) = g(x_g) + 1$. Таким образом, для любой общерекурсивной функции g имеем $f(x_g) \neq g(x_g)$. Это и означает, что $f \neq g$. Теорема доказана. $\square$

Следовательно, существуют частичные алгоритмы, которые нельзя доопределить до всюду определенных алгоритмов.

Теорема Райса. Эта теорема описывает в рамках общей теории алгоритмов еще один достаточно обширный круг алгоритмически неразрешимых проблем. Рассмотренные ранее подобные проблемы носили довольно экзотический характер: все они были так или иначе связаны с самоприменимостью алгоритма, когда алгоритм работает с собственным описанием (находится значение вычислимой функции f_x в точке, являющейся ее собственным номером в выбранной нумерации вычислимых функций: $f_x(x)$). Теорема Райса, опираясь на неразрешимость этой проблемы, устанавливает алгоритмическую неразрешимость вообще всякого нетривиального свойства вычислимых функций.

По-прежнему имеется некоторая нумерация алгоритмов $\varphi: N \rightarrow A^*$, в которой каждый алгоритм A_x имеет номер $\varphi^{-1}(A_x) = x$. Этот же номер имеет и функция f_x , которую вычисляет алгоритм A_x . (Следует помнить, что одна и та же функция, будучи вычисляема разными алгоритмами, может иметь в данной нумерации много номеров. Но это обстоятельство не влияет на нижеследующую теорему.)

Теорема 36.8 (Райс). Пусть C — любой непустой собственный класс вычислимых функций от одного аргумента (существуют как функции, принадлежащие C , так и вычислимые функции, не принадлежащие C). Тогда не существует алгоритма, который бы по номеру x функции f_x определял бы, принадлежит f_x классу C или нет. Иначе говоря, множество $\{x: f_x \in C\}$ неразрешимо.

Доказательство. Допустим противное, т.е. множество $\{x: f_x \in C\}$ разрешимо. Тогда оно обладает вычислимой характеристической функцией:

$$\chi_M(x) = \begin{cases} 1, & \text{если } x \in M, \text{ т.е. } f_x \in C, \\ 0, & \text{если } x \notin M, \text{ т.е. } f_x \notin C. \end{cases}$$

Пусть f_0 — нигде не определенная функция. Рассмотрим сначала случай, когда $f_0 \notin C$. Выберем тогда какую-нибудь конкретную вычислимую функцию $f_a \in C$ и определим функцию $F(x, y)$:

$$F(x, y) = \begin{cases} f_a(y), & \text{если значение } f_x(x) \text{ определено,} \\ f_0(y), & \text{если значение } f_x(x) \text{ не определено.} \end{cases}$$

Функция $F(x, y)$ вычислима. Для ее вычисления надо вычислять $f_x(x)$: если $f_x(x)$ определена, то этот процесс когда-нибудь остановится и нужно будет перейти к вычислению $f_a(y)$; если же

$f_x(x)$ не определена, то процесс не остановится, что равносильно вычислению функции $f_0(y)$.

Зафиксируем в функции $F(x, y)$ аргумент x . Тогда F станет вычислимой функцией от одного аргумента y . Номер этой функции в единой нумерации φ вычислимых функций зависит от значения x , т. е. является всюду определенной функцией $g(x)$. Ясно, что функция $g(x)$ вычислима, так как является суперпозицией двух вычислимых функций: $g(x) = \varphi^{-1}(F(x, y))$. Таким образом, $F(x, y) = f_{g(x)}(y)$ и, значит,

$$f_{g(x)}(y) = \begin{cases} f_a(y), & \text{если } f_x(x) \text{ определена,} \\ f_0(y), & \text{если } f_x(x) \text{ не определена.} \end{cases}$$

Отсюда ясно, что $f_{g(x)} \in C$ тогда и только тогда, когда $f_{g(x)} = f_a$ (так как $f_a \in C$), т. е. $f_x(x)$ определена. (В случае же, когда $f_x(x)$ не определена, мы имеем $f_{g(x)} = f_0$ и, следовательно, $f_{g(x)} \notin C$, так как $f_0 \notin C$.) Другими словами, $g(x) \in M$ тогда и только тогда, когда $f_x(x)$ определена. Это означает, что характеристическая функция χ_M на аргументах $g(x)$ имеет вид:

$$\chi_M(g(x)) = \begin{cases} 1, & \text{если } f_x(x) \text{ определена,} \\ 0, & \text{если } f_x(x) \text{ не определена.} \end{cases}$$

Последнее означает следующее. Поскольку функции χ_M и g вычислимы, то мы для каждого номера x можем выяснить, определено значение $f_x(x)$ или нет. Это, в свою очередь, означает, что построена разрешающая функция $\chi_M \circ g$ для проблемы самоприменимости алгоритма, что невозможно.

Если рассмотреть случай, когда $f_0 \in C$, то нужно выбрать $f_a \notin C$. Проведя аналогичные рассуждения, придем к следующей разрешающей функции для проблемы самоприменимости $1 - \chi_M(g(x))$, что также противоречит доказанной ранее неразрешимости этой алгоритмической проблемы. Теорема доказана. $\square$

Теорема Райса означает, что не существует единого алгоритма, который для каждой вычислимой функции (по ее номеру) определял бы, обладает эта функция тем или иным свойством или нет, например, является ли эта функция постоянной, монотонной, периодической, ограниченной и т. п. Но это лишь первое приближение к пониманию смысла этой теоремы. Дело в том, что мы пытаемся создать единый алгоритм, который имеет дело с функциями. Но что значит иметь дело с функцией? Функция должна быть как-то задана. В данном случае функция f_x задается вычисляющим ее алгоритмом A_x (мы помним, что каждая функция может вычисляться множеством алгоритмов). Разыскиваемый нами единый алгоритм как раз и имеет дело с алгоритмами, вычисляющими функции. Так вот, смысл теоремы Райса состоит в том, что

по описанию алгоритма, вычисляющего функцию, ничего нельзя узнать о свойствах функции, которую он вычисляет. Еще раз подчеркнем — не существует *единого* алгоритма, применимого к описаниям *всех* вычисляющих алгоритмов.

В частности, оказывается неразрешимой проблема *эквивалентности алгоритмов* (упоминавшаяся нами в § 33): по двум заданным алгоритмам нельзя узнать, вычисляют они одну и ту же функцию или нет.

Каждый, кто имел дело с программированием (написанием компьютерных программ), знает, что по тексту сколько-нибудь сложной программы, не запуская ее в работу, трудно понять, что она делает (какую функцию вычисляет). Если это понимание и приходит, то каждый раз по-своему; единого метода здесь не существует. Это своего рода практическое проявление теоремы Райса.

Мы уже обсуждали проблемы синтаксиса и семантики языка при рассмотрении формальных теорий. В теории алгоритмов появляется еще один аспект этой проблемы. Синтаксические свойства алгоритма — это свойства описывающих его текстов, т.е. свойства конечных слов в фиксированном алфавите. Семантические (или смысловые) свойства алгоритма связаны с тем, что он делает. Хорошо известно, что в процессе отладки программ синтаксические ошибки отыскиваются довольно легко (этому, в частности, способствуют и дополнительные программы-алгоритмы). Главные неприятности связаны именно с анализом семантики неотлаженной программы, т.е. с попытками установить, что же она делает вместо того, чтобы делать то, что мы хотим (и здесь нам уже никакие дополнительные программы помочь не могут). Образно выражаясь, можно сказать, что теорема Райса звучит так: по синтаксису алгоритма ничего нельзя узнать о его семантике.

Другие примеры алгоритмической неразрешимости. В начале § 23 отмечалось, что не существует алгоритма, позволяющего для каждой формулы логики предикатов определить, будет ли формула выполнимой или общезначимой. Это означает, что *массовые проблемы разрешения для общезначимости и выполнимости формул логики предикатов алгоритмически не разрешимы*.

Одной из наиболее знаменитых алгоритмических проблем математики являлась *10-я проблема Гильберта*, поставленная им в числе других в 1901 г. на Международном математическом конгрессе в Париже. Требовалось найти алгоритм, определяющий для любого диафантова уравнения, имеет ли оно целочисленное решение. Диафантово уравнение есть уравнение вида $F(x, y, \dots, z) = 0$, где $F(x, y, \dots, z)$ — многочлен с целыми показателями степеней и с целыми коэффициентами. В общем случае эта проблема долго оставалась нерешенной, и только в 1970 г. советский математик Ю. В. Матиясевич доказал ее неразрешимость.

Существует множество и других алгоритмических проблем, относительно которых установлена их неразрешимость. Среди них ряд алгебраических проблем, приводящих к различным вариантам *проблемы слов*, которые исследовались советскими математиками А. А. Марковым, П. С. Новиковым, А. И. Мальцевым.

В заключение еще раз отметим, что алгоритмическая неразрешимость означает лишь отсутствие единого способа для решения всех единичных задач данной бесконечной серии, в то время как каждая индивидуальная задача серии вполне может быть решена своим индивидуальным способом. Более того, может оказаться разрешимой (своим индивидуальным методом) не только каждая отдельная задача этого класса, но и целые подклассы задач этого класса. Поэтому, если проблема неразрешима в общем случае, нужно искать ее разрешимые частные случаи. Задача в более общей постановке имеет больше шансов оказаться неразрешимой.

Так, несмотря на отсутствие единого алгоритма, позволяющего для каждой формулы логики предикатов определить, является ли она выполнимой или общезначимой, мы в § 21 ответили на этот вопрос применительно к конкретным индивидуальным формулам, а в § 23 сумели даже отыскать алгоритмы решения данной задачи для целых классов формул некоторых специальных видов. Аналогична ситуация с диафантовыми уравнениями. Например, для частного случая диафантова уравнения

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

хорошо известно, что все его целые корни следует искать среди делителей свободного члена a_0 .

В то же время понимание сути проблемы алгоритмической неразрешимости и знание основных алгоритмических неразрешимостей является одним из важных элементов современной математической и логической культуры, особенно для тех, кто имеет профессиональные дела, связанные с компьютерами, программированием и информатикой.

§ 37. Теорема Гёделя о неполноте формальной арифметики

Эта теорема, уже неоднократно встречавшаяся нам, утверждает, что любая непротиворечивая формальная аксиоматическая теория, формализующая арифметику натуральных чисел, не является (абсолютно) полной. В настоящем параграфе дается доказательство этой теоремы, опирающееся на идеи и методы теории алгоритмов. Тем самым будет еще раз продемонстрирована на самом высоком уровне теснейшая связь математической логики и теории алгоритмов — двух математических дисциплин, образующих фундамент всей современной математики. Наше изложение

будет основываться на доказательстве, разработанном М. Арби-
бом [10.1].

После доказательства теоремы 35.7 о том, что существует пересчитываемое, но неразрешимое множество натуральных чисел, было заявлено, что она фактически включает в себя в неявном виде теорему Гёделя о неполноте формальной арифметики. Цель настоящего параграфа состоит в том, чтобы обосновать это заявление. Таким образом, в рамках общей теории алгоритмов, кроме тех теорем, которые были доказаны в двух предыдущих параграфах, будет продемонстрировано продвижение теории алгоритмов в направлении решения чисто логических проблем. Для этого сначала предстоит увязать терминологию логической проблемы о неполноте формальной арифметики с методологической терминологией общей теории алгоритмов, методами которой эта проблема будет решена. При этом утверждение теоремы 35.7 о существовании пересчитываемого, но неразрешимого множества натуральных чисел будет основополагающей предпосылкой для доказательства теоремы Гёделя, которую мы докажем в следующей формулировке: «*Каждая адекватная ω -непротиворечивая формальная арифметика неполна*». Далее, мы поясним, что будем понимать под формальной арифметикой, а также определим и разъясним те понятия, которые участвуют в приведенной формулировке теоремы Гёделя. Начнем с формальных аксиоматических теорий.

Формальные аксиоматические теории и натуральные числа. В § 28, п. 1, определено понятие *формальной аксиоматической теории*. Чтобы задать такую теорию T , нужно задать *алфавит* (счетное множество символов); в множестве всех слов, составленных из букв данного алфавита, выделить подмножество, элементы которого будут называться *формулами* (или правильно построенными выражениями) данной теории; в множестве формул выделить те, которые будут называться *аксиомами* теории; наконец, должно быть задано конечное число отношений между формулами, называемых *правилами вывода*. При этом должны существовать эффективные процедуры (алгоритмы) для определения того, являются ли данные слова (выражения) формулами (т.е. правильно построенными выражениями), являются ли данные формулы аксиомами и, наконец, получается ли одна данная формула из ряда других данных формул с помощью данного правила вывода. Это означает, что множество всех формул разрешимо и множество всех аксиом разрешимо. Следовательно, каждое из этих множеств пересчитываемо.

Понятия *вывода* и *теоремы* в формальной аксиоматической теории даны в определении 28.2.

Все теоремы, приводимые в настоящем параграфе, в соответствии с нашей терминологией являются фактически метатеоре-

мами, т.е. теоремами о свойствах (формальных) аксиоматических теорий. Но поскольку здесь никакой конкретной аксиоматической теории мы не рассматриваем, никаких теорем такой теории не доказываем, т.е. никаких теорем, кроме метатеорем, здесь не будет, то мы метатеоремы будем называть просто теоремами.

Теорема 37.1. *Множество $Th(T)$ всех теорем формальной аксиоматической теории T перечислимо.*

Доказательство. Мы уже отметили, что множество аксиом формальной теории перечислимо, т.е. мы можем их эффективно перенумеровать $A_1, A_2, A_3, \dots$. Поскольку все формулы состоят из конечного числа букв (символов), все выводы содержат конечное число формул и каждый вывод использует лишь конечное число аксиом, то ясно, что для каждого натурального n существует лишь конечное число выводов, имеющих не более чем n формул (шагов) и использующих только аксиомы $\{A_1, A_2, \dots, A_n\}$. Следовательно, двигаясь от $n = 1$ к $n = 2, n = 3$ и т.д., можно эффективно перенумеровать все теоремы данной теории. Это и означает, что множество теорем перечислимо. $\square$

Теперь от произвольных формальных теорий будем переходить к таким, которые так или иначе имеют дело с натуральными числами. Если мы хотим в нашей теории говорить о подмножестве Q множества натуральных чисел, то мы должны иметь эффективный способ выписывания для каждого натурального n формулы W_n , означающей, что $n \in Q$. Более того, если мы сможем доказать, что формула W_n является теоремой теории T тогда и только тогда, когда $n \in Q$, то будем говорить, что теория T *полуполна для Q* (или что в T имеется *полуполное описание Q*). Точнее, это определение сформулируем так.

Определение 37.2. Теория T называется *полуполной для множества натуральных чисел $Q \subseteq N$* , если существует перечислимое множество формул $W_0, W_1, \dots, W_n, \dots$, такое, что $Q = \{n : \vdash W_n\}$.

Определение 37.3. Теория T называется *полной для Q* , если она полуполна для Q и мы также имеем формулу $\neg W_n$, которая интерпретируется как $n \notin Q$, и мы можем доказать, что $\neg W_n$ является теоремой теории T тогда и только тогда, когда $n \notin Q$. Другими словами, теория T *полна для Q* , если в T для каждого n мы можем установить, принадлежит оно Q или нет. Точнее, это означает, что теория T называется *полной для множества натуральных чисел Q* , если она полуполна для Q и полуполна для его дополнения $\bar{Q}$.

Теорема 37.4. *Если теория T полуполна для множества Q , то Q перечислимо.*

Доказательство. По определению полуполноты T для Q множество Q есть множество номеров тех формул из некоторого перечислимого множества $\{W_0, W_1, \dots, W_n, \dots\}$ формул, которые являются теоремами теории T , т.е. принадлежит и множеству $Th(T)$.

Таким образом, Q есть множество номеров всех формул из множества $Th(T) \cap \{W_0, W_1, \dots, W_n, \dots\}$. Каждое из этих пересекаемых множеств перечислимо: первое — по предыдущей теореме 37.1, второе — по сказанному в начале доказательства. Следовательно, и их пересечение, по теореме 35.5, перечислимо. Но тогда перечислимо и множество номеров тех формул, которые входят в это пересечение. $\square$

Следствие 37.5. *Если Q перечислимое, но неразрешимое множество натуральных чисел, то никакая формальная теория не может быть полной для Q .*

Доказательство. Если множество Q перечислимо, но неразрешимо, то в силу теоремы 35.6 его дополнение $\bar{Q}$ неперечислимо. Тогда по теореме 37.4 никакая теория T не является полуполной для Q . Следовательно, никакая теория T неполна для Q . $\square$

От этого следствия до теоремы Гёделя совсем недалеко. Для этого нужно средствами некоторой формальной теории T развить теорию натуральных чисел, причем так, чтобы принадлежность чисел данному множеству Q можно было трактовать адекватно (т. е. число n принадлежит Q тогда и только тогда, когда некоторая эффективно сопоставленная ему формула теории T является теоремой этой теории). Это возможно только тогда, когда Q по меньшей мере перечислимо.

Формальная арифметика и ее свойства. Формальная арифметика как формальная аксиоматическая теория строится на базе формализованного исчисления предикатов, рассмотренного в § 25 и в Задачнике, § 11. Предметные переменные $x_1, x_2, x_3, \dots$ здесь будем называть числовыми, потому что вместо них будем подставлять натуральные числа.

Предметная переменная называется *свободной* в формуле, если она не стоит под знаком квантора (общности или существования), и *связанной* — в противном случае. Формула называется *замкнутой*, если все ее предметные переменные связаны, и *открытой*, если в ней имеются свободные переменные. *Замыканием* формулы F называется формула $C(F)$, получающаяся из F дописыванием спереди кванторов общности по всем переменным, свободным в F . Ясно, что для любой F формула $C(F)$ замкнута. Если F замкнута, то $C(F) = F$.

Функция $C(F)$ вычислима. Отсюда следует, что класс замкнутых формул разрешим, поскольку F ему принадлежит тогда и только тогда, когда $C(F) = F$, и для распознавания этого равенства существует вычислительная процедура.

С понятием подстановки в формулу мы уже знакомы (см. конец § 3). Если в формулу F вместо символа (слова) X везде, где он входит в F , вставить слово (формулу) H , то получим новое слово (формулу), обозначаемое $S_X^H F$ и называемое *результатом подстановки* в F слова H вместо слова X . Тогда ясно, что

$$S_X^H(\neg F) \equiv \neg S_X^H F; S_X^H(F \rightarrow G) \equiv S_X^H F \rightarrow S_X^H G;$$

если $i \neq j$, то $S_{x_i}^N(\forall x_j)(F) \equiv (\forall x_j)S_{x_i}^N F$, $S_{x_i}^N(\exists x_j)(F) \equiv (\exists x_j)S_{x_i}^N F$.

Имея дело с натуральными числами, мы хотели бы иметь возможность подставлять их в формулы формальной теории (арифметики), т.е. иметь возможность говорить о числах на языке нашей формальной теории. Для этой цели в формальной теории необходимо иметь слова, которые служили бы названиями натуральных чисел. Такие слова называются *нумералами*. Нумерал числа n обозначается n^* . Требование к этим названиям (именам) вполне естественное: различные числа должны называться различными именами, т.е. если $m \neq n$, то $m^* \neq n^*$. (Идея введения нумералов состоит в том, чтобы разделить вещи и имена этих вещей.)

Таким образом, в формулы арифметики мы будем подставлять вместо числовых переменных $x_1, x_2, x_3, \dots$ не сами натуральные числа $m, n, k, \dots$, а их нумералы (имена) $m^*, n^*, k^*, \dots$ соответственно.

Наконец, мы можем сформулировать последнее требование (аксиому), которое мы предъявляем к формальной арифметике. Назовем его *аксиомой арифметики*: если предметная переменная x_i не связана в F , то

$$(AA): S_{x_i}^{n^*} F \rightarrow (\exists x_i)(F).$$

Если ввести для $S_{x_i}^{n^*} F$ обозначение $F(n^*)$, то эта аксиома принимает вид:

$$(AA): F(n^*) \rightarrow (\exists x_i)(F).$$

Это исключительно естественное требование: если формула F превращается в истинное высказывание при подстановке в нее вместо переменной x_i какого-нибудь натурального числа n^* , то истинно и высказывание $(\exists x_i)(F)$.

Никаких других ограничений на формализацию арифметики не накладывается. Неважно, в частности, как определяются сложение и умножение натуральных чисел, как вводится отношение порядка, чем мы скрупулезно занимались при построении теории натуральных чисел на основе системы аксиом Пеано. Даже при таких самых общих допущениях на формализацию арифметики эта формализация будет подчиняться теореме Гёделя: если она будет непротиворечива, то она будет неполной.

Итак, определившись с понятием формальной арифметики, посвятим оставшуюся часть этого пункта понятиям ω -непротиворечивости, адекватности и полноты этой формальной теории, участвующим в точной формулировке теоремы Гёделя.

Начнем с понятия непротиворечивости. Как и всякая аксиоматическая теория, формальная арифметика называется *непротиворечивой*, если в ней нельзя доказать какое-либо утверждение и его отрицание, т.е. если не существует такой формулы F , что одновременно $\vdash F$ и $\vdash \neg F$.

Предположим теперь, что для некоторой формулы $G(x)$, содержащей свободно единственную предметную переменную x , установлено, что $\vdash G(n^*)$ для всех натуральных чисел $n = 0, 1, 2, 3, \dots$. Даже если в формальной арифметике невозможно доказать $\vdash (\forall x)(G(x))$, мы конечно же можем считать это утверждение следствием приведенного списка теорем. Следовательно, если в теории удастся доказать теорему $\vdash \neg(\forall x)(G(x))$, то такую формальную арифметику следует считать противоречивой.

Определение 37.6. Формальная арифметика называется ω -*непротиворечивой*, если в ней нет такой формулы $G(x)$ с единственной свободной предметной переменной x , что для всех натуральных чисел n справедливы теоремы $\vdash G(n^*)$ и $\vdash \neg(\forall x)(G(x))$.

Теорема 37.7. Если формальная арифметика ω -непротиворечива, то она непротиворечива.

Доказательство. В самом деле, если бы она была противоречива, то, как доказано в § 27, после определения 27.1, все ее формулы были бы теоремами, в том числе и те, которые создают ω -противоречивость формальной арифметики, и последняя была бы ω -противоречива. $\square$

Определение 37.8. Назовем n -местный предикат $P(x_1, \dots, x_n)$ над множеством натуральных чисел N *вполне представимым в формальной арифметике*, если существует такая формула $F(x_1, \dots, x_n)$, свободными предметными переменными которой являются n переменных $x_1, \dots, x_n$ (и только они), что: *a)* для каждого набора n натуральных чисел $(a_1, \dots, a_n)$, для которого предикат P превращается в истинное высказывание $P(a_1, \dots, a_n)$, имеет место теорема: $\vdash F(a_1^*, \dots, a_n^*)$; *б)* для каждого набора n натуральных чисел $(a_1, \dots, a_n)$, для которого предикат P превращается в ложное высказывание $P(a_1, \dots, a_n)$, имеет место теорема: $\vdash \neg F(a_1^*, \dots, a_n^*)$.

Таким образом, вполне представимость предиката в формальной арифметике означает, что мы средствами этой формальной теории всегда можем решить, превратится он в истинное или ложное высказывание при подстановке вместо всех его предметных переменных тех или иных натуральных чисел.

Разъясним теперь понятие адекватности формальной арифметики, участвующее в формулировке теоремы Гёделя. Мы хотели бы иметь возможность отвечать на вопросы о перечислимых множествах в такой арифметике. В теореме 37.4 мы показали, что лишь перечислимые множества чисел могут иметь полуполное описание в формальной теории, т.е. существует перечислимое множество формул $W_0, W_1, W_2, \dots$, такое, что $Q = \{n : \vdash W_n\}$. Адекватность нашей формальной теории (арифметики) могла бы означать, что она является полуполной для каждого перечислимого множества натуральных чисел, т.е. что в ней имеет полуполное описание всякое множество, которое вообще может иметь такое описание хотя бы в какой-нибудь теории.

В теореме 37.1 мы установили, что множество всех теорем формальной теории перечислимо, т.е. все теоремы и, значит, приводящие к ним выводы (доказательства) могут быть эффективно перенумерованы. Возьмем наше множество Q и соответствующее ему множество теорем $\{W_0, W_1, W_2, \dots\}$. Рассмотрим следующий предикат $P(x, y)$: « y — номер доказательства теоремы W_x ». Если высказывание $P(m, n)$ истинно, то это означает, что n есть номер вывода теоремы W_m , что, в свою очередь, означает, что $m \in Q$, т.е. n есть номер вывода о том, что $m \in Q$. Обратно, взяв конкретные числа m и n , мы можем эффективно построить теорему (формулу) W_m и эффективно построить n -й вывод, после чего эффективно определить, является ли построенный вывод выводом теоремы W_m , т.е. эффективно узнать, истинно ли высказывание $P(m, n)$. Следовательно, $P(x, y)$ — такой вычислимый предикат, что $Q = \{x : (\exists y)(\lambda[P(x, y)] = 1)\}$.

Сформулируем теперь определение.

Определение 37.9. Формальная арифметика называется *адекватной*, если для каждого перечислимого множества Q натуральных чисел существует вполне представимый в этой арифметике предикат $P(x, y)$ такой, что $Q = \{x : (\exists y)(\lambda[P(x, y)] = 1)\}$.

Под *полнотой* формальной арифметики будем понимать абсолютную полноту, т.е. если для каждой замкнутой формулы F этой теории либо она сама, либо ее отрицание является теоремой этой теории: $\vdash F$ или $\vdash \neg F$.

Теперь мы можем перейти непосредственно к формулировке и доказательству теоремы Гёделя.

Теорема Гёделя о неполноте. Теорема утверждает следующее.

Всякая ω -непротиворечивая и адекватная формальная арифметика не является полной.

Доказательство. Согласно теореме 35.7, выберем такое множество Q натуральных чисел, которое перечислимо, но неразрешимо. Так как наша формальная арифметика адекватна, то существует вполне представимый в ней предикат $P(x, y)$ такой, что

$$Q = \{x : (\exists y)(\lambda[P(x, y)] = 1)\}. \quad (*)$$

Вполне представимость предиката $P(x, y)$ в формальной арифметике означает, что найдется такая формула $F(x, y)$ этой теории, содержащая лишь две свободных предметных переменных, что для каждой пары натуральных чисел (a, b) , для которой $\lambda[P(a, b)] = 1$, имеет место теорема: $\vdash F(a^*, b^*)$, а для каждой пары натуральных чисел (a, b) , для которой $\lambda[P(a, b)] = 0$, имеет место теорема: $\vdash \neg F(a^*, b^*)$.

Применим к формуле $F(x, y)$ квантор общности по переменной y . Получим формулу с единственной свободной предметной переменной x : $G(x) \equiv (\exists y)(F(x, y))$. Покажем, что

$$Q = \{x : \vdash G(x^*)\}. \quad (**)$$

Предположим, что $m \in Q$. Тогда (согласно (*)) найдется такое натуральное n , что высказывание $P(m, n)$ истинно. Следовательно, имеет место теорема: $\vdash F(m^*, n^*)$. В силу аксиомы арифметики (AA) имеем теорему:

$$\vdash F(m^*, n^*) \rightarrow (\exists y)(F(m^*, y)).$$

Из двух последних теорем по правилу МР заключаем:

$$\vdash (\exists y)(F(m^*, y)), \text{ т.е. } \vdash G(m^*).$$

Это означает, что $m \in \{x : \vdash G(x^*)\}$. Таким образом, $Q \subseteq \{x : \vdash G(x^*)\}$.

Обратно, предположим, что $m \in \{x : \vdash G(x^*)\}$, т.е. $\vdash G(m^*)$, т.е. $\vdash (\exists y)(F(m^*, y))$. Отсюда, в силу известного выражения (по закону де Моргана) квантора существования через квантор общности, заключаем, что

$$\vdash \neg(\forall y)(\neg F(m^*, y)).$$

Поскольку наша формальная арифметика, кроме того, ω -непротиворечива, то, ввиду наличия в ней последней теоремы, должно существовать такое натуральное число n_0 , что формула $\neg F(m^*, n_0^*)$ не является теоремой этой арифметики. А раз так, то высказывание $P(m, n_0)$ истинно (если бы оно было ложно, то мы имели бы теорему $\vdash \neg F(m^*, n_0^*)$, что не так). По определению (*) множества Q , это означает, что $m \in Q$. Таким образом, $\{x : \vdash G(x^*)\} \subseteq Q$. Итак, равенство (**) доказано.

Теперь выясним, в каком отношении находятся между собой множества $\bar{Q}$ (дополнение Q) и $\{x : \vdash \neg G(x^*)\}$. Пусть $m \in \{x : \vdash \neg G(x^*)\}$, т.е. $\vdash \neg G(m^*)$. Тогда $m \in \bar{Q}$, ибо если бы $m \in Q$, то в силу (**) мы имели бы $\vdash G(m^*)$ и наша формальная арифметика была бы противоречивой, но это не так в силу ее ω -непротиворечивости (по условию) и теоремы 37.7. Таким образом, $\{x : \vdash \neg G(x^*)\} \subseteq \bar{Q}$.

Покажем, что последнее включение является строгим. Напомним, что мы выбрали множество Q перечислимым, но не являющимся разрешимым. Тогда согласно следствию 37.5 из теоремы 37.4, никакая формальная теория не может быть полной для Q . Равенство (**) говорит, что наша формальная арифметика полуполна для Q . Если бы имело место равенство $\bar{Q} = \{x : \vdash \neg G(x^*)\}$, то это означало бы, что наша формальная арифметика полуполна и для $\bar{Q}$ и, значит, она была бы полной для Q . Последнее невозможно в силу следствия 37.5 из теоремы 37.4. Следовательно, $\{x : \vdash \neg G(x^*)\} \neq \bar{Q}$.

Итак, $\{x : \vdash \neg G(x^*)\} \subset \bar{Q}$. Следовательно, существует такое число $m_0 \in \bar{Q}$, что $m_0 \notin \{x : \vdash \neg G(x^*)\}$, т.е. неверно, что $\vdash \neg G(m_0^*)$. В то же время неверно также, что $\vdash G(m_0^*)$, поскольку это, в силу (**),

означало бы, что $m_0 \in Q$, а это не так. Следовательно, мы нашли формулу $G(m_0^*)$, такую, что ни она сама, ни ее отрицание $\neg G(m_0^*)$ не являются теоремами нашей формальной арифметики. Это и означает, что данная формальная арифметика не является полной.

Теорема Гёделя полностью доказана. $\square$

Обратимся еще раз к высказыванию $\neg G(m_0^*)$. Согласно равенству (**), его можно интерпретировать как $m_0 \in Q$ и, следовательно, оно обязательно является «истинным» высказыванием. Но тем не менее оно не является теоремой нашей формальной арифметики. Если добавить формулу $G(m_0^*)$ к списку аксиом и рассмотреть новую формальную арифметику, то положение не изменится: для вновь полученной формальной арифметики верны все те предпосылки, которые привели нас к теореме Гёделя. Значит, мы снова найдем такое число m_1 , что высказывание $\neg G(m_1^*)$ истинно, но не является теоремой новой формальной арифметики и т.д.

Гёдель и его роль в математической логике XX в. Курт Гёдель родился 28 апреля 1906 г. в г. Брюнне (ныне г. Брно в Чехии). Окончил Венский университет, где защитил докторскую диссертацию и был доцентом в период 1933—1938 гг. После оккупации Австрии фашистской Германией эмигрировал в США. С 1940 по 1963 г. Гёдель работает в Принстонском институте высших исследований (с 1953 г. он профессор этого института). Гёдель — почетный доктор Йельского и Гарвардского университетов, член Национальной академии наук США и Американского философского общества. В 1951 г. Гёдель удостоен высшей научной награды США — Эйнштейновской премии. В статье, посвященной этому событию, другой крупнейший математик нашего времени Джон фон Нейман писал: «Вклад Курта Гёделя в современную логику поистине монументален. Это — больше, чем просто монумент, это веха, разделяющая две эпохи... Без всякого преувеличения можно сказать, что работы Гёделя коренным образом изменили сам предмет логики как науки». Гёдель заложил основы целых разделов математической логики: теории моделей (1930), конструктивной логики (1932—1933), формальной арифметики (1932—1933), теории алгоритмов и рекурсивных функций (1934), аксиоматической теории множеств (1938). Гёдель умер в Принстоне (США) 14 января 1978 г.

МАТЕМАТИЧЕСКАЯ ЛОГИКА И КОМПЬЮТЕРЫ, ИНФОРМАТИКА, ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Образно выражаясь, можно сказать, что компьютер состоит из материальной части и математического (программного) обеспечения, или, используя профессиональную лексику, из «железа» и «обуви». И к тому, и к другому имеет самое непосредственное отношение математическая логика, ни первое, ни второе без математической логики обойтись не могут. В § 12 и 13 было рассмотрено применение математической логики к релейно-контактным (переключательным) схемам, являющимся неотъемлемой составной частью современного компьютера. Часть настоящей главы также посвящена вопросам взаимодействия математической логики и компьютеров. Так, в § 38 рассказывается о применении математической логики к языкам программирования и к самому процессу программирования и получающимся в результате этого программам. В § 39 дается характеристика обратного процесса — применению компьютеров для поиска доказательств теорем математической логики и других математических дисциплин. Значительное внимание уделено методу резолюций для доказательства теорем в исчислениях высказываний и предикатов. В § 40 кратко описывается язык ПРОЛОГ — принципиально новый язык программирования, выросший непосредственно из математической логики (логики предикатов) и призванный стать языком компьютеров пятого поколения.

В свою очередь, информатика как наука начала оформляться вместе с созданием и бурным развитием вычислительной техники. Ее формирование и определение ее предмета продолжают по настоящее время. Информатика — наука о хранении, обработке и передаче информации с помощью компьютеров. Она включает в себя крупные разделы, изучающие алгоритмические, программные и технические средства хранения, обработки и передачи информации. Математическая логика оказалась единственной математической наукой, методы которой стали мощнейшими инструментами познания во всех разделах информатики. Поэтому сколько-нибудь серьезное изучение информатики немыслимо без освоения основ математической логики.

Вторая часть настоящего раздела посвящена тем вопросам математической логики, которые находят наиболее яркое применение

ние в информатике, а также краткому показу того, как математическая логика работает в некоторых разделах информатики. Здесь будет рассказано о применении математической логики при исследованиях, посвященных базам данных, базам знаний (§ 41) и системам искусственного интеллекта (§ 42).

§ 38. Математическая логика и программное обеспечение компьютеров

Чтобы компьютер работал, он должен быть оснащен программным обеспечением, т.е. комплексом программ, ориентирующих компьютер на решение задач того или иного класса. (Слово «программа» имеет греческое происхождение и означает «объявление», «распоряжение».) Уже само понятие компьютерной программы, предусматривающее четкое алгоритмическое предписание компьютеру о порядке и характере действий, предусматривает проникновение в программу, а также в процесс ее составления (в программирование) теории алгоритмов. Но при более пристальном рассмотрении процесс проникновения логики в программы и программирование оказывается значительно более глубоким и органичным. Не только один ее раздел — теория алгоритмов — работает здесь, но исключительно действенным оказывается само существо математической логики — ее язык, ее аксиоматические теории, выводы и теоремы в них, свойства этих теорий.

В данном параграфе дается краткий обзор основных направлений, по которым математическая логика внедряется в программирование, из которых программирование возникло и без которых существовать не может.

Теория алгоритмов и математическая логика — фундаментальная основа программирования. В 30-е гг. XIX в. английский математик Чарлз Бэббедж высказал впервые идею вычислительной машины. И только сто лет спустя логики разработали четыре математически эквивалентные модели понятия алгоритма (мы достаточно подробно рассмотрели в предыдущей главе три из них). Именно в теории алгоритмов были предугаданы основные концепции, которые легли в основу принципов построения и функционирования вычислительной машины с программным управлением и принципов создания языков программирования. Идею такой вычислительной машины впервые смогли реализовать болгарский ученый С. Атанасов в 1940 г. и немецкий ученый К. Цузе в 1942 г. Четыре главные модели алгоритма породили разные направления в программировании.

Первая модель — это *абстрактная вычислительная машина* (А. Тьюринг, Р. Пост). Она явилась абстрактным прообразом реальных вычислительных машин. До сих пор все вычислительные

машины в некотором смысле базируются на идее Тьюринга: их память физически состоит из битов, каждый из которых содержит либо 0, либо 1. Программное управление унаследовало от этих абстрактных машин и программу, помещенную в «постоянную память» (идея поместить программу ЭВМ в основную память, чтобы иметь возможность изменять ее в ходе вычислений, принадлежит Джону фон Нейману), а структура команды современной ЭВМ в значительной степени напоминает структуру команды машины Тьюринга. В рамках теории машин Тьюринга откристаллизовались важнейшие для компьютерных приложений логики понятия: вычислимая функция, разрешимая задача, неразрешимая (алгоритмически) задача. В [9.15] собрано большое количество определений абстрактных вычислительных машин и показано, как каждое из них можно свести к другому подходящей кодировкой входов и выходов.

Другая модель — это *рекурсивные функции*, идея которых восходит к гильбертовскому аксиоматическому подходу. От них унаследовало свои основные конструкции современное структурное программирование.

Третий способ описания алгоритмов — *нормальные алгоритмы А.А. Маркова*. Они послужили основой языка Рефал и многих других языков обработки символьной информации.

Четвертое направление в теории алгоритмов — так называемое *λ -исчисление* — базируется на идеях советского логика Р. Шейнфинкеля и американского логика Х. Б. Карри. Оказалось, что для определения всех вычислимых функций достаточно операций так называемой λ -абстракции и суперпозиции. Идеи λ -исчисления активно развиваются в языке Лисп, функциональном программировании и во многих других перспективных направлениях современного программирования.

Математическая логика стала бурно развиваться в начале XX в. на почве казалось бы исключительно далекой от приложений проблемы обоснования математики. Но именно эти исследования положили начало строгому определению алгоритмических языков, показали их колоссальные возможности и принципиальные ограничения, развили технику формализации. Поэтому, когда в программировании было осознано, что всякая программа есть формализация, то возникшие здесь математические проблемы упали на почву, тщательно подготовленную математической логикой.

Описание компьютерных программ с помощью математической логики. Первые попытки применить в программировании развитые логические исчисления и методы формализации предпринял американский логик Х. Б. Карри. В 1952 г. он сделал доклад «Логика программных композиций», идеи которого опередили свое время по крайней мере на четверть века. Карри рассмотрел задачу программирования как задачу составления более крупных программ из

готовых кусков. Были введены две базисные системы конструкций: первая — последовательное исполнение, разветвление и цикл, вторая — последовательное исполнение и условный переход. Он охарактеризовал логические средства, какие можно использовать для композиции программ из подпрограмм в каждом из этих случаев.

Как известно, компьютер является своего рода «идеальным бюрократом»: он не воспримет программу, написанную на не до конца формализованном языке, и приступит к работе лишь после того, как все выражено в полном соответствии с детальными инструкциями. Поэтому в 1960-е гг. на первый план вышли задачи точного определения формальных языков достаточно сложной структуры. Математическая логика, подпитываемая идеями программирования, успешно с ними справилась, разработав описание синтаксиса сложных и богатых по выразительным средствам формальных языков.

В середине 1960-х гг. практически одновременно появился ряд пионерских работ в области описания условий, которым удовлетворяет программа. Советский математик В. М. Глушков в 1965 г. ввел понятие алгоритмической алгебры, послужившее прообразом алгоритмических логик. Ф. Энгелер в 1967 г. предложил использовать языки с бесконечно длинными формулами, чтобы выразить бесконечное множество возможностей, возникающих при разных исполнениях программы. Но наибольшую популярность приобрели языки алгоритмических логик. Эти языки были изобретены практически одновременно американскими логиками Р. У. Флоридом (1967), С. А. Р. Хоаром (1969) и учеными польской логической школы, например А. Сальвицким и др. (1970).

Алгоритмическая логика (или динамическая логика, или программная логика, или логика Хоара) — раздел теоретического программирования, в рамках которого исследуются аксиоматические системы, представляющие средства для задания синтаксиса и семантики языков программирования, а также для синтеза компьютерных программ и их верификации (проверки правильности работы). Языки алгоритмических логик основываются на логике предикатов 1-го порядка и включают в себя высказывания вида $\{A\}S\{B\}$, читающиеся следующим образом: «Если до исполнения оператора S было выполнено A , то после него будет выполнено B ». Здесь A называется *предусловием*, B — *постусловием*, либо *обещанием* S . На этом языке даются логические описания операторов присвоения и условного перехода, ветвления, цикла.

Наряду с динамической логикой 1-го порядка рассматривается *пропозициональная динамическая логика* и ее обобщение — так называемая логика процессов, в которой выразимы некоторые свойства программы, зависящие от процесса ее выполнения. Различные динамические логики получаются при варьировании средств языков программирования, используемых в программах. Эти сред-

ства содержат массивы и другие структуры данных, рекурсивные процедуры, циклические конструкции, а также средства задания недетерминированных программ.

Динамическая логика является одним из типов логических систем, используемых для логического синтеза компьютерных программ. *Логический синтез* — один из способов перехода от спецификации программы к реализующему алгоритму, имеющий форму точного рассуждения в некоторой логической системе. В динамической логике спецификация задачи задается в виде двух формул исчисления предикатов — предусловия и постусловия, а аксиомами логической системы являются схемы предусловий и постусловий, связываемых теми или иными конструкциями языка программирования. Синтезируемая программа получается в форме выводимого в динамической логике утверждения, гласящего, что если аргументы задачи удовлетворяют заданному предусловию, то результат выполнения синтезированной программы удовлетворяет заданному постусловию.

В теоретических работах по динамическим логикам исследуются вопросы непротиворечивости и полноты аксиоматических систем, алгоритмические сложностные свойства множеств истинных формул, сравнения выразительной мощности языков динамической логики.

Принципиально иной способ определения семантики программ, пригодный скорее для описания всего алгоритмического языка, а не конкретных программ, предложил в 1970 г. американский логик Д. Скотт. Он построил математическую модель λ -исчисления и показал, как переводить функциональное описание языка структурного программирования в λ -исчисление и как определить математическую модель алгоритмического языка через модель λ -исчисления. Эта так называемая денотационная семантика алгоритмических языков, работы по которой насчитываются уже тысячами, стала практическим инструментом построения надежных трансляторов со сложных алгоритмических языков. Так еще одна абстрактная область математической логики нашла прямые практические приложения.

Описание программирования и анализ его концепций с помощью математической логики. *Программирование* — это процесс составления программы, плана действий. Было замечено, что классическая логика плохо подходит для описания этого процесса хотя бы потому, что она плохо подходит вообще для описания всякого *процесса* в математике. Еще в начале XX в. стало ясно, что в математике давно разошлись понятия «существовать» и «быть построенным», с античных времен трактовавшиеся как синонимы. Были выявлены так называемые математические объекты-«привидения» (множества, функции, числа), существование которых доказано, но построить которые нельзя. Причиной их появления явился эффект соче-

тания классической логики с теоремой Гёделя о неполноте формальной арифметики. Один из фундаментальных законов классической логики — закон исключенного третьего $P \vee \neg P$ в некоторой свободной трактовке фактически означает, что мы знаем все. Этот постулат конечно же никак нельзя назвать реалистическим: мы знаем чрезвычайно мало, и чем больше узнаем, тем лучше это понимаем. Голландский математик Л. Э. Я. Брауэр определил логические корни «привидений» еще до открытия теоремы Гёделя, в 1908 г., и начал построение так называемой интуиционистской математики, не принимающей закон $P \vee \neg P$ как универсальный. В 1930—1932 гг. другой голландец А. Гейтинг строго сформулировал логику, которой пользовались в интуиционистской математике, — интуиционистскую логику. Ее математическая интерпретация, данная советским математиком А. Н. Колмогоровым в то же время, сохранила свое значение до сих пор.

А. Н. Колмогоров рассмотрел логику как исчисление задач. Каждая формула алгебры высказываний рассматривается не просто как формула, но как требование решить задачу, т.е. построить объект, удовлетворяющий некоторым условиям. Это так называемая конструктивная интерпретация логики высказываний. Логические связки понимаются как средства построения формулировок более сложных задач из более простых, аксиомы — как задачи, решения которых даны, правила вывода — как способы преобразования решений одних задач в решения других. Отметим, что решение задачи — это не только сам искомый объект, но и доказательство того, что он удовлетворяет предъявляемым требованиям. Например, формула $A \wedge B$ понимается в колмогоровской интерпретации как задача, состоящая в том, чтобы построить и решение задачи A , и решение задачи B , правило вывода $A, B / A \wedge B$ — как преобразование, строящее из объекта a , решающего задачу A , и объекта b , решающего задачу B , пару (a, b) , решающую задачу $A \wedge B$. Объект a , решающий задачу, сопоставленную формуле A , называется реализацией A . Этот факт обозначается aRA . Центральным моментом конструктивного понимания логических формул является интерпретация импликации. Конструктивная импликация $A \Rightarrow B$ понимается как требование построить эффективное преобразование f , применимое ко всем реализациям формулы A и переводящее их в реализации формулы B .

Нечеткая колмогоровская формулировка логики как исчисления задач породила многочисленные различные конкретизации, дав целую систему точных математических определений. Эта формулировка нашла применение не только в интуиционистской логике, для которой она была создана, но и в других логических системах. Строгие математические семантики, основанные на идее Колмогорова, обычно называют семантиками реализуемости (в отличие от других видов логических семантик, которые базируют-

ся на системах истинностных значений). Первую реализуемость построил американский логик С. К. Клини в 1940 г. для арифметики с интуиционистской логикой. В 1960 — 1980-х гг. появились десятки понятий реализуемости как для систем, базирующихся на интуиционистской логике, так и для других логик. Советский логик А. А. Воронков в 1985 г. вывел условия, при которых классическая логика может рассматриваться как конструктивная. Из них, в частности, следует, что необходимым (но не достаточным) условием конструктивности классической теории является ее полнота, т. е. выводимость в ней для каждой замкнутой формулы F либо самой F , либо ее отрицания $\neg F$. (Тем самым еще раз подтвердилось прозрение Брауэра относительно логических корней неконструктивности.) Заметим, что примерами классических теорий, имеющих конструктивное истолкование, служат элементарная геометрия и алгебраическая теория вещественных чисел.

Описание программирования с помощью логики основано на определенной аналогии между выводом формулы в некотором логическом исчислении и программой решения задачи, отвечающей этой формуле при конструктивной интерпретации логики. Логическая теория, соответствующая структурным схемам программ, появилась в середине 1980-х гг. Структурные схемы соответствовали нарождающемуся новому типу логики — логики схем программ, которой пользуется программист для создания сложных, многовариантных, итеративных планов действий.

Имеется корректная и полная система конструктивных правил вывода (логика Ω_1), позволяющих при помощи некоторой структурной схемы построить доказательство возможности преобразовать A в B на базе заданных функций, преобразующих некоторые A_i в B_i :

$$\frac{A \Rightarrow B, C \Rightarrow D}{A \vee C \Rightarrow B \vee D} \text{ — правило условного оператора (ПУО);}$$

$$\frac{A \rightarrow B, B \Rightarrow C, C \rightarrow D}{A \Rightarrow D} \text{ — правило релаксации (ПР);}$$

$$\frac{A \vee C \Rightarrow B \vee C}{A \Rightarrow B} \text{ — правило заикливания (ПЗ);}$$

$$\frac{A \Rightarrow A}{\neg A} \text{ — правило бесконечного цикла (ПБЦ);}$$

$$\frac{\neg A}{A \Rightarrow A} \text{ — правило ошибки (ПО).}$$

Все перечисленные правила имеют конструктивное истолкование. Для ПУО и ПЗ оно видно из их названий. В ПУО A и B — охраны создаваемого условного оператора, в ПЗ C — инвариант создаваемого цикла, B — условие его завершения. ПР не преобразует, оно лишь говорит о том, что то же f можно использовать и в более частной ситуации, чем $A \Rightarrow B$. ПБЦ утверждает, что застой не может быть вечен. ПО постулирует существование нигде не определенной функции «ошибка».

Таким образом, конструктивное описание ситуации, где классические средства работают плохо, оказалось весьма компактным и эффективным.

Логика Ω_1 — лишь одна из простейших логик схем программ, успешно используемых в автоматизированном планировании действий.

Интуиционистская логика из конструктивных логик с точки зрения синтаксиса оказалась наиболее близкой к традиционной логике. Она полностью сохранила язык исчисления предикатов и логические связки классической логики (вложив в них свой, конструктивный, смысл). Она по возможности сохранила и правила классической логики постольку, поскольку они не влекут закона исключенного третьего $P \vee \neg P$ (принципа всезнания в конструктивной интерпретации) или закона двойного отрицания $\neg\neg P \Rightarrow P$. Этот закон, как выяснил Брауэр, влечет принцип всезнания, а сам конструктивно может быть истолкован как существование Общего Решателя Задач (такой же нонсенс, как вечный двигатель).

Задача построения программы выражается в интуиционистской логике с помощью функциональной формулы:

$$(\forall x)[A_1 \wedge \dots \wedge A_n \Rightarrow (\exists y)(B_1 \wedge \dots \wedge B_k)].$$

Здесь x — входные переменные создаваемой программы; y — ее результаты; B_i задают связи вход-выход; A_i амбивалентны: они могут представлять как условия на входы, так и входные значения сложных типов (структуры данных, функции-параметры). Например, формула

$$(\forall x)[x \geq 0 \Rightarrow (\exists y)(y \geq 0 \wedge y^2 = x)]$$

интерпретируется как задача построения программы вычисления квадратного корня из x , а формула

$$(\forall x, y)[x < y \wedge (\forall z)(x \leq z \wedge z \leq y \Rightarrow (\exists u)(M(z, u))) \Rightarrow (\exists v)(\forall z, u)(x \leq z \wedge z \leq y \wedge M(z, u) \Rightarrow u < v)]$$

может трактоваться как задача построения оператора, ставящего в соответствие функции, определенной на $[x, y]$ и перерабатывающей z в u , ее верхнюю границу.

Из-за отсутствия принципа всезнания выразительные возможности интуиционистской логики существенно повышаются по сравне-

нию с классической. На ее языке можно постулировать не только знание, но порой и незнание. Например, то, что значение действительного числа не может быть задано точно, постулируется в форме

$$\neg(\forall x, y)(x > y \vee y > x \vee x = y).$$

Но повышение выразительной силы и «аккуратности» выводов в интуиционистской логике по сравнению с классической имеет и обратную сторону: поиск вывода в ней существенно сложнее. В частности, метод резолюций (см. § 39) в ней неприменим, потому что формулы не могут быть разложены на дизъюнкты.

Интуиционистская логика хорошо подходит для описания задач, в которых требуется вычислить новые величины по заданным величинам и ни один из вычислительных ресурсов (время, память, надежность) не налагает ограничений. Для других ситуаций интуиционистскую логику приходится варьировать.

Впервые на возможности логики в качестве инструмента анализа понятий программирования обратили внимание в середине 1970-х гг. в связи с развитием теории верификации (проверки правильности) программ. Оказалось, что для многих конструкций программирования, совместное использование которых не приводит к алгоритмической невычислимости, невозможно построить полную формальную систему, описывающую их взаимодействие. Например, рассмотрение логики схем программ позволило установить, что операторы GO TO естественно получаются в том случае, если все рассматриваемые действия можно считать глобальными преобразованиями состояния системы. Циклы оказались хорошо совместимы с массивами и плохо — с рекурсивными структурами данных, а процедуры высших типов — наоборот. Массивы и сложные структуры данных плохо совместимы с присваиваниями (в данном случае присваивание дается на целый ряд операторов, несущих различный логический смысл).

В общем, можно сделать вывод, что нет средств программирования хороших либо плохих самих по себе; хороши или плохи их комбинации. При этом любая логически разумная комбинация оказывается неуниверсальной, она приспособлена лишь для определенного класса задач.

Верификация (доказательство правильности) программ с помощью математической логики. Широчайшее использование компьютеров в самых разнообразных сферах человеческой деятельности выдвигает на одно из первых мест *вопрос о надежности программного обеспечения компьютеров*. Как известно, правильность созданной программы обычно проверяется на ряде так называемых тестовых примеров, на начальных данных, для которых результат известен или его можно предсказать. Нетрудно понять, что такая проверка способна лишь выявить наличие ошибок в программе, но не доказать их отсутствие, что, разумеется, не одно и то же.

Поэтому исключительно важна задача строгого доказательства правильности программ, и именно для этой цели и начали разрабатываться программные и динамические логики.

С интуиционистской точки зрения программа будет правильной, если в результате ее выполнения будет достигнут тот результат, с целью получения которого и была написана программа. (Обратите внимание, что мы не рассматриваем программы, содержащие синтаксические ошибки, т. е. предполагаем, что с точки зрения языка программирования программа написана безупречно.) Доказательство правильности программы состоит в предъявлении такой цепочки аргументов, которые убедительно свидетельствуют о том, что это действительно так, т. е. что программа на самом деле решает поставленную задачу.

Сформулируем теперь точное *определение понятия правильности программы*. Пусть α — программа, P — утверждение, относящееся к входным данным, которое должно быть истинно перед выполнением программы α (оно называется *предусловием* программы α), Q — утверждение, которое должно быть истинно после выполнения программы α (оно называется *постусловием* программы α). Различают два вида правильности программ: *частичную* и *тотальную* (полную). Программа α называется *частично правильной* относительно условия P и постусловия Q , если всякий раз, когда перед выполнением α условие P истинно для входных значений переменных и α завершает работу, постусловие Q также будет истинно для выходных значений переменных. В этом случае будем использовать запись $P[\alpha]Q$. Программа α называется *тотально правильной* относительно P и Q , если она частично правильна относительно P и Q и α обязательно завершает свою работу для входных значений переменных, удовлетворяющих условию P . В этом случае пишем $P[\alpha!]Q$.

Обратим внимание на то, что понятие правильности программы α сформулировано относительно соответствующих утверждений (условий) P и Q . Поэтому из истинности утверждения $P[\alpha]Q$ (или $P[\alpha!]Q$ соответственно) не обязательно следует истинность утверждения о правильности программы при других пред- и постусловиях. Аналогичным образом, замена в $P[\alpha]Q$ (или $P[\alpha!]Q$) программы α на программу β , вообще говоря, не сохраняет истинностного значения утверждения о правильности. Не следует также думать, что при данных условиях P и Q существует только одна программа α , для которой высказывание $P[\alpha]Q$ (или $P[\alpha!]Q$) истинно.

Говорить о правильности программы самой по себе бессмысленно. Программа пишется с целью решения той или иной конкретной задачи. Каждая правильно поставленная задача содержит в себе условие (то, что дано) и вопрос, на который нужно дать ответ. При составлении программы условие задачи превращается в предусловие, а вопрос преобразуется в постусловие, имеющее

уже форму не вопроса, а утверждения, которое должно быть истинно всякий раз, когда ответ на вопрос задачи правилен.

Из определений следует, что всякая тотально правильная программа является частично правильной при тех же пред- и постусловиях. Обратное конечно же неверно. Ясно, что тотальная правильность «лучше» частичной, хотя доказать тотальную правильность программы, по-видимому, сложнее, чем частичную.

Для доказательства частичной правильности операторных программ обычно используются различные модификации *метода Флойда*, который состоит в следующем. На схеме программы выбирают контрольные точки так, чтобы любой циклический путь проходил по крайней мере через одну точку. С каждой контрольной точкой ассоциируется специальное условие (индуктивное утверждение или инвариант цикла), которое истинно при каждом переходе через эту точку. С входом и выходом схемы также ассоциируются пред- и постусловия. Затем каждому пути программы между двумя соседними контрольными точками сопоставляется так называемое условие правильности. Выполнимость всех условий правильности гарантирует частичную правильность программы.

Один из способов доказательства завершения работы программы состоит во введении в программу дополнительных счетчиков для каждого цикла и в доказательстве их ограниченности в процессе доказательства частичной правильности программы.

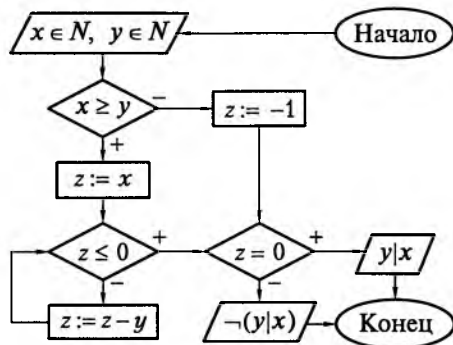
Одна из модификаций метода Флойда заключается в построении конечной аксиоматической системы (так называемой «логики Хоара»), состоящей из схем аксиом и правил вывода, в которой в качестве теорем выводимы утверждения о частичной правильности программ, в частности на языке программирования Паскаль. Такая система используется и для задания аксиоматической семантики языка Паскаль. Аксиоматические системы, родственные логике Хоара, разработаны и для других алгоритмических языков программирования.

Для доказательства правильности рекурсивных программ используется метод математической индукции, связанный с определением наименьшей неподвижной точки, а для программ со сложными структурами данных (например, графами, деревьями) — индукция по структуре данных. При этом в теоретических исследованиях по логике Хоара рассматриваются обычные свойства аксиоматизаций в логике — их непротиворечивость и полнота.

Пример 38.1. Рассмотрим простой пример программы и проанализируем ее на правильность. Требуется составить программу, которая для любых натуральных x и y давала бы ответ на вопрос, делится ли x на y . Будем писать « $y|x$ » вместо « x делится на y ». Тогда определение делимости можно записать следующим образом:

$$(\forall x \in N)(\forall y \in N)[y|x \leftrightarrow (\exists n \in N)(ny = x)].$$

Что должен делать компьютер, чтобы выяснить, существует ли такое n , что $ny = x$? Заменяем последнее условие на следующее $x = y + y + \dots + y$ (n слагаемых), которое, в свою очередь, равносильно следующему: $0 = x - y - y - \dots - y$ (n вычитаемых). Проверка этого условия уже под силу компьютеру: нужно организовать цикл, который на каждом шаге вычитает сначала из x число y , затем из результата снова y , и так до тех пор, пока не получится число 0 или отрицательное число. В первом случае ответ на вопрос о делимости x на y будет положительным, во втором — отрицательным. Структурная схема программы, реализующей указанный алгоритм, представлена ниже.



Итак, условие, налагаемое на входные данные: $x \in N, y \in N$; условие, которое необходимо проверить: $z = 0$. Докажем правильность этой структурной схемы и соответствующей программы методом от противного. Суть этого метода состоит в следующем. Допустим, что требуется доказать утверждение A . Мы принимаем гипотезу о том, что A ложно, т.е. истинно $\neg A$. Если из $\neg A$ удастся вывести противоречие $B \wedge \neg B$, то заключаем, что $\neg A$ на самом деле ложно (поскольку влечет противоречие). Значит, истинно A .

В случае с рассматриваемой программой мы хотим доказать, что выдача нашей программой результата $z = 0$ действительно будет происходить в том и только в том случае, когда x делится на y . Это значит, что доказываемое утверждение A имеет вид: « $z = 0 \leftrightarrow y|x$ ». Допустим, что это утверждение неверно. Это означает, что ложна одна из импликаций « $z = 0 \rightarrow y|x$ » или « $y|x \rightarrow z = 0$ ». Предположим сначала, что ложна первая импликация « $z = 0 \rightarrow y|x$ », т.е. $z = 0$ истинно, но x на y не делится. В соответствии со структурной схемой $z = 0$ либо когда $x = 0$, либо когда в процессе вычитания $x - y - y \dots - y$ на некотором шаге получится 0. В первом случае x делится на y в противоречие с допущением. То же происходит и во втором случае. Если $x - y - y \dots - y = 0$, то $x - ny = 0$, т.е. $x = ny$ для некоторого n , что и означает делимость x на y .

Допустим теперь, что ложна вторая импликация, т.е. что x делится на y , но $z \neq 0$. Неравенство $z \neq 0$ может иметь место в одном из

следующих трех случаев: а) при невыполнении условия $x \geq y$, т.е. при $x < y$; б) после завершения цикла; в) в ходе выполнения цикла. Поскольку присваивание $z := x$ при $x \neq 0$ приводит к вхождению в цикл (так как из $x \neq 0$ следует $x > 0$, $z > 0$), поэтому никаких других возможностей для $z \neq 0$, кроме указанных трех, на структурной схеме не существует. Рассмотрим последовательно эти три возможности:

а) если $x < y$, то по структурной схеме $z := -1$, т.е. $z \neq 0$, а значит, x не делится на y в противоречие с допущением;

б) если цикл завершен и $z \neq 0$, то $z < 0$. Это означает, что $x - ky < 0$, т.е. $x < ky$, и $\neg(\exists n \in \mathbb{N})(x = ny)$. Следовательно, x не делится на y , что также противоречит допущению;

в) $z \neq 0$ в ходе выполнения цикла. Но в этом случае мы и не требуем, чтобы был дан ответ на вопрос о делимости x на y . Мы рассчитываем его получить после выполнения программы, а не в ходе ее выполнения. Но только что было доказано, что если цикл завершится с $z \neq 0$, то x на y не делится. Здесь мы обнаруживаем, что цикл может и не завершиться, если z будет оставаться положительным. Это будет происходить в том случае, когда $y = 0$ и $z - 0 = z = x > 0$. Но так и должно быть: ведь в этом случае мы будем пытаться установить, делится ли положительное число x на 0 , а такая операция запрещена.

Таким образом, мы устанавливаем, что если наша программа завершится, то она решит поставленную задачу, т.е. мы доказали частичную правильность нашей программы. Чтобы сделать нашу программу тотально правильной, нужно предусмотреть ее завершение и в выявленном исключительном случае. Для этого можно, например, перед проверкой условия $x \geq y$ проверить утверждение « $x > 0 \wedge y = 0$ ». Если оно истинно, перейти к присваиванию $z := -1$, если же оно ложно — перейти к проверке $x \geq y$.

В заключение отметим, что исследования по логическому описанию программ и программирования убедительно показали, что логический анализ позволяет анализировать концепции языков программирования и находить многие скрытые недоработки в этих концепциях. Пожалуй, до сих пор это применение строгих математических методов в качестве инструмента критики концепций (зачастую совершенно не продуманных, вставляемых ради «усиления» языков программирования) является важнейшим применением математической логики в области программирования.

§ 39. Применение компьютеров для доказательства теорем математической логики

Мы уже отмечали, что формальные аксиоматические теории с их четкими понятиями аксиом и правил вывода, казалось бы, созданы для того, чтобы их развитие поручить электронно-вычислительной машине. И конечно же самым первым претенден-

том на союз с компьютером является формализованное исчисление высказываний. Исторически так оно и произошло: первые теоремы, доказанные компьютером, были теоремы формализованного исчисления высказываний. В логике и компьютерных науках стали говорить об автоматическом, или механическом, или машинном доказательстве теорем. В настоящем параграфе сначала будет рассказано об одной из первых попыток применить компьютер для поиска доказательств математических теорем — о компьютерной программе «Логик-теоретик», созданной в первой половине 1950-х гг. в США.

Программа «Логик-теоретик» и программы, близкие к ней. В 1957 г. известные американские специалисты по информатике А. Ньюэлл, Г. Саймон, Дж. Шоу [9.18] сообщили, что при помощи разработанной ими программы «Логик-теоретик» на электронно-вычислительной машине IBM-704 получены доказательства для ряда (38) теорем формализованного исчисления высказываний, содержащихся в известном труде Б. Рассела и А. Уайтхеда «Principia Mathematica» (1925—1927).

В память машины с самого начала было помещено пять аксиом исчисления высказываний Рассела — Уайтхеда и три правила вывода. Кроме того, программа составлена так, что каждая из уже доказанных теорем оставалась в памяти машины и могла использоваться для дальнейших доказательств. Алгоритм поиска доказательств имел так называемый эвристический характер. Под «эвристиками» здесь понимается выявление общих правил, позволяющих решить поставленную задачу без необходимости систематического перебора всех потенциально существующих вариантов. С помощью своей программы «Логик-теоретик» ее создатели попытались смоделировать процесс поиска такого доказательства человеком. В качестве доводов, подтверждающих, что программа моделирует человеческое мышление, приводились результаты сравнения записей доказательств теорем в виде программы с записями рассуждений «думающего вслух» человека.

В основу алгоритма программы «Логик-теоретик» были положены следующие три эвристических метода: метод подстановки, метод отделения (*modus ponens*) и метод целеобразования.

Метод подстановки предназначен для поиска среди исходных аксиом и ранее доказанных теорем такой, которую требуется доказать в данный момент. При этом программа пытается определить, какие переменные или подформулы в уже имеющейся формуле нужно заменить и на какие формулы, чтобы получить ту формулу, которую требуется доказать. Для этого программа выполняет подстановки одних формул в другие и осуществляет равносильные преобразования формул на основании наличия в своей памяти основных равносильностей алгебры высказываний (коммутативность, ассоциативность, идемпотентность конъюнкции и

дизъюнкции, законы поглощения и де Моргана, выражение импликации через дизъюнкцию и отрицание и т. п.).

Сам поиск доказательства той или иной теоремы (формулы) осуществляется методами отделения и целеобразования. *Метод отделения* состоит в том, что доказываемая формула заменяется более простой, доказав которую мы затем доказываем исходную формулу. Если F — теорема, подлежащая доказательству, то машина ищет аксиому или уже доказанную теорему вида $G \rightarrow F$. Затем делается попытка решить подзадачу — доказать теорему G . Если она окажется доказанной, то из двух теорем G и $G \rightarrow F$ по правилу МР (modus ponens) оказывается доказанной и теорема F .

Метод целеобразования предусматривает многократное использование метода отделения. Например, при необходимости доказать теорему $F \rightarrow H$ машина ищет ранее доказанную теорему вида $F \rightarrow G$. Если такая теорема найдена в памяти, то перед машиной встает новая подзадача — доказать теорему $G \rightarrow H$. Если и ее доказательство найдено, то из этих импликаций выводится требуемая теорема $F \rightarrow H$.

Таким образом, общая идея алгоритма поиска доказательства заданной теоремы F состоит в восстановлении цепочки-доказательства так называемым обратным ходом, отправляясь от самой формулы F и восстанавливая ее вплоть до уже доказанных теорем или до аксиом. Процесс поиска предшествующих формул исключительно неоднозначен и, как бы он ни был организован, носит переборный характер. И успешность выбора той или иной формулы не может быть оценена локально, в момент выбора. Поэтому программа вынуждена перебирать варианты, заходить в тупики, проходить циклы, прежде чем она сможет найти правильный путь решения. Повышение эффективности процесса вывода — центральная проблема всех автоматизированных систем дедуктивного вывода.

Как уже отмечено, с помощью этой программы была доказана часть теорем исчисления высказываний из книги Рассела и Уайтхеда «Principia Mathematica». Например, первая из этих теорем имеет вид: $(F \rightarrow \neg F) \rightarrow \neg F$. Эту теорему машина доказала в четыре шага и напечатала результат на выводном устройстве через 10 с после начала работы программы. Доказывая теорему $(F \vee (G \vee H)) \rightarrow \rightarrow ((F \vee G) \vee H)$, машина через 23 мин после начала работы объявила об исчерпании возможностей данной программы. Простая на вид, но сложная для доказательства теорема $\neg(F \rightarrow G) \rightarrow \neg F$ была доказана через 12 мин в пять этапов. На этом примере, кстати, наглядно демонстрируются принципиальные преимущества эвристических методов: если бы та же машина использовала не эвристические, а лишь чисто переборные методы, то для доказательства последней теоремы ей потребовалось бы несколько тысяч лет машинного времени [9.24, с. 253].

Создатели программы «Логик-теоретик» показали также, что их программа может не только доказывать известные теоремы исчисления высказываний, но и может выдвигать новые теоремы и стремиться к их доказательству.

Аналогичные исследования по проблеме машинного поиска логического вывода велись и в Советском Союзе. Наибольшую известность получили исследования Н. А. Шанина и его сотрудников. В [9.28] решается такая проблема: в заданном конкретном формализованном исчислении высказываний требуется составить алгоритм, выясняющий для любых формул $F_1, F_2, \dots, F_m$ и G этого исчисления, выводима ли формула G из формул $F_1, F_2, \dots, F_m$, и при утвердительном ответе на этот вопрос искомый алгоритм должен строить (и это в проблеме главное) вывод формулы G из формул $F_1, F_2, \dots, F_m$. Машинная программа, реализующая удовлетворяющий указанным требованиям алгоритм, работала на машине «Урал-4» — одной из лучших советских электронно-вычислительных машин первой половины 1960-х гг.

Отметим также работы американского программиста Ван Хао [9.5], который в 1959 г. составил три программы для доказательства теорем исчисления высказываний и исчисления предикатов, реализовав их на машине IBM-704. Первая из них позволила машине за 37 мин доказать более двухсот теорем из первых пяти глав упоминавшейся книги Рассела и Уайтхеда «Principia Mathematica», причем 12/13 этого времени было израсходовано на ввод и вывод данных, так что время, потраченное собственно на доказательство, составило менее 3 мин. По второй программе машина сама составляла формулы исчисления высказываний и выбирала из них нетривиальные теоремы, строя их доказательства. В течение 1 ч было образовано и проверено около 14 тыс. формул, из которых выделено около тысячи теорем.

Наконец, третья программа предназначалась для доказательства более 150 теорем следующих пяти глав «Principia Mathematica» для исчисления предикатов с равенством. В течение 1 ч машина нашла доказательства для 85 теорем, которые были стройнее и короче доказательств, приведенных Расселом и Уайтхедом.

Позже появились программы, которые для доказательства теорем формализованного исчисления высказываний стали эффективно использовать метатеорию, т. е. теоремы о теоремах формальной теории. Первой такой программой стала программа французского математика Ж. Питра, созданная в 1966 г. Использование метатеорем позволило осуществить наибольший глобальный обзор поиска и сконцентрировать внимание на наиболее важных направлениях, не загружая память несущественными результатами. Программа Ж. Питра работает с шестью формализованными исчислениями высказываний, базирующимися на системах аксиом Рассела, Лукашевича, Гильберта, Бернея и Шеффера. Она отыскивает все основные теоремы, причем иногда дает для них оригинальные доказательства. Про-

грамма умеет работать и на уровне предположений: ей задается конкретное выражение и требуется его доказать. Достоинство программы в том, что с ее помощью удалось доказать некоторые теоремы, которые не смог доказать ее создатель. Вот суждение об этом самого Лукашевича: «Нужно быть очень опытным и искусным в построении логических доказательств, чтобы вывести закон коммутативности $(P \rightarrow (Q \rightarrow R)) \rightarrow (Q \rightarrow (P \rightarrow R))$ или даже закон упрощения $P \rightarrow (Q \rightarrow P)$ ». Программа Ж. Питра эффективно доказывает оба этих утверждения в рассматриваемой аксиоматике.

Метод резолюций для доказательства теорем исчисления высказываний и исчисления предикатов. Этот метод, разработанный американским математиком Дж. Робинсоном [9.20] в 1965 г., способствовал значительному прогрессу в автоматическом доказательстве теорем. Корни этого метода лежат в исследованиях известного французского логика Ж. Эрбрана, который в 1930 г. доказал очень важную теорему, послужившую основой для предложенного им механического метода доказательства теорем. (Эрбран погиб в 1931 г. в возрасте 23 лет в Альпах во время восхождения на одну из вершин.) Как известно, в исчислении предикатов каждая теорема является общезначимой формулой (т. е. истинной во всякой интерпретации). Следовательно, необщезначимая формула не может быть теоремой. Так вот, Эрбран предложил алгоритм, устанавливающий необщезначимость формулы и, следовательно, ее недоказуемость. Точнее, он предложил алгоритм для нахождения интерпретации, не удовлетворяющей данной формуле, т. е. интерпретации, на которой формула превращается в ложное высказывание. Если заданная формула в действительности была общезначимой, то такой интерпретации не находилось, и алгоритм Эрбрана устанавливал этот факт за конечное (может быть, большое) число шагов. Если же заданная формула в действительности не была общезначимой, то алгоритм Эрбрана не мог установить этого факта за конечное число шагов. Таким образом, при отсутствии в то время вычислительных машин алгоритм Эрбрана оказался весьма трудоемким для ручных вычислений и не получил практического применения.

С появлением вычислительных машин интерес к механическому доказательству теорем резко возрос. В 1960 г. эрбрановский алгоритм был реализован на ЭВМ, были сделаны попытки его усовершенствования, но полученные программы были все же малоэффективны. Значительный прогресс в деле автоматического доказательства теорем начался с открытия Робинсоном в 1965 г. принципа резолюций.

Робинсон пришел к заключению, что правила вывода, которые следует применять при автоматизации процесса доказательства теорем при помощи компьютера, не обязательно должны совпадать с правилами вывода, используемыми человеком. Он обнаружил, что общепринятые правила вывода, в частности пра-

вило *modus ponens*, специально выбраны «слабыми», чтобы человек смог индуктивно проследить за каждым шагом процедуры доказательства. Робинсон открыл более сильное правило вывода, которое он назвал *резолюцией* (или *правилом резолюции*). Это правило трудно поддается восприятию человеком, но эффективно реализуется на компьютере. Оно имеет следующий вид:

$$G \vee F, H \vee \neg F \models G \vee H. \quad (1)$$

Нетрудно проверить, что формула $G \vee H$ действительно является логическим следствием двух формул, стоящих слева. При этом говорят, что формула $G \vee F$ *резольвирует* с формулой $H \vee \neg F$, а формула $G \vee H$ называется *резольвентой* формул $G \vee F$ и $H \vee \neg F$. Если при этом в условии отсутствует формула G (или она тождественно ложна), то правило (1) принимает приведенный ниже вид (2). Если в условии отсутствует формула H (или она тождественно ложна), то правило (1) принимает вид $G \vee F, \neg F \models G$. Наконец, в случае отсутствия и G и H говорят, что правило резолюции дает (порождает) пустую формулу. (Фактически это означает, что из F и $\neg F$ выводится любая формула.)

Сравнив правило резолюции (1) с правилом *modus ponens*: $F, F \rightarrow H \models H$, записанным в виде

$$F, H \vee \neg F \models H, \quad (2)$$

можно видеть, что первое является обобщением второго. Наконец, приведенное выше правило резолюции можно представить в виде:

$$\neg G \rightarrow F, F \rightarrow H \models \neg G \rightarrow H, \quad (3)$$

и в таком виде оно совпадает с правилом цепного заключения.

Основываясь на подходящей системе аксиом и правиле резолюции как единственном правиле вывода, можно построить полное формализованное исчисление предикатов первого порядка.

Приступим теперь к описанию метода резолюций для доказательства теорем в формализованных исчислениях. Начнем с *формализованного исчисления высказываний*. Отметим прежде одну простую идею.

Пусть даны формулы $F_1, \dots, F_m$ и G . Нетрудно доказать, что формула G будет логическим следствием формул $F_1, \dots, F_m$ тогда и только тогда, когда формула $F_1 \wedge \dots \wedge F_m \wedge \neg G$ является противоречием (т. е. тождественно ложна). В самом деле,

$$F_1, \dots, F_m \models G \Leftrightarrow (F_1 \wedge \dots \wedge F_m) \rightarrow G$$

(см., например, теорему 6.4). Далее, формула $(F_1 \wedge \dots \wedge F_m) \rightarrow G$ будет тавтологией, если и только если ее отрицание $\neg((F_1 \wedge \dots \wedge F_m) \rightarrow G)$ будет противоречием. Равносильными преобразованиями эта формула приводится к требуемой:

$$\neg((F_1 \wedge \dots \wedge F_m) \rightarrow G) \equiv \neg(\neg(F_1 \wedge \dots \wedge F_m) \vee G) \equiv \\ \equiv \neg(\neg F_1 \vee \dots \vee \neg F_m \vee G) \equiv F_1 \wedge \dots \wedge F_m \wedge \neg G.$$

Наконец, по теореме адекватности формализованного исчисления высказываний (теорема 16.7) имеем

$$F_1, \dots, F_m \vdash G \Leftrightarrow F_1, \dots, F_m = G.$$

Таким образом, доказательство выводимости формулы G из формул $F_1, \dots, F_m$ в формализованном исчислении высказываний сводится к доказательству тождественной ложности формулы $F_1 \wedge \dots \wedge F_m \wedge \neg G$.

В свою очередь, чтобы доказать тождественную ложность формулы $F_1 \wedge \dots \wedge F_m \wedge \neg G$, достаточно доказать, что из совокупности формул $F_1, \dots, F_m, \neg G$ логически следует любая формула. Для этого и служит *метод резолюций*. Он состоит в том, что к формулам из множества $\{F_1, \dots, F_m, \neg G\}$ применяется правило резолюции. Получаемые формулы (резольвенты) также включаются в это множество, и к ним также может применяться это правило вывода. Порождение резольвент происходит до тех пор, пока не будет получена пустая формула. Как было отмечено выше, это и будет означать, что исходное множество $\{F_1, \dots, F_m, \neg G\}$ формул противоречиво, а формула $F_1 \wedge \dots \wedge F_m \wedge \neg G$ тождественно ложна.

Рассмотрим простой пример. Пусть $F_1 \equiv \neg P \vee \neg Q \vee R$, $F_2 \equiv P$, $F_3 \equiv Q$, $G \equiv R$. Спрашивается, следует ли формула G из формул F_1, F_2, F_3 . Рассматриваем множество формул:

- (1): $\neg P \vee \neg Q \vee R$ ($\equiv F_1$);
- (2): P ($\equiv F_2$);
- (3): Q ($\equiv F_3$);
- (4): $\neg R$ ($\equiv \neg G$).

Применяем к формулам (1) и (2) правило резолюции. Получаем:

- (5): $\neg Q \vee R$.

Теперь применяем правило резолюции к формулам (3) и (5). Получаем:

- (6): R .

Наконец, применение правила резолюции к формулам (4) и (6) дает пустую формулу:

- (7): $\square$ (где $\square$ — символ пустой формулы).

Таким образом, формула G является логическим следствием формул F_1, F_2, F_3 .

Присмотревшись внимательнее к приведенному примеру, видим, что участвующие в нем формулы F_1, F_2, F_3, G имеют специфический вид, что на практике конечно же имеет место не всегда. Специфичность их вида состоит в том, что все они являются (совершенными) дизъюнктивными одночленами. Поэтому, если заданы произвольные формулы $F_1, \dots, F_m, G$, то нужно составить

формулу $F_1 \wedge \dots \wedge F_m \wedge \neg G$, привести ее равносильными преобразованиями к (совершенной) конъюнктивной нормальной форме: $F_1 \wedge \dots \wedge F_m \wedge \neg G \equiv D_1 \wedge D_2 \wedge \dots \wedge D_k$, а затем применять метод резолюций к множеству $S = \{D_1, D_2, \dots, D_k\}$ (элементы этого множества называются *дизъюнктами* данной совокупности формул).

Перейдем теперь к рассмотрению *метода резолюций в логике предикатов*, для чего собственно этот метод и был создан.

Каждая формула логики предикатов, которая участвует в доказательстве по методу резолюций, должна быть представлена в специальном стандартном виде. Первый шаг на пути к преобразованию формулы к такому виду — это приведение ее к предваренной нормальной форме, бескванторная часть которой приведена к конъюнктивной нормальной форме. Эта процедура была подробно рассмотрена нами в § 22 выше.

Например, применяя указанную процедуру к формуле

$(\forall x)\{P(x) \rightarrow [(\forall y)(P(y) \rightarrow R(x, y)) \wedge \neg(\forall y)(Q(x, y) \rightarrow P(y))]\} \equiv$,
получаем

$$\begin{aligned} &\equiv (\forall x)\{\neg P(x) \vee [(\forall y)(\neg P(y) \vee R(x, y)) \wedge (\exists y)(\neg(\neg Q(x, y) \vee P(y)))]\} \equiv \\ &\equiv (\forall x)\{\neg P(x) \vee [(\forall y)(\neg P(y) \vee R(x, y)) \wedge (\exists y)(Q(x, y) \wedge \neg P(y))]\} \equiv \\ &\equiv (\forall x)\{\neg P(x) \vee [(\forall y)(\neg P(y) \vee R(x, y)) \wedge (\exists t)(Q(x, t) \wedge \neg P(t))]\} \equiv \\ &\equiv (\forall x)\{\neg P(x) \vee (\forall y)(\exists t)[(\neg P(y) \vee R(x, y)) \wedge (Q(x, t) \wedge \neg P(t))]\} \equiv \\ &\equiv (\forall x)(\forall y)(\exists t)\{\neg P(x) \vee [(\neg P(y) \vee R(x, y)) \wedge Q(x, t) \wedge \neg P(t)]\} \equiv \\ &\equiv (\forall x)(\forall y)(\exists t)[(\neg P(x) \vee \neg P(y) \vee R(x, y)) \wedge (\neg P(x) \vee Q(x, t)) \wedge \\ &\wedge (\neg P(x) \vee \neg P(t))]. \end{aligned}$$

Далее, производится так называемая *сколемизация* полученной формулы, целью которой является удаление всех кванторов существования. Эта процедура заключается в следующем. Если на первом месте в формуле стоит квантор существования, то стоящая под ним предметная переменная всюду в данной формуле заменяется некоторым конкретным предметом (индивидом), а сам квантор существования опускается. Например, для формулы $(\exists x)(\forall y)(P(x, y))$ эта процедура дает $(\forall y)(P(a, y))$. Если перед квантором существования $\exists u$ стоят кванторы общности $\forall x_1, \dots, \forall x_k$, то выбирается новый k -местный функциональный символ f , все u в формуле заменяются на $f(x_1, \dots, x_k)$, а квантор $\exists u$ опускается. Получаемая формула называется *сколемовской нормальной формой* для данной формулы. Например, для рассмотренной выше формулы эта процедура дает

$$(\forall x)(\forall y)[(\neg P(x) \vee \neg P(y) \vee R(x, y)) \wedge (\neg P(x) \vee Q(x, f(x, y))) \wedge (\neg P(x) \vee \neg P(f(x, y)))].$$

Получившиеся дизъюнктивные одночлены образуют *множество дизъюнктов* исходной формулы, которое, подобно тому как это было в исчислении высказываний, участвует в доказательстве по методу резолюций. Для вышерассмотренной формулы приходим к следующему множеству дизъюнктов:

$$S = \{\neg P(x) \vee \neg P(y) \vee R(x, y), \neg P(x) \vee Q(x, f(x, y)), \\ \neg P(x) \vee \neg P(f(x, y))\}.$$

Выше мы установили, что для доказательства выводимости формулы G из формул $F_1, \dots, F_m$ в исчислении высказываний достаточно доказать тождественную ложность формулы $F_1 \wedge \dots \wedge F_m \wedge \neg G$, т.е. противоречивость множества дизъюнктов $\{F_1, \dots, F_m, \neg G\}$. Аналогичным способом можно действовать и в исчислении предикатов. Но здесь нужно попытаться построить модель множества формул $\{F_1, \dots, F_m, \neg G\}$, т.е. найти такую интерпретацию, при которой все бы эти формулы превратились в истинные высказывания. Если такая модель существует, то G не может быть следствием формул $F_1, \dots, F_m$. Если же такой модели не существует, то G является следствием формул $F_1, \dots, F_m$. Ясно, что в общем случае поиск такой интерпретации придется вести среди необозримо большого количества интерпретаций (в зависимости от вида формул $F_1, \dots, F_m, G$). Но оказывается, круг исследуемых интерпретаций все же можно значительно сузить. Достаточно рассматривать интерпретации не на всевозможных множествах, а на так называемом универсуме Эрбрана. Интерпретации, возникающие на универсуме Эрбрана, называются эрбрановскими интерпретациями.

Универсум Эрбрана для множества S формул логики предикатов обозначается $H(S)$ и строится рекурсивно следующим образом:

- 1) множество всех индивидов из S принадлежит $H(S)$; если в S их нет, то $H(S)$ приписывается произвольный индивид a ;
- 2) если термы $t_1, \dots, t_n$ принадлежат S , то $H(S)$ содержит также $f(t_1, \dots, t_n)$, где f — любой n -местный функциональный символ из S ;
- 3) никаких других термов в $H(S)$ нет.

Ясно, что при выборе любой интерпретации, т.е. при произвольном приписывании значений истинности (0 или 1) простейшим (атомарным) формулам из S , никаких других объектов предметной области, помимо объектов из $H(S)$, не потребуется. В этом смысле $H(S)$ — наиболее общая область интерпретации формул из S , так что поиск модели множества формул S можно ограничить эрбрановскими интерпретациями, и если мы установим, что такой модели для множества $\{F_1, \dots, F_m, \neg G\}$ среди этих интерпретаций нет, то ее не будет существовать вовсе, а значит, G будет следствием формул $F_1, \dots, F_m$. Если же модель множества формул S существует, то она существует и среди ее эрбрановских интерпретаций. Универсум Эрбрана, вообще говоря, бесконечен, но счетен.

Например, если задано следующее множество формул (дизъюнктов) $S = \{P(x) \vee Q(a) \vee \neg P(f(a)), \neg Q(b) \vee P(g(x, y))\}$, имеющее множество индивидов $\{a, b\}$ и множество функциональных символов $\{f, g\}$, то его универсум Эрбрана представляет собой бесконечное множество $H(S) = \{a, b, f(a), f(b), g(a, a), g(a, b), g(b, a), g(b, b), f(f(a)), \dots\}$.

Второй пример: пусть в формулы из S входят константы (индивиды) a, b, c , предметные переменные x, y, z , одноместная предикатная переменная P и двухместная предикатная переменная Q . Тогда $H(S) = \{a, b, c\}$. Для построения эрбрановской интерпретации множества формул S нужно далее приписать значения истинности каждой конкретизации предикатных переменных на $P(x)$ и $Q(y, z)$ на универсуме Эрбрана. Перечислим сначала все такие конкретизации: $P(a), P(b), P(c), Q(a, a), Q(a, b), Q(a, c), Q(b, a), Q(b, b), Q(b, c), Q(c, a), Q(c, b), Q(c, c)$. (Совокупность всех этих конкретизаций называется *эрбрановской базой*.) Каждому элементу этой базы нужно теперь приписать значение истинности 0 или 1. Поскольку элементов в базе 12, то, как мы знаем, это можно сделать $2^{12} = 4096$ различными способами. Таким образом, мы получим 4096 эрбрановских интерпретаций данного множества формул.

Форма правила резолюции в логике предикатов остается той же самой, что и в логике высказываний. Но в формулах логики предикатов содержатся предметные переменные, которых не было в формулах логики высказываний, и применение данного правила здесь несколько усложняется. В этом случае над формулами логики предикатов производится еще одна процедура (после того, как из них после их сколемизации образовано множество дизъюнктов) — *процедура унификации предметных переменных*.

Суть этой процедуры состоит в том, что в данных формулах некоторые предметные переменные заменяются конкретными предметами (индивидами), чтобы для формул, к которым нельзя было раньше применить правило резолюций, теперь это стало возможным. Например, если к формулам $P(a) \vee \neg Q(a, b)$ и $Q(x, y) \vee \neg R(x, y)$ нельзя применить правило резолюций, то после замены (подстановки) во второй формуле x на a и y на b получаем формулы $P(a) \vee \neg Q(a, b)$ и $Q(a, b) \vee \neg R(a, b)$, к которым это правило применимо, и оно дает формулу (резольвенту) $P(a) \vee \neg R(a, b)$. (Отметим, что к формулам $P(a) \vee \neg Q(b, c)$ и $Q(c, c) \vee \neg R(b, c)$ правило резолюции не применимо, — говорят, что они не резольвируются.) Подстановку t в x обозначим $\{t/x\}$. В случае выполнения множества подстановок $\{t_1/x_1, \dots, t_n/x_n\}$ необходимо соблюдение ряда условий: а) x_i является переменной, а t_i — термом (константой, переменной, символом функции), отличным от x_i ; б) для любой пары подстановок t_i/x_i и t_j/x_j в правых частях символов / не содержатся одинаковые переменные.

Как и в исчислении высказываний, в исчислении предикатов правило резолюции, примененное к формулам $P(a)$ и $\neg P(a)$, дает пустую формулу. Это означает, что исходное множество формул $F_1, \dots, F_m, \neg G$ противоречиво, а значит, формула G выводима из формул $F_1, \dots, F_m$. С точки зрения семантики возможность выведения пустой формулы означает, что нельзя построить эрбрановскую модель множества формул $F_1, \dots, F_m, \neg G$.

Наконец, о методе резолюций для доказательства теорем исчисления предикатов. Для того чтобы автоматизировать процесс доказательства того, что формула G выводима из формул $F_1, \dots, F_m$, было бы хорошо найти эффективный алгоритм, основывающийся на правиле резолюции, который позволял бы обнаруживать противоречивость множества формул $F_1, \dots, F_m, \neg G$. Представим себе, что существует некая активная сила (человек или машина), которая по случайному закону применяет правило резолюции к формулам из множества $\{F_1, \dots, F_m, \neg G\}$. После каждого выполнения резолюции получающаяся резольвента добавляется в это множество. Если будет сгенерирована пустая формула, то это и будет означать, что исходное множество формул противоречиво, и тогда эта активная сила прекратит свое действие. Если G выводима из $F_1, \dots, F_m$, то множество формул $\{F_1, \dots, F_m, \neg G\}$ действительно противоречиво, и активная сила рано или поздно сгенерирует пустую формулу и тем самым обнаружит эту противоречивость. Тем не менее в процессе работы может быть сгенерировано огромное количество резольвент. Поэтому для создания эффективного алгоритма поиска пустой формулы необходимо наложить ограничения на данный процесс и направить его активность на участки, которые с наибольшей вероятностью могут привести к появлению пустой формулы.

Таким образом, при использовании метода резолюций возможна не одна стратегия поиска решения задачи, и важнейшей проблемой при этом является проблема эффективности алгоритма поиска доказательства. Разработано большое число стратегий поиска доказательства методом резолюций (или, как говорят, исчисления резолюций), использующие, в частности, различного рода ограничения на вид исходных дизъюнктов (наиболее распространены так называемые дизъюнкты Хорна). Каждая из этих стратегий обладает своими преимуществами. При чем для одной и той же теоремы (формулы) некоторые стратегии могут работать хорошо, а другие — плохо. С другой стороны, одна и та же стратегия для одних теорем работает хорошо, а других — плохо.

Рассмотрим подробнее так называемую *нисходящую* (или *обратную*) стратегию на следующем конкретном примере. Пусть имеются формулы: $P(a) \vee \neg Q(a, b)$, $Q(x, y) \vee \neg R(x, y)$, $S(b)$, $R(a, b)$. Требуется выяснить, является ли формула $P(a)$ следствием перечисленных. Сначала добавляем к данному множеству формул отрицание доказываемой формулы. В результате получаем следующее множество формул:

- (1): $P(a) \vee \neg Q(a, b)$;
- (2): $Q(x, y) \vee \neg R(x, y)$;
- (3): $S(b)$;
- (4): $R(a, b)$;
- (5): $\neg P(a)$.

Действие данного алгоритма метода резолюций будет сфокусировано на следствиях добавления формулы (5) к данному множеству формул (1) — (4). Алгоритм характеризуется следующими двумя требованиями: в первой выполняемой резолюции следует использовать только что добавленную формулу (5); в каждой последующей резолюции должна участвовать резолювента предыдущей резолюции (это предотвращает хаотическое «блуждание» алгоритма и порождение им необозримого количества «лишних» формул). Согласно первому требованию на первом шаге применяем правило резолюции к формулам (5) и (1), которые резольвируют друг с другом. В результате получаем формулу

$$(6): \neg Q(a, b).$$

Согласно второму требованию на следующем шаге должна участвовать формула (6). Она резольвирует с формулой (2). Результатом будет формула

$$(7): \neg R(a, b).$$

(Обратите внимание на то, что в формуле (2) была предварительно проведена унификация предметных переменных с помощью подстановки $a/x, b/y$.) Формула (7) резольвирует с формулой (4). Их резолювентой является пустая формула. Это означает, что множество формул (1) — (5) противоречиво, что, в свою очередь, означает, что формула $P(a)$ является следствием формул (1) — (4).

Рассмотренная стратегия метода резолюций является нисходящей, так как она начинает процесс решения с отрицания заключения, а далее в процессе решения используются остальные исходные формулы, что продолжается до тех пор, пока не будет выведена пустая формула. Данная стратегия решения называется также стратегией поиска «сначала вглубь», поскольку результат последней резолюции всегда используется в следующей за ней резолюции.

§ 40. От математической логики к логическому программированию

Здесь будет кратко рассказано о языке логического программирования ПРОЛОГ, возникновение и развитие которого непосредственно связаны с открытием метода резолюций для доказательства теорем в логике, рассмотренного в предыдущем параграфе. Его название происходит от слов PROgramming in LOGic, т.е. ПРОграммирование в ЛОГике, или ПРОграммирование при помощи ЛОГики. В его основу положен математический аппарат логики предикатов 1-го порядка и теории логического вывода.

Возникновение языка ПРОЛОГ и его развитие. После того как Робинсон в 1965 г. открыл правило вывода, названное им правилом резолюции, значительно активизировались работы по созданию автоматизированного метода доказательства теорем через опровержение. Первоначально попытки создания алгоритма решения задач,

базирующегося на правиле резолюции, оказывались успешными только для очень небольших задач. Существенно усовершенствовали такие алгоритмы Лавленд, Ковальски и Кузнер, разработав метод устранения моделей (1968) и метод селектирующей функции (1971). В 1974 г. Ковальски первым предложил метод, в соответствии с которым логический язык (именно язык логики предикатов) можно было бы использовать как язык программирования. Кольмерор и Руссель воспользовались результатами этих работ и к 1975 г. создали язык программирования, основывающийся на логике предикатов и правиле резолюции, названный ими ПРОЛОГ.

В течение 1970-х гг. язык ПРОЛОГ прошел путь развития от интересующего лишь узких специалистов экспериментального языка, созданного европейскими учеными, до одного из ведущих языков программирования, широко используемого во всем мире. В 1977 г. Уоррен и Перейра из Эдинбургского университета (Великобритания) создали интерпретатор/компилятор языка ПРОЛОГ для компьютера DEC-10, а в 1980 г. в Империзл Колледже разработан интерпретатор языка микроПРОЛОГ для персональных компьютеров.

В 1981 г. в Японии было объявлено о начале работ по созданию компьютеров пятого поколения. Они должны отличаться от компьютеров предыдущих поколений тем, что в них встроены функции программиста. По словесному заданию задачи, сформулированному на ограниченном профессиональном языке, эти компьютеры способны сами построить необходимую рабочую программу (синтезировать ее из отдельных модулей, хранящихся в памяти компьютера) и выполнить ее. В качестве основной методологии разработки программных средств для компьютеров пятого поколения было избрано логическое программирование. В состав такого компьютера должна входить так называемая база знаний, в которой хранится информация о закономерностях, присущих данной проблемной области, и методах решения характерных для нее задач. Кроме того, в его состав должен входить специальный блок — решатель, который осуществляет процедуры логического вывода. С помощью решателя на основании сведений из базы знаний автоматически синтезируются нужные для пользователя программы. Полезный эффект от таких систем будет заключаться в том, что в распоряжение широких слоев общества будут предоставлены мощные вычислительные ресурсы и что возрастет производительность труда в ряде отраслей промышленности, в которых сейчас она традиционно низка.

Общая характеристика языка ПРОЛОГ. Язык ПРОЛОГ существенно отличается от традиционных алгоритмических языков программирования, таких, как «Бейсик», «Паскаль» и т. п. При использовании последних для решения задач на компьютере пользователь сначала должен разработать алгоритм решения задачи, затем записать (закодировать) его на алгоритмическом языке

программирования и, наконец, «прогнать» программу на компьютере и получить результат.

В ПРОЛОГЕ дело обстоит иначе. Пользователь лишь формулирует задачу, осуществляет ее постановку, т.е. сообщает компьютеру необходимые факты и правила, по которым эти факты соотносятся друг с другом. Затем формулируется вопрос, на который компьютер отвечает самостоятельно, исходя из той «базы знаний», т.е. набора фактов и правил, которые пользователь сообщил компьютеру. Запись фактов происходит на языке логики предикатов. Правило построения выводов из имеющихся фактов — правило резолюции. Таким образом, ПРОЛОГ — это язык описания фактов, правил вывода заключений и постановки вопросов к базам данных, записываемых на языке математической логики. Фактически вопрос представляет собой теорему логики предикатов, а работа программы состоит в том, чтобы доказать эту теорему на основе фактов и правил из базы данных.

Компьютерная система языка ПРОЛОГ представляет собой интерпретатор, состоящий из следующих независимых подпрограмм: сканер, унификатор, управление, печать.

Подпрограмма *сканер* осуществляет синтаксический контроль исходного текста программы и его перевод во внутреннюю форму хранения программы — в дерево. Дерево хранится в памяти машины в виде упорядоченной совокупности массивов.

Подпрограмма *унификатор* выполняет в процессе поиска доказательства по методу резолюций действия для унификации двух термов, т.е. проводит поиск такой совокупности значений переменных, входящих в данные термы, при подстановке которых в эти термы они станут равными, а соответствующие формулы резолируемыми.

Подпрограмма *управления* осуществляет процесс поиска доказательства. Алгоритм ее действия основан на правиле резолюции. Чтобы этот процесс произошел, программист должен четко описать задачу при помощи так называемых фраз (или клауз, или формул, или дизъюнктов) Хорна, выраженных на языке ПРОЛОГ. В каждой фразе формулируется некоторое отношение между термами. Терм — это обозначение, представляющее некоторую сущность из исследуемой области. Для того чтобы привести в действие данный алгоритм решения задачи, программист должен написать вопрос, согласно которому будет необходимо выяснить, является ли конкретная формула следствием заданного множества формул, представленных в программе.

Наконец, подпрограмма *печать* выводит на экран все значения переменных, указанных в вопросе и удовлетворяющих совокупности фактов и правил.

Краткое описание языка ПРОЛОГ и примеры. Язык ПРОЛОГ начинается со следующих основных синтаксических конструкций.

Атом — последовательность букв, цифр и знаков минус, начинающаяся с буквы или знака минус, длиной не более 256 символов. *Переменная* — либо буква, либо атом, заканчивающийся символом апострофа, либо символом подчеркивания. *Целое* — значение целого находится в пределах от 0 до 32767. *Терм* — выражение вида $F(x, y, \dots, z)$, где F — атом, называемый именем терма; $x, y, \dots, z$ — аргументы, в качестве которых могут выступать любые синтаксические конструкции входного языка. *Список* — упорядоченная совокупность объектов (элементов списка), в качестве которых могут выступать любые синтаксические конструкции языка, включая сами списки.

Перечисленные грамматические конструкции могут образовывать *предложения* (или фразы, клаузы, формулы, дизъюнкты), на вид которых наложено следующее ограничение. Все они должны быть *дизъюнктами Хорна*. Это такие совершенные дизъюнктивные одночлены, которые имеют не более одного вхождения положительной переменной (т.е. переменной без знака отрицания). Их общий вид: $B \vee \neg A_1 \vee \neg A_2 \vee \dots \vee \neg A_n$. Ясно, что этот вид равносильен следующему: $\neg(A_1 \wedge A_2 \wedge \dots \wedge A_n) \vee B$, т.е. $(A_1 \wedge A_2 \wedge \dots \wedge A_n) \rightarrow B$.

Выделяют следующие три типа таких предложений: факт, правило и вопрос.

Факт (или допущение без условий) имеет вид: B . Факт означает, что B истинно, или что цель B определена. Факты записываются в форме предикатов от одной или нескольких переменных. Например, высказывания «Водород — элемент 1-й группы», «Хлор — элемент 7-й группы» записываются на ПРОЛОГЕ в следующей форме:

! ЭЛЕМЕНТ (H, 1);

! ЭЛЕМЕНТ (Cl, 7).

Правило (или условное допущение) имеет вид: $B \vee \neg A_1 \vee \dots \vee \neg A_n$, или в эквивалентной форме $B \leftarrow (A_1 \wedge \dots \wedge A_n)$. При этом B называется заключением, A_1 — условием 1, ..., A_n — условием n . Читается: заключение B будет истинным, если условия $A_1, \dots, A_n$ будут все истинными. Правило — это формальная запись вывода умозаключения. Правило определяет зависимость одних объектов или действий от других.

Например, правило «Элемент x вступает в реакцию с элементом y , если x — элемент 7-й группы» на ПРОЛОГЕ запишется так:

! РЕАКЦИЯ(x, y) $\leftarrow$ ЭЛЕМЕНТ($x, 1$), ЭЛЕМЕНТ($y, 7$).

Совокупность фактов и правил образует *базу данных*. К базе данных можно задавать вопросы, обеспечивая тем самым запуск программы на исполнение.

Вопрос имеет вид: $\neg A_1 \vee \dots \vee \neg A_n$ или $\neg(A_1 \wedge \dots \wedge A_n)$.

Работа программы направлена на поиск такого факта B в базе данных, которое выводится из условий $A_1, \dots, A_n$. Таким образом, вопрос представляет собой теорему, а работа программы состоит в том, чтобы доказать эту теорему на основе фактов и правил из базы данных.

Пример 40.1. В качестве примера рассмотрим задачу из курса химии 7-го класса: какие химические элементы могут вступать в реакцию друг с другом.

Прежде всего создадим «базу знаний» для данной задачи. (Обратим внимание на то, что в конце каждого термина необходимо ставить знак «;», а в правилах вместо союза «и» ставить запятую.) База знаний данной задачи имеет вид:

! ЭЛЕМЕНТ(Н, 1);

! ЭЛЕМЕНТ(Сl, 7);

! ЭЛЕМЕНТ(Na, 1);

! ЭЛЕМЕНТ(І, 7);

! ЭЛЕМЕНТ(С, 4);

РЕАКЦИЯ(x , y) $\leftarrow$ ЭЛЕМЕНТ(x , 1), ЭЛЕМЕНТ(y , 7);.

Вопросы к базе знаний в ПРОЛОГЕ выражаются в форме предикатов, перед которыми ставится знак «?» При этом искомые значения обозначаются переменными:

? РЕАКЦИЯ(x , y);.

Ответ на этот вопрос компьютер ищет, руководствуясь правилом: «Элемент x вступает в реакцию с элементом y , если x есть элемент 1-й группы и y есть элемент 7-й группы». В базе знаний отыскиваются факты, удовлетворяющие этим условиям. Ответ будет следующий: $x = \text{H}$, $y = \text{Cl}$, $x = \text{Na}$, $y = \text{I}$.

Задачу можно усложнить, добавив в базу знаний в качестве фактов все элементы таблицы Менделеева, а в качестве правил — все возможные реакции взаимодействия между ними.

Пример 40.2. Рассмотрим еще один пример ПРОЛОГ-программы. Составим программу классификации животных. Это — одна из ведущих тем в курсе биологии 7-го класса. Прежде всего необходимо установить существенные определяющие признаки для такой системы классификации животных. Введем предикат, фиксирующий эти признаки животного:

! ПРИЗНАК(<животное>, <строение>, <дыхание>, <кровообращение>, <размножение>).

Введем в базу знаний следующие факты:

! ПРИЗНАК(волк, хордовое, легочное, теплокровное, живородящее);

! ПРИЗНАК(крокодил, хордовое, легочное, холоднокровное, яйцекладущее);

! ПРИЗНАК(окунь, хордовое, жаберное, холоднокровное, икрокладущее);

! ПРИЗНАК(голубь, хордовое, легочное, теплокровное, яйцекладущее).

Теперь введем в базу знаний следующие правила:

! МЛЕКОПИТАЮЩЕЕ(x) $\leftarrow$ ПРИЗНАК(x , хордовое, легочное, теплокровное, живородящее);

! ПТИЦА(x) $\leftarrow$ ПРИЗНАК(x , хордовое, легочное, теплокровное, яйцекладущее);

! ПРЕСМЫКАЮЩЕЕСЯ(x) $\leftarrow$ ПРИЗНАК(x , хордовое, легочное, холоднокровное, яйцекладущее);

! РЫБА(x) $\leftarrow$ ПРИЗНАК(x , хордовое, жаберное, холоднокровное, икрокладущее); .

Теперь можем задавать вопросы. На вопрос «? РЫБА(x);» получим ответ x = окунь; на вопрос «? МЛЕКОПИТАЮЩЕЕ(x);» получим ответ x = волк и т. д.

Имеющуюся базу знаний можно расширять, вводя в нее новые факты и новые правила. Например, предикат поведения:

! ПОВЕДЕНИЕ(<животное>, <питание>, <среда обитания>); .

Соответственно новые правила: хищное млекопитающее, водоплавающее млекопитающее и т. д.

! ХИЩМЛЕКОПИТАЮЩЕЕ(x) $\leftarrow$ МЛЕКОПИТАЮЩЕЕ(x), ПОВЕДЕНИЕ(x , плотоядное, —);

! ВОДМЛЕКОПИТАЮЩЕЕ(x) $\leftarrow$ МЛЕКОПИТАЮЩЕЕ(x), ПОВЕДЕНИЕ(x , — , вода); .

(В случае, если какой-либо признак не имеет значения, в правилах и вопросах ставится знак «—».)

Таким образом, используя минимальные средства логического программирования и создавая простейшие информационно-логические системы, можно строить интересные и полезные обучающие компьютерные системы по различным предметам. При этом обучающие возможности таких систем реализуются не только (а может, и не столько) в процессе задавания вопросов и получения ответов, но и в процессе построения самой «базы знаний». Примеры таких систем по некоторым школьным предметам (географии, истории, иностранному языку) описаны в статье¹.

Сферы применения языка ПРОЛОГ. Во-первых, на языке ПРОЛОГ прекрасно реализуется модель реляционной базы данных, представляющая собой хорошо разработанный формализм.

Во-вторых, исследователи, специализирующиеся в области программной инженерии, показали, что логическую спецификацию системы можно непосредственно преобразовать в логическую программу на языке ПРОЛОГ.

В-третьих, Кольмеррор, создавший язык ПРОЛОГ, первоначально предназначал его для обработки естественного языка. Он разработал на ПРОЛОГЕ систему грамматического разбора естественного языка нисходящим методом. Этот формализм был доработан учеными, которые продемонстрировали его успешное применение к системам, которые обрабатывают запросы, сформулированные на естественном языке.

¹ С. Григорьев, М. Морозов. Давайте попробуем ПРОЛОГ // Информатика и образование. 1987. № 4.

В-четвертых, все основные концепции, используемые в формализмах представления знаний для задач искусственного интеллекта, включая семантические сети, фреймы, правила продукций и объектно-ориентированное программирование, можно выразить при помощи логики и реализовать средствами логического программирования.

В-пятых, при представлении знаний одной из главных задач является выбор такой формы представления, которая может быть использована в экспертных системах. При помощи ПРОЛОГА были построены экспертные системы для ряда сфер, включая решение уравнений, медицину, законодательство, юриспруденцию, архитектуру, автоматизацию заводского производства, проектирование электронных схем, синтез микропрограмм, анализ финансового положения и помощь в принятии решений. Простейшие примеры экспертных систем были рассмотрены в предыдущем пункте.

§ 41. Математическая логика и информатика

Информатика — находящаяся в становлении наука, изучающая законы и методы накопления, передачи и обработки информации с помощью ЭВМ (компьютера). В англоязычных странах эта наука получила название «computer science» («вычислительная наука»). Понятие информатики охватывает области, связанные с разработкой, созданием, использованием и материально-техническим обслуживанием систем обработки информации, включая машины, оборудование, математическое обеспечение, организационные аспекты. Таким образом, информатику определяют три неразрывно связанные между собой части: алгоритмические, программные и технические средства.

Современная информатика уходит своими корнями в математику и кибернетику, электронику и системотехнику, логику и лингвистику. Основные научные направления информатики образуют следующие научные дисциплины: теоретические основы вычислительной техники, статистическая теория информации, теория вычислительного эксперимента, алгоритмизация, программирование, искусственный интеллект. Прикладная информатика обслуживает науку, технику, производство и другие виды человеческой деятельности путем создания и передачи в общество информационно-технологии.

О логических аспектах некоторых из перечисленных дисциплин информатики мы уже говорили в предыдущих параграфах настоящей главы. В настоящем параграфе будет указано на логический аспект теории баз данных.

Общее понятие о базе данных. Обработка больших массивов информации — наиболее массовая область применения компьютеров. Одним из способов хранения и обработки информации яв-

ляются так называемые базы данных. Под данными понимается информация, находящаяся в памяти компьютера или подготовленная для ввода в компьютер. *База данных* — это организованная совокупность (система) данных, предназначенная для длительного хранения (обычно во внешней памяти компьютера) и постоянного применения. База данных должна быть способна выдавать ответы на запросы. При этом можно запрашивать то, что непосредственно хранится в базе, но можно запрашивать и производную информацию, т. е. информацию, как-то выражаемую через базисную. База данных является не случайным собранием сведений, но является постоянной основой для некоторого вида конкретной деятельности человека — пользователя базы данных. Базы данных подразделяются на иерархические, сетевые, реляционные. В реляционных базах информация хранится в виде отношений между данными, а в сетевых и иерархических учитывается некоторая геометрия связей данных. База данных снабжается совокупностью языковых и программных средств, предназначенных для создания, обслуживания (ведения) и использования базы данных многими пользователями — так называемая система управления базами данных.

Понятие базы знаний представляет собой обобщение понятия базы данных. *База знаний* — организованная совокупность знаний, представленная в форме, допускающей автоматизированное использование этих знаний с помощью компьютера. При этом база знаний содержит не только конкретные факты из той или иной области, но и описание правил и общих закономерностей. Например, при решении задач из тригонометрии базой данных могут служить таблицы значений тригонометрических функций, а в базу знаний будут дополнительно включены различные тригонометрические тождества, выражающие свойства тригонометрических функций и взаимосвязи между ними.

С теорией и практикой баз данных и баз знаний связаны различные области математики — математическая логика, алгебра, геометрия.

В следующем пункте рассматривается пример реляционной базы данных, на котором поясняется применение математической логики для описания запросов в базах данных.

Реляционная база данных и логика запросов в ней. Реляционная база данных с математической точки зрения представляет собой конечный набор конечных отношений различной арности между заранее определенными множествами элементарных данных. Другими словами, реляционная база данных (точнее, каждое ее состояние) — это конечная модель в смысле математической логики. Над отношениями модели можно осуществлять различные алгебраические операции. Тем самым теория реляционных баз данных становится областью приложений математической логики

и современной алгебры и опирается на точный математический формализм.

Пример 41.1. Рассмотрим простой пример реляционной базы данных, содержащей информацию о студенческой группе за один семестр. Будем исходить из трех множеств данных: D_1 — множество студентов в данной группе, D_2 — список изучаемых за семестр предметов, D_3 — спортивные секции, в которых занимаются студенты. Далее введем множество переменных $X = \{x, y, z, u\}$; при этом считаем, что $x, y \in D_1$, $z \in D_2$, $u \in D_3$. Таким образом, каждой переменной отвечает множество данных, которые эта переменная пробегает: $D_x = D_y = D_1$, $D_z = D_2$, $D_u = D_3$.

Наконец рассмотрим еще определенный список Φ отношений между студентами и учебными предметами, между студентами и спортивными секциями, между студентами и студентами:

а) прежде всего в этот список включим отношения $\varphi_2, \varphi_3, \varphi_4, \varphi_5$ между множеством D_x студентов и множеством D_z учебных предметов. При этом, например, $(x, z) \in \varphi_3$, если студент x по предмету z в данном семестре имеет «тройку». Аналогичен смысл остальных отношений. Каждое из этих отношений можно мыслить как двухместный предикат $\varphi_i(x, z)$, заданный на множествах D_x, D_z , а соответствующее бинарное отношение, являющееся подмножеством декартова произведения $D_x \times D_z$, будет множеством истинности этого предиката;

б) символом $\psi(x, u)$ обозначим отношение (или предикат) между множеством студентов D_x и множеством спортивных секций D_u , означающее, что студент x занимается в секции u ;

в) введем еще три отношения, на этот раз на множестве всех студентов, связанных с «моральным климатом» в студенческой группе: $f_1(x, y)$ означает, что студент x относится к студенту y доброжелательно; $f_2(x, y)$ — x безразличен к y ; $f_3(x, y)$ — x относится к y недоброжелательно. Соответствующие бинарные отношения являются подмножествами декартова произведения $D_x \times D_y$.

Указанный набор Φ определяет базисную информацию — информацию о состоянии дел на каждый данный момент. Эта информация хранится в виде подмножеств соответствующих декартовых произведений.

Например:

$$\varphi_2:$$

Смирнов	алгебра
Иванов	алгебра
Иванов	геометрия

$$\psi:$$

Петров	туризм
Смирнов	шахматы
Смирнов	бокс

$$\varphi_3:$$

Смирнов	геометрия
Иванов	мат. анализ

$$f_1:$$

Петров	Смирнов
Петров	Иванов
Смирнов	Петров

$$\varphi_4:$$

Смирнов	мат. анализ
Иванов	англ. язык

$$f_2:$$

Иванов	Петров

$$\varphi_5:$$

Петров	алгебра
Петров	геометрия
Петров	мат. анализ
Петров	англ. язык
Смирнов	англ. язык

$$f_3:$$

Смирнов	Иванов
Иванов	Смирнов

$x, y \in D_1 = \{\text{Иванов, Петров, Смирнов}\};$

$z \in D_2 = \{\text{алгебра, геометрия, математический анализ, английский язык}\};$

$u \in D_3 = \{\text{бокс, шахматы, туризм}\}.$

Обработка информации, хранящейся в базе данных, предполагает определенные действия с базисными подмножествами. Для осуществления этих действий необходимо всю базисную информацию сделать однородной, т. е. «уравнять» в одном и том же большом декартовом произведении. Для этого рассмотрим множество $D = D_x \times D_y \times D_z \times D_u$. Проектирование этого множества D на рассматривавшиеся ранее множества $D_x \times D_y$, $D_x \times D_z$ и $D_x \times D_u$ позволяет рассматривать в качестве базисных отношений некоторые подмножества в D . Например, если предикат $\varphi_5(x, z)$ имеет своим множеством истинности бинарное отношение $A \subseteq D_x \times D_z$, то это же отношение можно рассматривать одновременно как подмножество A' в D по правилу: упорядоченная четверка (d_x, d_y, d_z, d_u) из D принадлежит A' , если $(d_x, d_y) \in A$. Теперь все исходные базисные бинарные отношения, заданные на разнообразных множествах, рассматриваются как четырехместные отношения, заданные на одних и тех же множествах D_x, D_y, D_z, D_u , т. е. как подмножества одного и того же множества D .

Перейдем теперь к запросам в нашей базе данных. Допустим, что нас интересует список студентов, которые отлично учатся по всем предметам, занимаются спортом, ко всем доброжелательны и не имеют врагов. Все эти качества могут быть описаны следующей формулой «идеального» студента:

$$(\forall z)(\varphi_5(x, z)) \wedge (\exists u)(\psi(x, u)) \wedge (\forall y)(f_1(x, y)) \wedge (\exists y)(f_3(y, x)).$$

Это есть формула логики предикатов, в которой предметные переменные, кроме одной переменной — x , связаны. Таким образом, формула задает одноместный предикат, зависящий от переменной x , пробегающей множество D_1 всех студентов данной группы. Множество истинности этого предиката есть подмножество множества D_1 и представляет собой множество «идеальных» студентов группы. В данном случае оно состоит из единственного студента Петрова.

Таким образом, формула логики предикатов определяет некоторый запрос в базе данных, ответ на который выдается в зависимости от состояния базы данных в данный момент времени.

Приведем другие примеры запросов. Формула

$$(\exists z_1)(\exists z_2)(z_1 \neq z_2 \wedge \varphi_2(x, z_1) \wedge \varphi_2(x, z_2))$$

запрашивает список студентов, имеющих хотя бы две «двойки». Формула

$$\neg(\exists u)(\psi(x, u))$$

дает список студентов, не занимающихся спортом, а формула

$$(\exists u_1)(\exists u_2)(u_1 \neq u_2 \wedge \psi(x, u_1) \wedge \psi(x, u_2))$$

дает список студентов, занимающихся по меньшей мере двумя видами спорта. Наконец формула

$$\neg(\exists x)(\varphi_2(x, z))$$

дает список предметов, по которым нет неудовлетворительных оценок.

Обсудим более подробно *понятие запроса в базе данных*. Отметим, во-первых, что один и тот же запрос может быть представлен разными формулами. Например, в формуле «идеального» студента вместо $\neg(\exists y)(f_3(y, x))$ можно писать $(\forall y)(\neg f_3(y, x))$, что равносильно $(\forall y)(f_1(y, x) \vee f_2(y, x))$. Ясно, что от формы записи запроса зависит скорость вычисления ответа, и поэтому далеко не безразлично, какую запись запроса выбрать.

Две формулы называют равносильными, если в любых состояниях и в любых системах данных этим формулам отвечает один и тот же результат вычислений (ответ). Другими словами, равносильные формулы — это формулы, имеющие одинаковое семантическое содержание. Тогда под запросом можно понимать не одну формулу, а весь класс равносильных ей формул. Правда, здесь возникают трудности, связанные с необходимостью уточнить понятие состояния и с необходимостью предвидеть все возможные состояния базы данных. Эти трудности преодолеваются с помощью математической логики. В математической логике имеется еще один (синтаксический) подход к определению той же равносильности формул, не требующий обращения к состояниям (к семантике). Он основан на подходящем формализованном исчислении. В каждом таком исчислении, как мы знаем, имеется понятие формулы, некоторые формулы объявляются аксиомами исчисления и указываются правила вывода. Две формулы F и G объявляются эквивалентными, если формула $F \leftrightarrow G$ (или $(F \rightarrow G) \wedge (G \rightarrow F)$, или $(\neg F \vee G) \wedge (F \vee \neg G)$) выводима из аксиом (т.е. является теоремой исчисления). Доказывается метатеорема адек-

ватности исчисления: две формулы равносильны в семантическом смысле тогда и только тогда, когда они эквивалентны в указанном сейчас синтаксическом смысле.

Имеется и еще одно применение аксиоматического подхода в теории баз данных. В схему базы данных, как правило, включается определенный набор аксиом, которым должны удовлетворять состояния. В общем случае система аксиом базы данных — это некоторый набор формул в языке первой ступени, связанном с данной базой. Аксиомы выделяют определенный набор состояний и вносят определенное содержание в набор Φ , в общем, бессодержательных символов отношений. В базах данных эти ограничения называют еще ограничениями целостности. В различных конкретных ситуациях они возникают естественным образом.

Например, в рассмотренном выше примере базы данных студенческой группы добавим еще один одноместный предикат $\xi(x)$, означающий, что студент x получает стипендию. Тогда можем ввести аксиому:

$$(\exists z)(\varphi_2(x, z) \vee \varphi_3(x, z)) \rightarrow \neg \xi(x).$$

Эта аксиома означает, что во всех рассматриваемых состояниях наличие «двойки» или «тройки» хотя бы по одному предмету лишает студента права на стипендию.

§ 42. Математическая логика и системы искусственного интеллекта

Коротко можно сказать, что под искусственным интеллектом понимается раздел информатики, изучающий методы, способы и приемы моделирования и воспроизведения с помощью компьютера разумной деятельности человека, связанной с решением задач. По существу, всякая задача, для которой неизвестен алгоритм решения, может быть отнесена к искусственному интеллекту. Основными проблемами в области искусственного интеллекта являются поиск и представление знаний. Цель исследований при этом состоит не только в разработке новых теоретических построений, но и в создании для компьютеров соответствующих программ наиболее общего характера. Использование компьютеров в качестве материальной основы искусственного интеллекта позволяет как бы изнутри взглянуть на мыслительные процессы, протекающие в человеческом мозгу.

Проблематика искусственного интеллекта имеет тесные взаимосвязи с лингвистикой, психологией и логикой, которые изучают явления, относящиеся к познанию, пониманию и умозаключениям. Эти связи носят взаимный характер: с одной стороны лингвисты, психологи, специалисты в области математической логики переводят в компьютерные программы те новые модели,

которые они разрабатывают, а с другой — исследователи в области искусственного интеллекта изучают эти модели и пытаются воссоздать на их основе логику эффективных методов решения задач. Впервые после фундаментального пересмотра картины мира, связанного с именами Коперника и Дарвина, разработка методов искусственного интеллекта возвращает нас к вопросу о месте человека в природе. По существу, впервые оспаривается исключительность человеческого разума.

Основными разделами искусственного интеллекта являются теория представления знаний, теория обработки информации, выраженной на естественном языке, теория восприятия и распознавания образов, автоматическое доказательство математических теорем, моделирование игр, робототехника, теория и создание экспертных систем. Как и раньше, в этом параграфе мы кратко акцентируем внимание на роли математической логики в теориях, связанных с искусственным интеллектом.

История развития и предмет искусственного интеллекта как науки. Искусственный интеллект как наука насчитывает уже около полувека. Это одна из тех научных дисциплин, становление и бурное развитие которых напрямую связаны с созданием и динамичным совершенствованием вычислительных машин. Начало исследований в области искусственного интеллекта связывают с работами А. Ньюэлла, Г. Саймона, Дж. Шоу, которые в 1950-х гг. исследовали процессы решения различных задач. Первой программой искусственного интеллекта стала созданная ими программа «Логик-теоретик» (о ней говорилось в начале § 42), предназначенная для доказательства теорем в формализованном исчислении высказываний и работа которой была впервые продемонстрирована 9 августа 1956 г. В 1957 г. была создана первая программа для игры в шахматы NSS (Newell, Shaw, Simon). Эти программы и созданная позже программа «Универсальный решатель задач» были основаны на так называемом эвристическом методе. (Эвристика — это правило, которое позволяет сделать выбор при отсутствии точных теоретических оснований. Эвристика — своего рода антипод алгоритма.) Эти работы положили начало первому этапу исследований в области искусственного интеллекта, когда эвристический метод решения задачи рассматривается как свойственный человеческому мышлению вообще, для которого характерно возникновение «догадок» о пути решения задачи с последующей их проверкой. Это был путь составления программ, моделирующих мышление. Этот подход, кстати, и обусловил появление и дальнейшее распространение термина «искусственный интеллект». (Отметим из этой области программу, созданную в 1960 г. Дж. Гелернтером, которая доказывала теоремы из школьного курса геометрии лучше, чем ее создатель.)

В конце 1950-х гг. появились также работы в области искусственного интеллекта, которые в противоположность ранним рабо-

там Ньюэлла и Саймона, больше относились к формальным математическим представлениям, нежели к эвристическим. Способы решения задач в этих исследованиях развивались на основе методов математической логики. Моделированию же человеческого мышления придавалось второстепенное значение. Мощный толчок в развитии этого направления оказала разработка в 1960-е гг. Робинсоном метода резолюций для доказательства теорем в логике предикатов и являющегося, по крайней мере теоретически, исчерпывающим методом доказательства (см. § 39). Методологическое значение этих работ заключалось в том, что основное внимание в исследованиях по искусственному интеллекту переместилось с разработки методов воспроизведения в компьютере человеческого мышления на разработку машинно-ориентированных методов решения задач, т.е. на разработку программ, способных решать «человеческие задачи».

Исследовательским полигоном для развития методов искусственного интеллекта на первом этапе являлись всевозможные игры, головоломки, математические задачи (задача об обезьянах и бананах, милиционерах и людоедах, Ханойской башне, игра в 15 и др.). В конце 1960-х гг. стали делаться первые попытки применения разработанных методов для решения задач не в искусственных, а в реальных проблемных средах. Они натолкнулись на большие трудности, связанные прежде всего с проблемами описания знаний о внешнем мире, организации их хранения и достаточно эффективного поиска, введения в память ЭВМ новых знаний и устранения устаревших (в том числе автоматического их извлечения из среды), проверки полноты и непротиворечивости знаний и т.п. Эти проблемы привели к постановке задачи создания интегральных роботов, т.е. таких устройств, которые реализовали бы целый спектр «интеллектуальных» функций, таких, как восприятие информации о внешней среде, целенаправленное поведение, формирование действий, обучение, общение с человеком и другими роботами. Для формирования целенаправленного поведения интегральный робот должен прежде всего обладать необходимым комплексом знаний о реальном мире, в котором он функционирует. Эти знания должны быть заложены в робот в виде модели внешнего мира или, точнее, модели проблемной среды, т.е. той части внешнего мира, которая существенна для решения задач, ставящихся перед роботом. Модель проблемной среды — это совокупность взаимосвязанных сведений, необходимых и достаточных для решения соответствующего класса задач. В систему знаний робота должны быть заложены и алгоритмы, позволяющие воспроизводить «мысленные» преобразования среды и строить на этой основе план решения очередной задачи. Проведение работ, связанных с созданием интегральных роботов, можно считать вторым этапом исследований по искусственному интеллекту.

С середины 1970-х гг. начался третий этап исследований систем искусственного интеллекта. Его характерной чертой явилось смещение центра внимания исследователей с создания автономно функционирующих систем, самостоятельно (или в условиях ограниченного общения с человеком) решающих в реальной среде поставленные перед ними задачи, к созданию человеко-машинных систем, соединяющих в единое целое интеллект человека и способности вычислительных машин для достижения общей цели — решения задачи, поставленной перед интегральной человеко-машинной решающей системой. На первый план выдвинулась не разработка отдельных методов машинного решения задач, а разработка методов и средств, обеспечивающих тесное взаимодействие человека и вычислительной системы в течение всего процесса решения задачи с возможностью оперативного внесения человеком изменений в ходе этого процесса.

Представление знаний в системах искусственного интеллекта. Теория представления знаний — фундаментальнейший раздел искусственного интеллекта. Ее назначение — найти такие способы описания и представления фактов, общих сведений, закономерностей, правил и предписаний об окружающем мире, которые позволят использовать все эти знания с помощью некоторых универсальных и формальных процедур анализа, рассуждения и синтеза, доступных для программной реализации на ЭВМ. Для реализации этих универсальных процессов разработаны специальные логико-алгоритмические языки, позволяющие объединить вычислительные, комбинаторные и логические шаги в обработке сложноорганизованной информации (например, язык «Лисп»).

Традиционно выделяются две группы методов представлений знаний — декларативные и процедурные. В *декларативных методах* знания — это данные, так или иначе структурированные. В *процедурных методах* знания также представляются в ЭВМ структурами данных, но при этом с элементами структур ассоциируются некоторые специализированные процедуры. В группе декларативных методов представления знаний выделяются логические и сетевые (основанные на аппарате семантических сетей).

Основная идея логического подхода к представлению знаний состоит в том, чтобы рассматривать всю систему знаний, необходимую для решения каких-то задач как совокупность фактов (утверждений). Факты представляются как формулы в некоторой логике (первого или высшего порядков, модальной, многозначной, нечеткой или какой-либо другой). Система знаний отображается совокупностью таких формул. Будучи представленной в компьютере, она образует базу знаний. Формулы неделимы и при модификации базы знаний могут лишь добавляться и удаляться.

Логические методы представления знаний обеспечивают простую и ясную систему для записи фактов, обладающую четко оп-

ределенной семантикой (по крайней мере, для методов, основанных на традиционной логике первого порядка). Каждый факт представляется в базе знаний только один раз, независимо от того, как он будет использоваться в дальнейшем.

Логические методы предоставляют также и развитый аппарат вывода новых фактов из тех, которые представлены в базе знаний явно. Основным инструментом манипуляции знаниями является операция логического вывода.

При этом в системах прямой дедукции новые знания получают, применяя выводы к фактам и правилам. Алгоритм завершает работу при получении некоторого знания, эквивалентного цели (или непосредственно влекущего ее). Систему прямой дедукции можно толковать как систему, основанную на теореме о прямой дедукции: формула G является логическим следствием формул $F_1, \dots, F_m$ тогда и только тогда, когда формула $F_1 \wedge \dots \wedge F_m \wedge \neg G$ является тождественно ложной.

В системах обратной дедукции выводы применяют к цели и к правилам, чтобы построить новые частичные цели. Алгоритм завершает работу, когда все частичные цели соответствуют фактам. Такую систему с логической точки зрения можно толковать как систему, в которой применяется теорема об обратной дедукции: формула G является логическим следствием формул $F_1, \dots, F_m$ тогда и только тогда, когда формула $\neg F_1 \vee \dots \vee \neg F_m \vee G$ является тавтологией (тождественно истинна).

Инструмент логического вывода определяет интенсивное использование логических методов при создании так называемых экспертных систем и всевозможных решателей задач. Имеется и другое применение этого аппарата, важное для любых систем искусственного интеллекта. Это — возможность контроля логической целостности базы знаний, т. е. ее непротиворечивости и соответствия предусмотренным правилам (ограничениям целостности).

Основная идея подхода к представлению знаний, основывающемуся на аппарате семантических сетей, состоит в том, чтобы рассматривать проблемную среду как совокупность объектов (сущностей) и связей (отношений) между ними. Объекты представляются при этом поименованными вершинами, а отношения — направленными поименованными ребрами. Система знаний отображается сетью (семантическая сеть) — ориентированным графом, составленным из поименованных вершин и ребер, или совокупностью таких сетей. Но было показано, что и этот метод представления знаний можно переписать и переинтерпретировать с помощью подходящего логического формализма.

Итак, мы видим, что роль математической логики во всех системах, связанных с приобретением, хранением и использованием знаний, исключительно велика. По существу, логика неизбежна в этих исследованиях. Она доставляет средство, хорошо подхо-

дящее для представления знаний и рассуждений. Она может рассматриваться как формализм для ссылок. Она может рассматриваться как метод подтверждения рассуждений и семантического анализа представленных знаний.

Поскольку конечная цель — представление знаний, основным критерием адекватности используемого логического языка является его выразительность. Системы искусственного интеллекта чаще всего ограничиваются применением языков логики высказываний и логики предикатов. Логика предикатов достаточно выразительна для решения многих проблем представления знаний в искусственном интеллекте и служит своего рода эталоном выразительности. (Тем не менее некоторые знания формализуются лишь в логических языках более высоких порядков.) Некоторые проблемы представления знаний и рассуждений решаемы лишь с помощью логических языков и ассоциированных с ними дедуктивных (аксиоматических) систем. В частности, благодаря точному определению принципов применения логических операторов и связок (отрицания, конъюнкции, дизъюнкции, равенства, кванторов общности и существования) логика позволяет выразить некоторые часто полезные парадигмы рассуждений. Например, логика предикатов с равенством дает возможность: а) выразить, что нечто обладает определенным свойством, не указывая, что именно (роль квантора существования); б) выразить, что каждый элемент некоего множества обладает определенным свойством, без указания того, что представляет собой каждый такой элемент (роль квантора общности); в) выразить, что хотя бы одно из двух утверждений ложно, не говоря, какое именно (роль конъюнкции); г) выразить, что хотя бы одно из двух утверждений истинно, не говоря, какое именно (роль дизъюнкции); д) явно сказать, что нечто ложно (роль отрицания); е) утверждать или оставлять неустановленным тот факт, что два различных выражения означают один и тот же объект (роль равенства).

Формальная логика связана с формализацией и обоснованием корректных рассуждений, которые также называются общезначимыми: их правильность несомненна при всех интерпретациях. Дедуктивные системы логики специально приспособлены для формализации этого класса рассуждений. Но рассуждения, которые желательно моделировать в приложениях искусственного интеллекта, не всегда общезначимы. Часто они приблизительны и неопределенны по сути или от неполноты, или неопределенности предпосылок. Выведенные из неопределенных рассуждений заключения должны допускать возможность отказа от них, если предпосылки, приведшие к принятию предположения о возможности этих заключений, больше не подтверждаются или если новая информация блокировала эту дедукцию. Дедуктивные системы классической логики не позволяют прямо формализовать такие рассуждения. Для

этих целей разработаны различные неклассические логические системы. Среди них — немонотонные логики Мак-Дермотта, логики умолчаний Рейтера, автоэпистемические логики Столнекера и Мура.

В заключение отметим, что математическая логика представляет собой важнейшее и мощнейшее средство анализа знаний и рассуждений. Она выполняет роль блюстителя логических принципов и правил в подавляющем большинстве систем искусственного интеллекта. Она может прямо использоваться для представления знаний и рассуждений. Она может пригодиться для ссылок и как эталон выразительности, модель компетенции, гарант элементарных логических принципов. Она определяет принципы и законы, незаменимые при решении многих проблем. Она позволяет анализировать смысл некоего представления знаний и обоснованность выводов. Она является преимущественно средством анализа знаний и рассуждений как таковых.

Экспертные системы. Экспертные системы — один из актуальнейших прикладных разделов искусственного интеллекта и одно из значительных его практических достижений. Они используются в многочисленных областях: интерпретация, прогноз, диагностика, мониторинг, планирование, проектирование, отладка, ремонт, управление.

С функциональной точки зрения под экспертной системой понимается вычислительная система (пакет прикладных программ), которая использует знания специалистов о некоторой конкретной узкоспециализированной предметной области и которая в пределах этой области способна принимать решения на уровне эксперта-профессионала. Экспертная система в отличие от решения задачи по алгоритму не исключает человека из процесса решения, а, наоборот, сохраняет за ним инициативу. В то же время экспертная система не является просто пассивным источником полезной информации наподобие книжного справочника или компьютерной базы данных. В нужные моменты экспертная система подсказывает дальнейшее направление расследования, помогает изменить план поиска, просчитывает варианты, развивает цепочки умозаключений в поисках противоречий.

Экспертная система должна содержать пять основных компонентов: интерфейс с пользователем, базу знаний, систему логического вывода (составляющими ядро любой экспертной системы), а также модуль приобретения знаний, модуль отображения и объяснения решений. В качестве внутренних языков в экспертной системе чаще всего используются логические языки. Описание задачи (запроса) пользователя на выбранном языке представления знаний поступает в подсистему логического вывода, которая, используя информацию из базы знаний, генерирует рекомендации по решению данной задачи. Основу базы знаний экспертной системы составляют факты и правила. В подсистеме логического вывода ре-

ализуется некоторая стратегия выбора соответствующего правила из базы знаний, тесно связанная со способом представления знаний в экспертной системе и характером решаемых задач.

Язык ПРОЛОГ в системах искусственного интеллекта. При помощи ПРОЛОГА были построены экспертные системы для многочисленных областей науки и практики: решение уравнений, медицина, законодательство, юриспруденция, архитектура, автоматизация заводского производства, проектирование электронных схем, синтез микропрограмм, анализ финансового положения, помощь в принятии решений. В ПРОЛОГЕ применяется стратегия решения задач с обратным ходом решения: он начинает свою работу с цели и продвигается назад до тех пор, пока не встретит факты.

Может ли машина мыслить. Вместе с созданием первых вычислительных машин и решением ими первых интеллектуальных задач возник вопрос о том, может ли машина мыслить и может ли она в своей «мыслительной» деятельности превзойти своего создателя — человека. Бурный прогресс вычислительной техники привел к тому, что многие ограничения «интеллекта» вычислительных машин оказались преодоленными за счет более изощренного искусства программирования, многие различия между человеком и машиной, которые до последнего времени казались весьма существенными, оказались только количественными. Машины овладели многими качествами, присущими интеллектуальной деятельности человека. Они научились приспосабливаться, быть «творческими», иметь целенаправленное поведение. Тем не менее любой человек, знакомый с вычислительными машинами, хорошо знает, что все эти действия весьма примитивны по сравнению с соответствующими действиями человека, и «интеллект» машин не идет ни в какое сравнение с человеческим. И все же возможно ли создание в обозримом будущем вычислительной машины, превосходящей по своим интеллектуальным возможностям человека? Дискуссий и мнений на этот счет было высказано необозримое количество. В заключение мы отметим одно из них. Оно приведено в брошюре [5.16] известного американского логика Э. Нагеля и опытного популяризатора науки Дж. Р. Ньюмена, переведенной на большинство европейских языков. Выдающаяся теорема Гёделя о неполноте формальной арифметики оказалась весьма привлекательной для многочисленных околomатематических исследований, включая философские. Стимулировала она и размышления в области философии искусственного интеллекта.

В заключительных замечаниях к своей брошюре Нагель и Ньюмен, во-первых, отмечают роль теоремы Гёделя в осознании того, что мы понимаем под процессом математического доказательства. «Выводы, к которым пришел Гёдель, ... показывают также, что имеется бесконечно много истинных арифметических предложений, которые нельзя формально вывести из произвольной данной систе-

мы аксиом посредством некоторого точного перечня правил вывода. Отсюда следует, что аксиоматический подход к арифметике натуральных чисел, кроме всего прочего, не в состоянии охватить всю область истинных арифметических суждений. Отсюда также вытекает, что то, что мы понимаем под процессом математического доказательства, не сводится к использованию аксиоматического метода. Формализованные аксиоматические процедуры доказательств основаны на некотором множестве выделенных и фиксированных с самого начала аксиом и правил вывода. Как видно уже из самих рассуждений, использованных в гёделевских доказательствах, изобретательность математиков в деле отыскания новых правил доказательства не поддается никаким априорным ограничениям. Таким образом, совершенно безнадежно рассчитывать на то, что понятию убедительного математического доказательства можно придать раз и навсегда четко очерченные логические формы.» [5.6, с. 57 — 58].

Во-вторых, Нагель и Ньюмен перекидывают мостик от теоремы Гёделя к проблеме мыслящей машины, искусственного интеллекта. «Заключения, к которым пришел Гёдель, порождают, естественно, и вопрос, можно ли построить вычислительную машину, сравнимую по своим «творческим» математическим возможностям с человеческим мозгом. Современные вычислительные машины обладают некоторым точно фиксированным запасом команд, которые умеют выполнять их элементы и блоки; команды соответствуют фиксированным правилам вывода некоторой формализованной аксиоматической процедуры. Таким образом, машина решает задачу, шаг за шагом выполняя одну из «встроенных» в нее заранее команд. Однако, как видно из гёделевской теоремы о неполноте, уже в элементарной арифметике натуральных чисел возникает бесчисленное множество проблем, выходящих за пределы возможностей любой конкретной аксиоматической системы, а значит, и недоступных для таких машин, сколь бы остроумными и сложными ни были их конструкции и с какой бы громадной скоростью ни проделывали они свои операции. Для каждой конкретной задачи в принципе можно построить машину, которой эта задача была бы под силу; но нельзя создать машину, пригодную для решения любой задачи» [5.6, с. 58 — 59].

Результаты исследований Гёделя конечно же не должны служить поводом для интеллектуального пессимизма. Они вовсе не означают принципиальной ограниченности человеческого мышления, наличия каких-то совершенно непознаваемых истин или несостоятельности строгого математического доказательства. Означают они лишь то, что возможности человеческого мышления не сводятся к полностью формализуемым процедурам, что нам еще предстоит открывать и изобретать новые принципы доказательств, что природа и возможности человеческого разума неизмеримо тоньше и богаче любой из известных пока машин.

ВСЕСИЛЬНА ЛИ ЛОГИКА В ПОЗНАНИИ ЗАКОНОВ МЫШЛЕНИЯ?

Вопрос состоит в том, насколько универсален и насколько всемогущ аксиоматический метод и строгий логический вывод в его рамках — важнейшие инструменты математической логики — в качестве единственно возможного способа доказательства истинности тех или иных утверждений.

Еще великий естествоиспытатель итальянец Галилео Галилей (1564—1642), исследовавший с помощью наклонной пизанской башни законы движения и изучавший аристотелеву логику, заметил: «Мне кажется, что логика учит познавать, правильно ли сделаны выводы из готовых уже рассуждений и доказательств; но чтобы она могла научить нас находить и строить такие рассуждения и доказательства — этому я не верю». Теперь уже общепризнано, что способность мышления к интуитивным суждениям является важным фактором, позволяющим мышлению открывать новые факты, новое знание, *находить* доказательства, *строить* рассуждения. «Доказывают при помощи логики, изобретают при помощи интуиции,» — категорически утверждает французский математик А. Пуанкаре¹. Его мнение разделяет русский математик В. А. Стеклов (1863—1925): «Метод открытия и изобретения один и тот же, та же интуиция, ибо при помощи логики никто ничего не открывает»².

И тем не менее логика, и прежде всего математическая логика — уникальная наука: она сама своими строгими методами доказательства установила границы своей применимости. Это произошло после доказательства в 1931 г. К. Гёделем его знаменитой теоремы о неполноте формальной арифметики. Не может быть подвергнута тотальной аксиоматизации вся математическая наука целиком. Могут быть аксиоматизированы лишь отдельные ее части. Аксиоматический подход не в состоянии охватить всю область истинных утверждений, т. е. *истинное утверждение не всегда может быть доказано*. Эти логические теоремы по существу разрушали восходящее к Лейбницу и Декарту мнение, будто всякое

¹ Пуанкаре А. О науке. — М. 1983. С. 360.

² Цит. по: Эрдниев П. М. О взаимосвязи логики и психологии в решении вопросов методики математики // Математика в школе. 1977. № 6. С. 68—70.

истинное утверждение подвластно обоснованию методами математического доказательства.

Отсюда можно извлечь по меньшей мере два вывода.

Вывод первый. Может быть, недоказуемыми являются лишь экзотические формулы геделевского типа, в которых зашифрованы утверждения, относящиеся к самим этим формулам. Может быть, выводимость лишь ненамного меньше истинности. Но в 1936 г. польским математиком А. Тарским был получен еще более сильный результат. Он доказал, что для достаточно богатых формальных теорий понятие истинности в них не может быть выражено на языке самой теории. Это уже означало, что дедуктивный или аксиоматический метод не всесилен в поисках истины и не может быть признан в этом деле единственно возможным, уникальным.

Теорема Тарского, включающая в себя теоремы Гёделя как частные следствия, наталкивает на мысль, что различие между истинностью и выводимостью (доказуемостью) довольно значительно. Но установить, насколько оно велико, удалось только сравнительно недавно. Все математические формулы были разбиты вначале на классы сложности так, что эти классы образовали расширяющуюся цепь и каждый класс содержал в себе предыдущий и, в свою очередь, содержался в последующем классе. С увеличением классов сложность формул в них возрастала. Затем было показано, что множество выводимых формул целиком содержится в самом нижнем, нулевом классе. И наконец, доказано, что множество истинных формул не помещается даже в тот предельный класс, который получается при стремлении показателя сложности к бесконечности. Известный математик Ю. И. Манин так прокомментировал эту ситуацию: «Выводимость находится на нижней ступеньке бесконечной лестницы, а истинность располагается где-то над всей лестницей».

Конечно, эти результаты, показывающие, что расстояние от доказуемости (выводимости) до истинности столь велико, могут служить солидным основанием для значительной доли пессимизма в оценке роли логики (и, в частности, математической логики) в процессе познания окружающего мира и истины. Некоторые определенные философы истолковывают эти результаты как полное отрицание роли логики в процессе познания, считая, что она нужна лишь для придания уже полученным результатам общепонятной и убедительной формы, а сам механизм получения этих результатов совершенно иной. Не следует истолковывать эти результаты и как полный крах формального подхода к математическим теориям. Эти результаты несомненно означают, что первоначальная, «максималистская» гильбертовская программа финитистского подхода к обоснованию математики не может быть реализована в полном объеме: нельзя построить математику как

некоторую фиксированную совокупность средств, которые можно было бы объявить единственно законными и с их помощью строить метатеории любых теорий. Невозможность полной формализации содержательно определенных математических теорий — это не недостаток подхода или концепции, а объективный факт, неустранимый никакой концепцией, «суровая правда» об устройстве мира, изучаемого этой теорией. Невозможность адекватной формализации теории означает, что надо либо искать формализуемые ею фрагменты, либо строить какую-то более сильную формальную теорию, которая, правда, снова будет неполна, но, быть может, будет содержать всю исходную теорию.

Рассматриваемые выдающиеся результаты Гёделя и Тарского демонстрируют не только слабость математической логики в процессах познания, но и ее силу, еще раз являя уникальность этой науки. Фактически средствами математической логики устанавливаются границы применимости самой математики. Наука с такими уникальными возможностями не может быть бесполезна для дела познания окружающего мира, и думается, что ее будущие результаты заставят еще не раз как математиков, так и философов обратиться к их интерпретации.

Интересно отметить, что подобная ситуация, когда вдруг обнаруживается ограниченность того или иного научного метода, который доселе представлялся как всеобъемлющий и единственно мыслимый, характерна не только для математики. Так, в биологии мы привыкли думать, что все ныне живущее образовалось в результате естественного отбора в соответствии с известной теорией Дарвина. Но в самые последние годы ученые, исследовав микроструктуру органической материи, сделали поразительный вывод: если бы возникновение и развитие жизни на нашей планете, считая от появления на Земле первых живых молекул до человека, шло по Дарвину, оно потребовало бы намного больше времени, чем это произошло в действительности. Значит, естественный отбор — не единственный движущий фактор эволюции¹.

Вывод второй по существу уже сделан: то, что мы *интуитивно* понимаем под процессом математического доказательства, не сводится к использованию лишь аксиоматического метода и законов традиционной и математической логики. Этот вывод сформулирован в *Меморандуме американских математиков*²: «Математическое мышление не сводится к дедуктивным рассуждениям, оно не состоит только в формальных доказательствах. Мыслительные процессы, подсказывающие нам, что доказывать и как доказывать, также составляют часть математического мышления, как и само

¹ Карпенков С. Концепции современного естествознания. — М. — 2000.

² Меморандум американских математиков // Математика в школе. 1964. № 4. С. 90—92.

доказательство, которым они завершаются. Выделять понятие, приспособленное к конкретной ситуации, обобщать исходя из наблюдаемых частных случаев, рассуждать по индукции, по аналогии и находить интуитивные доводы для выделяемой догадки — все это математические способы мышления».

Совершенно безнадежно рассчитывать на то, что понятию убедительного математического доказательства можно придать раз и навсегда очерченные логические формы, связанные с определенными аксиомами и правилами вывода. Логика традиционная и выросшая на ее основе математическая логика отражают лишь часть тех законов, по которым происходит наше мышление, по которым мышление производит истинные утверждения.

В связи с такой ситуацией математическая наука пытается найти новые нетрадиционные подходы к проблеме доказательности истинности, к пониманию того, что есть доказательство, что следует считать доказанным и обоснованным. Один из таких подходов напрямую связан с вероломным вторжением компьютеров во все сферы жизни, в науку, в математику. Эту тенденцию отмечает известный российский математик академик РАН В.А. Садовничий, считая, что математика вынуждена признать права на такую же математическую договоренность и доказательность за другими схемами рассуждений, отличными от классического логического вывода, основанного на аксиомах. «В частности, — говорит он, — за аргументацией с помощью примеров, за рассуждениями по аналогии или путем ассоциаций, за использованием мнений авторитетных специалистов (экспертов). Наконец, за доказательствами, в основе которых лежит простая вера в сходимость бесконечного вычислительного процесса. Ведь никакое вычисление нельзя продолжать бесконечно, и где-то, на каком-то шаге мы его обрываем и полученную таким образом приближенную числовую величину принимаем за решение рассматриваемой задачи — за истину. Но сходимость многих вычислительных алгоритмов, используемых в машинных расчетах, не доказана в классическом понимании. Тем не менее именно на этой вере возведено практически все здание современных компьютерных вычислений и приложений. Многообразные вычислительные процедуры существуют и используются, но их строгое теоретическое обоснование либо отсутствует, либо остается неполным... Таким образом, ясно, что с появлением компьютеров мир математики стал меняться. Изменяются не только математическое мышление, математические подходы, но и научное мировоззрение в целом»¹. Именно такова ситуация с современным решением проблемы четырех красок: полученное доказательство чрезвычайно длинно, к тому же суще-

¹ Садовничий В.А. Математическое образование: настоящее и будущее // Математика. 2000. № 40. С. 3.

ственно (до нескольких тысяч часов машинного времени) использует компьютер для проверки большого количества промежуточных утверждений¹.

Подобная тенденция подмечается и другими исследователями, считающими, что в будущем «математическая теория, узаконивающая заведомо нестрогие переходы, будет лучше соответствовать реальному процессу»².

По существу, это означает, что математика и в этом своем качестве начинает теснее сближаться с гуманитарными науками, в которых подобные нестрогие (с точки зрения математики) критерии и нормы истинности вырабатывались на протяжении столетий и прочно вошли в их обиход. Выразительная характеристика такого подхода к проблеме доказательности в гуманитарных науках дана известным филологом академиком А. А. Зализняком (опубликовано, кстати, в журнале «Успехи математических наук»): «У гуманитария же вообще нет возможности что-либо доказать в абсолютном смысле этого слова. Если слово «доказать» и применяется иногда в гуманитарных науках, то лишь в несколько ином, более слабом смысле, чем в математике. Строгого определения для этого «доказательства в слабом смысле», по-видимому, дать невозможно. Практически имеется в виду, что предложенная гипотеза, во-первых, полностью согласуется со всей совокупностью уже известных фактов, имеющих отношение к рассматриваемой проблеме, во-вторых, является почему-либо безусловно предпочтительной из всех прочих мыслимых гипотез, удовлетворяющих первому требованию. В отличие от математического доказательства «доказательство в слабом смысле» может и рухнуть, если откроются новые факты или будет выяснено, что автор не учел каких-то принципиально мыслимых возможностей. Все это не значит, однако, что утверждения гуманитарных наук вообще не могут претендовать ни на какую точность и надежность и что в этой области любая гипотеза не хуже и не лучше, чем любая другая. В гуманитарных науках, так же, как, например, в естествознании, долгим опытом выработаны критерии, позволяющие оценивать степень обоснованности того или иного утверждения даже при условии невозможности доказательства в абсолютном смысле»³.

Как это ни покажется парадоксальным, но фактически и в математике — как в научной, так и в школьной — реально используются такие доказательства, которые далеки от строгих ло-

¹ Самохин А. В. Проблема четырех красок: неоконченная история доказательства // Соросовский образовательный журнал. 2000. Т. 6, № 7. С. 91 — 96.

² Беляев Е. А., Перминов В. Я. Философские и методологические проблемы математики. — М., 1981. С. 133.

³ Зализняк А. А. Лингвистика по А. Т. Фоменко // Успехи математических наук. 2000. Т. 55, № 2. С. 163.

гических канонов, а представляя собой рассуждения, которые призваны убедить определенный круг людей в справедливости того или иного утверждения. «В математике, — отмечает Г. В. Дорофеев¹, — при оценке доказанности той или иной теоремы фактически пользуются методом «экспертной оценки», а в роли экспертов выступают коллеги — математики, слушатели докладов на семинарах, рецензенты и члены редколлегий математических журналов». Аналогичную мысль высказывает Ю. И. Манин²: «Доказательство становится таковым только в результате социального акта «принятия доказательства». Это относится к математике в той же мере, что и к физике, лингвистике или биологии. Эволюция признанных критериев доказательности — почти не исследованная тема в истории науки... Каждое предложенное доказательство апробируется на приемлемость математиками, иногда нескольких поколений».

Эти обстоятельства накладывают на такое понимание доказательства субъективный оттенок: то, что убеждает одного, может быть неубедительным для другого. В этом смысле может показаться, что и в математике понятие доказательства также весьма расплывчато и неопределенно и напоминает по своей строгости доказательства в гуманитарных науках. Тем не менее это не так. «Математика не существовала бы как наука, — справедливо считает Г. В. Дорофеев³, — если бы не существовало более или менее единого мнения относительно того, является ли данное рассуждение доказательством. И действительно, в каждом разделе математики имеется определенный стандарт строгости, хотя формально он нигде не описан, нигде не зафиксирован. Более того, как показывает история математики, этот стандарт изменялся по мере развития математики, и то, что казалось строгим, скажем, в XVII—XVIII вв., подвергалось критике в XIX в., а многие рассуждения математиков XIX в. были сочтены совершенно неубедительными математиками и особенно логиками XX в.»

Позволим себе высказать гипотезу: критерии доказательности в математике, строгости математических доказательств развивались и совершенствовались вместе с развитием логики. Не случайно само понятие доказательства появилось в древнегреческой математике вместе со становлением логики как науки, а современного уровня строгости оно достигло в XX в. вместе со становлением логики как математической науки и превращением ее в математическую логику. Поэтому, хотя в современной математике и нет строгого определения понятия строгого доказательства математической теоремы, тем не менее каждый математик осознает

¹ *Дорофеев Г. В.* Математика для каждого. — М., 1999. С. 219.

² *Манин Ю. И.* Доказуемое и недоказуемое. — М., 1979. С. 53—54.

³ *Дорофеев Г. В.* Математика для каждого. — М., 1999. С. 220.

эту строгость *интуитивно*. За каждым математическим доказательством он ощущает величественную тень незыблемых логических законов и критериев, выработанных математической логикой на протяжении XX в. Хотя рассматриваемое им доказательство и не во всех своих деталях именно таково, интуитивно он осознает, что оно может быть преобразовано в такое, пусть даже для этого потребуются приложить очень много усилий и потратить очень много времени. Важно ощущать принципиальную возможность такой трансформации. Такое интуитивное ощущение строгости должно быть воспитано как в будущем ученом-математике, так и в будущем учителе математики. У каждого из них базой для этого воспитания будет служить фундаментальная логическая подготовка, заложенная в юношеском возрасте. Именно она будет служить источником интуиции о логической строгости, будет подпитывать это интуитивное чувство.

Список литературы

1. Традиционная логика

1. *Аристотель*. Сочинения: В 4 т. — М., 1976—1981.
2. *Ахманов А. С.* Логическое учение Аристотеля. — М., 1960.
3. *Бойко А. П.* Занимательная логика (задачи и упражнения). — М., 1994.
4. *Бойко А. П.* Краткий курс логики. — М., 1995.
5. *Бочаров В. А.* Аристотель и традиционная силлогистика. — М., 1984.
6. *Гетманова А. Д.* Логика. — М., 1986.
7. *Гетманова А. Д., Никифоров А. А., Панов М. И.* Логика (10—11 классы). — М., 1995.
8. *Гетманова А. Д.* Занимательная логика для школьников (Ч. 1: Для 4—7 классов). — М., 1998.
9. *Горский Д. П.* Логика. — М., 1963.
10. *Горский Д. П., Ивин А. А., Никифоров А. А.* Краткий словарь по логике. — М., 1991.
11. *Зебет В.* Элементарная логика: Пер. с нем. — М., 1985.
12. *Ивин А. А.* Строгий мир логики. — М., 1988.
13. *Ивин А. А.* Искусство правильно мыслить. — М., 1990.
14. *Иелев Ю. В.* Курс лекций по логике. — М., 1988.
15. *Игошин В. И.* Логика с элементами математической логики. — Саратов, 2004.
16. *Кириллов В. И., Старченко А. А.* Логика. — М., 1987.
17. Логика / Под. ред. Г. А. Левина. — Минск, 1974.
18. *Лукаевич Я.* Аристотелевская силлогистика с точки зрения современной формальной логики: Пер. с англ. — М., 1959.
19. *Мельников В. Н.* Логические задачи. — Киев; Одесса, 1989.
20. *Переверзев В. Н.* Логистика: Справочная книга по логике. — М., 1995.
21. *Розен В. В.* Дедуктивные умозаключения. — Саратов, 1990.
22. *Смирнов В. А.* Погружение силлогистики в исчисление предикатов // Логическая семантика и модальная логика. — М., 1967.
23. *Стяжкин Н. И.* Логика с элементами математической логики. — М., 1974.
24. *Субботин А. Л.* Теория силлогистики в современной формальной логике. — М., 1965.
25. *Субботин А. Л.* Традиционная и современная формальная логика. — М., 1969.
26. Упражнения по логике / Под ред. В. И. Кириллова. — М., 1990.

2. Логика и наука. Логика и математика. Основания математики

1. *Вейль Г.* Математика и логика: Пер. с англ. // Математика. Теоретическая физика. — М., 1984.
2. *Гетманова А. Д.* О соотношении математики и логики // Логические исследования. — М., 1959.
3. *Гильдерман Ю. И.* Вооружившись интегралом... — Новосибирск, 1980.

4. Гончаров С. С., Ершов Ю. Л., Самохвалов К. Ф. Введение в логику и методологию науки. — М., 1994.
5. Зиновьев А. А. Основы логической теории научных знаний. — М., 1967.
6. Йех Т. Теория множеств и метод форсинга: Пер. с англ. — М., 1973.
7. Кац М., Улам С. Математика и логика (ретроспектива и перспектива): Пер. с англ. — М., 1971.
8. Колмогоров А. Н. К логическим основам теории информации и теории вероятностей // Проблемы передачи информации. — М., 1969. Т. 5. Вып. 3. — С. 3—7.
9. Копнин П. В. Логические основы науки. — Киев, 1968.
10. Коэн П. Дж. Теория множеств и континуум-гипотеза: Пер. с англ. — М., 1969.
11. Куратовский К., Мостовский А. Теория множеств: Пер. с англ. — М., 1970.
12. Кусраев А. Г. Булевы алгебры и булевозначные модели // Соросовский образовательный журнал. — 1997. — № 9. — С. 116—122.
13. Ледли Р., Ластед Л. Медицинская диагностика и методы выбора решений: Пер. с англ. // Математические проблемы в биологии. — М., 1966.
14. Логическая структура научного знания / Сб. статей под ред. П. В. Таванец. — М., 1965.
15. Нейскашова Е. В. Идеи нестандартного анализа в истории науки и в преподавании // Математика в школе. — 1999. — № 3. — С. 76—79.
16. Применения логики в науке и технике / Сб. статей под ред. П. В. Таванец. — М., 1960.
17. Расёва Е., Сикорский Р. Математика метаматематики: Пер. с англ. — М., 1972.
18. Рвачёв В. Л. Геометрические приложения алгебры логики. — Киев, 1967.
19. Сикорский Р. Булевы алгебры: Пер. с англ. — М., 1969.
20. Смирнов В. А. Логические методы анализа научного знания. — М., 1987.
21. Тарский А. Введение в логику и методологию дедуктивных наук: Пер. с англ. — М., 1948.
22. Успенский В. А. Что такое нестандартный анализ? — М., 1987.
23. Формальная логика и методология науки / Сб. статей под ред. П. В. Таванец. — М., 1964.
24. Френкель А., Бар-Хиллел И. Основания теории множеств: Пер. с англ. — М., 1966.

3. Основания геометрии

1. Больяй Я. Appendix: Пер. с лат. — М.; Л., 1950.
2. Болтянский В. Г. Загадка «аксиомы параллельных» // Квант. — 1991. — № 4. — С. 8—13.
3. Болтянский В. Г., Волович М. Б., Семушин А. Д. Векторное изложение геометрии. — М., 1982.
4. Винберг Э. В. О неевклидовой геометрии // Соросовский образовательный журнал. — 1996. — № 3. — С. 104—109.
5. Гильберт Д. Основания геометрии: Пер. с нем. — М.; Л., 1948.
6. Гиндикин С. Г. Феликс Клейн // Квант. — 1975. — № 12.
7. Гиндикин С. Г. Волшебный мир Анри Пуанкаре // Квант. — 1976. — № 3.
8. Делоне Б. Н. Краткое изложение доказательства непротиворечивости планиметрии Лобачевского. — М., 1953.

9. *Ефимов Н. В.* Высшая геометрия. — М., 1961.
10. *Каган В. Ф.* Лобачевский. — М.; Л., 1944.
11. *Каган В. Ф.* Основания геометрии (Учение об основании геометрии в ходе его исторического развития). — М.; Л., 1949.
12. *Каган В. Ф.* Очерки по геометрии. — М., 1963.
13. Комментарии к введениям книги Евклида (отрывок) // Историко-математические исследования: Вып. 11. — М., 1958.
14. *Костин В. И.* Основания геометрии. — М., 1948.
15. *Кутузов В. В.* Геометрия Лобачевского и элементы оснований геометрии. — М., 1955.
16. *Лаптев Б. Л.* Н. И. Лобачевский и его геометрия. — М., 1976.
17. *Лобачевский Н. И.* Геометрические исследования по теории параллельных линий // Квант. — 1992. — № 12. — С. 3—10.
18. *Рабинович В. Л.* Доказательство непротиворечивости геометрии Лобачевского на основании системы аксиом школьного курса геометрии // Математика в школе. — 1977. — № 1.
19. *Рашевский П. К.* Геометрия и ее аксиоматика // Математическое просвещение. Вып. 5. — С. 73—98.
20. *Рагановский Н. М., Столяр А. А.* Векторное построение стереометрии. — Минск, 1974.
21. *Розенфельд Б. А.* История неевклидовой геометрии. — М., 1976.
22. *Смилга В.* Как начиналась геометрия // Квант. — 1992. — № 2. — С. 11—17.
23. *Соловьев Ю. Н.* Николай Иванович Лобачевский // Квант. — 1992. — № 11. — С. 2—9.
24. *Трайнин Я. Л.* Основания геометрии. — М., 1961.
25. *Широков П. А.* Краткий очерк основ геометрии Лобачевского. — М., 1983.

4. Числовые системы

1. *Андронов И. К.* Арифметика (развитие понятия числа и действий над числами). — М., 1962.
2. *Блох А. Ш.* Числовые системы. — Минск, 1982.
3. *Гоним Е. Г.* Теоретическая арифметика. — М., 1959.
4. *Демидов И. Т.* Основания арифметики. — М., 1963.
5. *Игошин В. И.* Конспект лекций по курсу «Числовые системы». — Саратов, 1999.
6. *Кантор И. Л., Солодовников А. С.* Гиперкомплексные числа. — М., 1973.
7. *Колмогоров А. Н.* Обобщение понятия числа. Неотрицательные рациональные числа // Математика — наука и профессия. — М., 1988. — С. 255—267.
8. *Ландау Э.* Основы анализа (Действия над целыми, рациональными, иррациональными, комплексными числами): Пер. с нем. — М., 1947.
9. *Ларин С. В.* Числовые системы. — М., 2001.
10. *Нечаев В. И.* Числовые системы. — М., 1975.
11. *Понтрягин Л. С.* Обобщения чисел. — М., 1986.
12. *Проскураков И. В.* Числа и многочлены. — М., 1965.
13. *Проскураков И. В.* Понятия множества, группы, кольца и поля. Теоретические основы арифметики // Энциклопедия элементарной математики. Т. 1. — М.; Л., 1951. — С. 75—252.
14. *Сильвестров В. В.* Системы чисел // Соросовский образовательный журнал. — 1998. — № 8. — С. 121—127.

15. *Феферман С.* Числовые системы: Пер. с англ. — М., 1971.

16. *Яглом И. М.* Комплексные числа. — М., 1963.

5. Учебники и пособия по математической логике, рекомендуемые студентам педагогических вузов

1. *Беран Л.* Упорядоченные множества: Пер. с чеш. — М., 1981.

2. *Варпаховский Ф. Л.* Элементы теории алгоритмов. — М., 1979.

3. *Ефремов Г. О.* Алгебра логики и контактные схемы. — М., 1969.

4. *Игошин В. И.* Математическая логика и теория алгоритмов. — Саратов, 1991.

5. *Игошин В. И., Петрова Е. С.* Множества и графы. — Саратов, 1981.

6. *Иножарский В. К.* Математическая логика и алгоритмы. — Орел, 1970.

7. *Калбертсон Дж. Т.* Математика и логика цифровых устройств: Пер. с англ. — М., 1965.

8. *Калужнин Л. А.* Что такое математическая логика? — М., 1964.

9. *Криницкий Н. А.* Алгоритмы вокруг нас. — М., 1984.

10. *Лихтарников Л. М., Сукачёва Т. Г.* Математическая логика: Курс лекций. Задачник-практикум и решения. — СПб., 1999.

11. Математическая логика / Под ред. А. А. Столяра. — Минск, 1991.

12. *Матросов В. Л.* Теория алгоритмов. — М., 1989.

13. *Мендельсон Э.* Введение в математическую логику: Пер. с англ. — М., 1976.

14. *Михайлов А. В., Рыжова Н. И., Швецкий М. В.* Лекции по основам математической логики. Формальные системы нулевого порядка. — СПб., 1998.

15. *Моценский В. А.* Лекции по математической логике. — Минск, 1973.

16. *Нагель Э., Ньюмен Д.* Теорема Гёделя: Пер. с англ. — М., 1970.

17. *Непейвода Н. Н.* Прикладная логика. — Ижевск, 1997.

18. *Никольская И. Л.* Математическая логика. — М., 1981.

19. *Новиков П. С.* Элементы математической логики. — М., 1973.

20. *Пензов Ю. Е.* Элементы математической логики и теории множеств. — Саратов, 1968.

21. Современные основы школьного курса математики / Н. Я. Виленкин, К. И. Дуничиб, Л. А. Калужнин, А. А. Столяр. — М., 1980.

22. *Столл Р. Р.* Множества. Логика. Аксиоматические теории: Пер. с англ. — М., 1968.

23. *Столяр А. А.* Элементарное введение в математическую логику. — М., 1965.

24. *Трахтенброт В. А.* Алгоритмы и вычислительные автоматы. — М., 1974.

25. *Успенский В. А., Вережагин Н. К., Плиско В. Б.* Вводный курс математической логики. — М., 1991.

26. *Фрейденталь Х.* Язык логики: Пер. с англ. — М., 1969.

27. *Эдельман С. Л.* Математическая логика. — М., 1975.

28. *Энгелер Э.* Метаматематика элементарной математики: Пер. с нем. — М., 1987.

6. Сборники задач

1. *Байиш Ж.-К.* Логические задачи: Пер. с фр. — М., 1983.

2. *Гаврилов Г. П., Сапоженко А. А.* Сборник задач по дискретной математике. — М., 1977.

3. Гиндикин С. Г. Алгебра логики в задачах. — М., 1972.
4. Гохман А. В., Спивак М. А., Розен В. В. Сборник задач по математической логике и алгебре множеств. — Саратов, 1969.
5. Драбкина М. Е. Логические упражнения по элементарной математике. — Минск, 1965.
6. Игошин В. И. Задачник-практикум по математической логике. — М., 1986.
7. Игошин В. И. Тетрадь по математической логике с печатной основой. — Саратов, 1996—1999.
8. Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов. — М., 1975.
9. Михайлов А. В., Рыжова Н. И., Швецкий М. В. Упражнения по основам математической логики. Формальные системы нулевого порядка. — СПб., 1998.
10. Рыжова Н. И., Швецкий М. В. Упражнения по основам формальной символической логики. — СПб., 1998.
11. Смаллиан Р. М. Принцесса или тигр?: Пер. с англ. — М., 1985.
12. Шапиро С. И. Решение логических и игровых задач. — М., 1984.

7. Фундаментальные пособия по математической логике и смежным вопросам алгебры

1. Ван дер Варден Б. Л. Алгебра: Пер. с нем. — М., 1976.
2. Гильберт Д., Аккерман В. Основы теоретической логики: Пер. с нем. — М., 1947.
3. Гильберт Д., Бернайс П. Основания математики. Логические исчисления и формализация арифметики: Пер. с англ. — М., 1979.
4. Гладкий А. В. Математическая логика. — М., 1998.
5. Гудстейн Р. Л. Математическая логика: Пер. с англ. — М., 1961.
6. Ершов Ю. Л., Палютин Е. А. Математическая логика. — М., 1979.
7. Ершов Ю. Л., Тайманов А. Д., Тайцлин М. А. Элементарные теории // Успехи математических наук. 1965. — Т. 20. — № 4. — С. 37—108.
8. Карри Х. Основания математической логики: Пер. с англ. — М., 1969.
9. Кейслер Г., Чэн Ч. Теория моделей: Пер. с англ. — М., 1977.
10. Клаус Г. Введение в формальную логику: Пер. с нем. — М., 1960.
11. Клини С. Введение в метаматематику: Пер. с англ. — М., 1957.
12. Клини С. Математическая логика: Пер. с англ. — М., 1973.
13. Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. — М., 1982.
14. Колмогоров А. Н., Драгалин А. Г. Математическая логика. Дополнительные главы. — М., 1984.
15. Кондаков Н. И. Логический словарь-справочник. — М., 1975.
16. Линдон Р. Заметки по логике: Пер. с англ. — М., 1968.
17. Манин Ю. И. Доказуемое и недоказуемое. — М., 1979.
18. Марков А. А. Элементы математической логики. — М., 1984.
19. Маслов С. Ю. Теория дедуктивных систем и ее применение. — М., 1986.
20. Салий В. Н. Решетки с единственными дополнениями. — М., 1984.
21. Слупецкий Е., Борковский Л. Элементы математической логики и теории множеств: Пер. с пол. — М., 1965.
22. Смальян Р. Теория формальных систем: Пер. с англ. — М., 1981.
23. Справочная книга по математической логике: В 4 ч.: Пер. с англ.; Под ред. Дж. Барвайса. — М., 1982—1983.
24. Чёрч А. Введение в математическую логику: Пер. с англ. — М., 1960.

25. Шёнфилд Дж. Математическая логика: Пер. с англ. — М., 1975.
26. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М., 1966.

8. Теория алгоритмов

1. Булос Дж., Джеффри Р. Вычислимость и логика: Пер. с англ. — М., 1994.
2. Еришов Ю. Л. Теория нумераций. — М., 1977.
3. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций: Пер. с англ. — М., 1983.
4. Криницкий Н. А. Алгоритмы вокруг нас. — М., 1977.
5. Макаренков Ю. А., Столяр А. А. Что такое алгоритм? — Минск, 1989.
6. Мальцев А. И. Алгоритмы и рекурсивные функции. — М., 1965.
7. Манин Ю. И. Вычислимое и невычислимое. — М., 1980.
8. Марков А. А., Нагорный Н. М. Теория алгоритмов. — М., 1984.
9. Машина Тьюринга // Квант. 1992. № 7.
10. Машины Тьюринга и вычислимые функции: Пер. с нем. / Г.-Д. Эббингауз, Ф.-К. Ман, К. Якобс и др. — М., 1972.
11. Минский М. Вычисления и автоматы: Пер. с англ. — М., 1971.
12. Нагель Э., Ньюмен Дж. Р. Теорема Гёделя: Пер. с англ. — М., 1970.
13. Петер Р. Рекурсивные функции: Пер. с нем. — М., 1954.
14. Роджерс Х. Теория рекурсивных функций и эффективная вычислимость: Пер. с англ. — М., 1972.
15. Семенов А. Л., Успенский В. А. Математическая логика в вычислительных науках и вычислительной практике // Вестник АН СССР. — 1986. — № 7. — С. 93—103.
16. Трахтенброт Б. А. Алгоритмы и вычислительные автоматы. — М., 1974.
17. Успенский В. А. Лекции о вычислимых функциях. — М., 1960.
18. Успенский В. А. Машина Поста. — М., 1979—1988.
19. Успенский В. А. Теорема Гёделя о неполноте. — М., 1982.
20. Успенский В. А., Семенов А. Л. Теория алгоритмов: основные открытия и приложения. — М., 1987.

9. Математическая логика и компьютеры

1. Анго А. Математика для электро- и радиоинженеров: Пер. с фр. — М., 1965.
2. Андерсон Р. Доказательство правильности программ: Пер. с англ. — М., 1982.
3. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем. — М., 1997.
4. Бузук Г. Л. Логика и компьютер. — М., 1971.
5. Ван Хао. На пути к механической математике // Кибернетический сборник. Вып. 5. — М., 1962. — С. 114—165.
6. Вычислительные машины и мышление: Пер. с англ. / Сб. статей под ред. Э. Сейгенбаума и Дж. Фельдмана. — М., 1967.
7. Гаек П., Гавранек Т. Автоматическое образование гипотез: Пер. с англ. — М., 1984.
8. Грис Д. Наука программирования: Пер. с англ. — М., 1984.
9. Еришов А. П. Введение в теоретическое программирование. — М., 1977.
10. Игошин В. И. Контактные схемы — элементы ЭВМ. — Саратов, 1991.
11. Кайберг Г. Вероятность и индуктивная логика: Пер. с англ. — М., 1978.

12. *Калабеков Б. А., Мамзелев И. А.* Цифровые устройства и микропроцессорные системы. — М., 1987.

13. *Калбертсон Дж. Т.* Математика и логика цифровых устройств: Пер. с англ. — М., 1965.

14. *Мелихов А. Н., Чефранов А. Г.* Применение ЭВМ для решения задач математической логики. — Таганрог, 1988.

15. *Минский М.* Вычисления и автоматы: Пер. с англ. — М., 1971.

16. *Непомнящий В. А., Рякин О. М.* Прикладные методы верификации программ. — М., 1988.

17. *Нивергельт Ю., Фаррар Дж., Рейнголд Э.* Машинный подход к решению математических задач: Пер. с англ. — М., 1977.

18. *Ньюэлл А., Шоу Дж. С., Саймон Г. А.* Процессы творческого мышления: Пер. с англ. // Психология мышления. — М., 1965. — С. 500—530.

19. *Поспелов Д. А.* Логические методы анализа и синтеза схем. — М., 1968.

20. *Робинсон Дж. А.* Машинно-ориентированная логика, основанная на принципе резолюции: Пер. с англ. и нем. // Сб. статей под ред. А. М. Матюшкина. Вып. 7. — М., 1970. — С. 194—218.

21. *Трачик В.* Дискретные устройства автоматики: Пер. с пол. — М., 1978.

22. *Тьюринг А.* Может ли машина мыслить?: Пер. с англ. — М., 1960.

23. *Хилтон А. М.* Логика и цепи переключения: Пер. с англ. — М.; Л., 1962.

24. *Финк Д.* Вычислительные машины и человеческий разум: Пер. с англ. — М., 1967.

25. *Флорин Ж.* Синтез логических устройств и его автоматизация: Пер. с фр. — М., 1966.

26. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем: Пер. с англ. — М., 1983.

27. *Шестаков В. И.* Математическая логика и автоматика // Математика в школе. — 1958. — № 6; — 1959. — № 1.

28. *Шанин Н. А.* Алгоритм машинного поиска естественного логического вывода в исчислении высказываний. — М.; Л., 1965.

10. Математическая логика и информатика, искусственный интеллект

1. *Арбиб М.* Мозг, машина и математика: Пер. с англ. — М., 1968.

2. *Вейцбаум Дж.* Возможности вычислительных машин и человеческий разум: Пер. с англ. — М., 1982.

3. *Беркли Э.* Символическая логика и разумные машины: Пер. с англ. — М., 1961.

4. *Борщев В. Б.* Логический подход к описанию реляционных баз данных: Пер. с англ. // Семиотика и информатика. 1980. Вып. 16. С. 78—122.

5. *Брауэр Ф. Л., Гооз Г.* Информатика. Вводный курс: В 2 ч. — М., 1990. Ч. 2. Приложение Е. К истории информатики. С. 656—680.

6. *Грэй П.* Логика, алгебра и базы данных: Пер. с англ. — М., 1989.

7. *Гутчин И. Б.* Кибернетические модели творчества. — М., 1969.

8. *Дейт К.* Введение в системы баз данных: Пер. с англ. — М., 1980.

9. *Ефимов Е. И.* Решатели интеллектуальных задач. — М., 1982.

10. *Ефимов Н. Н., Фролов В. С.* Основы информатики. Введение в искусственный интеллект. — М., 1991.

11. Искусственный интеллект: В 3 кн.: Справочник. — М., 1990.

12. *Ковальски Р.* Логика в решении проблем: Пер. с англ. — М., 1990.

13. *Кузин Е. С.* Интеллектуализация ЭВМ. — М., 1989.

14. Логика и компьютер: моделирование рассуждений и проверка правильности программ / Н. А. Алешина, А. М. Анисов и др. — М., 1990.

15. *Лорьер Ж. -Л.* Системы искусственного интеллекта: Пер. с фр. — М., 1991.
16. *Малпас Дж.* Реляционный язык ПРОЛОГ и его применение: Пер. с англ. — М., 1990.
17. *Мейер Д.* Теория реляционных баз данных: Пер. с англ. — М., 1987.
18. *Мичи Д., Джонстон Р.* Компьютер — творец: Пер. с англ. — М., 1987.
19. *Нильсон Н.* Принципы искусственного интеллекта: Пер. с англ. — М., 1985.
20. *Осуга С.* Обработка знаний: Пер. с яп. — М., 1989.
21. *Плоткин Б. И.* Универсальная алгебра, алгебраическая логика и базы данных. — М., 1991.
22. *Поспелов Д. А.* Фантазия или наука: на пути к искусственному интеллекту. — М., 1982.
23. *Поспелов Д. А.* Моделирование рассуждений. — М., 1989.
24. Построение экспертных систем: Пер. с англ. / Ф.Хейес-Рот, Д. Уотерман, Д.Ленат и др. Под ред. Ф.Хейес-Рота. — М., 1987.
25. Приобретение знаний: Пер. с яп. / С.Осуга, Ю.Сазэки, Х.Судзуки и др. Под ред. С.Осуги и Ю.Сазэки. — М., 1990.
26. *Слейгл Дж.* Искусственный интеллект: Пер. с англ. — М., 1973.
27. *Тейз А., Грибомон Т.* Логический подход к искусственному интеллекту: от классической логики к логическому программированию: Пер. с фр. — М., 1990.
28. *Тимофеев А. В.* Информатика и компьютерный интеллект. — М., 1991.
29. *Ульман Дж.* Основы систем баз данных: Пер. с англ. — М., 1983.
30. Экспертные системы. Принципы работы и примеры: Пер. с англ. / А.Брукинг, П.Джонс, Ф.Кокс и др. Под ред. Р.Форсайта. Сб. статей. — М., 1987.
31. *Элти Дж., Кумбс М.* Экспертные системы: концепции и примеры: Пер. с англ. — М., 1987.
32. *Эндрю А.* Искусственный интеллект: Пер. с англ. — М., 1985.

11. Книги, рекомендуемые школьникам

1. *Бизам Д., Герцег Я.* Игра и логика (85 логических задач): Пер. с венг. — М., 1975.
2. *Бизам Д., Герцег Я.* Многоцветная логика (175 задач): Пер. с венг. — М., 1978.
3. *Гжегорчик А.* Популярная логика: Пер. с пол. — М., 1972.
4. *Депман И. Я.* Первое знакомство с математической логикой. — Л., 1965.
5. *Жоль К. К.* Логика в лицах и символах. — М., 1993.
6. *Касаткин В. Н., Верлань А. Ф., Переход И. А.* Элементы кибернетики — школьнику: Сборник упражнений и задач. — Киев, 1974.
7. *Кольман Э., Зих О.* Занимательная логика: Пер. с чеш. — М., 1966.
8. *Кутасов А. Д.* Элементы математической логики. — М., 1977.
9. *Кэррол Л.* История с узелками: Пер. с англ. — М., 1973.
10. *Либер А. Е.* Двоичная булева алгебра и ее приложения. — Саратов, 1966.
11. *Мадер В. В.* Школьнику об алгебре логики. — М., 1993.
12. *Мадер В. В.* Тайны ряда N . — М., 1995.
13. *Хаваш К.* Так — логично!: Пер. с венг. — М., 1985.
14. *Шевченко В. Е.* Некоторые способы решения логических задач. — Киев, 1979.
15. *Яглом И. М.* Необыкновенная алгебра. — М., 1968.

Оглавление

Предисловие	3
Введение. Математическая логика в системе современного образования	6
Логика и интуиция (6). Логика традиционная и математическая логика (7). Немного истории. Математическая логика — логика или математика? Математическая логика в обучении математике. Математическая логика и современные ЭВМ	
Глава I. Алгебра высказываний	15
§ 1. Высказывания и операции над ними	15
Понятие высказывания. Отрицание высказывания. Конъюнкция двух высказываний. Дизъюнкция двух высказываний. Импликация двух высказываний. Эквивалентность двух высказываний. Союзы языка и логические операции (язык и логика). Общий взгляд на логические операции	
§ 2. Формулы алгебры высказываний	23
Конструирование сложных высказываний. Понятие формулы алгебры высказываний. Логическое значение составного высказывания. Составление таблиц истинности для формул. Классификация формул алгебры высказываний. Мышление и математическая логика	
§ 3. Тавтологии алгебры высказываний	33
О значении тавтологий. Основные тавтологии. Основные правила получения тавтологий	
§ 4. Логическая равносильность формул	39
Понятие равносильности формул. Признак равносильности формул. Примеры равносильных формул. Равносильные преобразования формул. Равносильности в логике и тождества в алгебре	
§ 5. Нормальные формы для формул алгебры высказываний	45
Понятие нормальных форм. Совершенные нормальные формы. Представление формул алгебры высказываний совершенными дизъюнктивными нормальными (СДН) формами. Представление формул алгебры высказываний совершенными конъюнктивными нормальными (СКН) формами. Два способа приведения формулы алгебры высказываний к совершенной нормальной форме	
§ 6. Логическое следование формул	53
Понятие логического следствия. Признаки логического следствия. Два свойства логического следования. Следование и равносильность формул. Правила логических умозаключений. Еще один способ проверки логического следования. Нахождение следствий из данных посылок. Нахождение посылок для данного следствия	
§ 7. Приложение алгебры высказываний к логико-математической практике	64
Прямая и обратная теоремы. Необходимые и достаточные условия. Противоположная и обратная противоположной теоремы. Закон контрапозиции. Мо-	

дификация структуры математической теоремы. Методы доказательства математических теорем. Дедуктивные и индуктивные умозаключения. Правильные и неправильные дедуктивные умозаключения. Решение логических задач. Принцип полной дизъюнкции. Одно обобщение принципа полной дизъюнкции

Глава II. Булевы функции 89

§ 8. Множества, отношения, функции 89

Понятие множества. Включение и равенство множеств. Операции над множествами. Бинарные отношения и функции. Понятие n -арного отношения

§ 9. Булевы функции от одного и двух аргументов 93

Происхождение булевых функций. Булевы функции от одного аргумента. Булевы функции от двух аргументов. Свойства дизъюнкции, конъюнкции и отрицания. Свойства эквивалентности, импликации и отрицания. Выражение одних булевых функций через другие

§ 10. Булевы функции от n аргументов 100

Понятие булевой функции. Число булевых функций. Выражение булевых функций через конъюнкцию, дизъюнкцию и отрицание. Булевы функции и формулы алгебры высказываний. Нормальные формы булевых функций

§ 11. Системы булевых функций 106

Полные системы булевых функций. Специальные классы булевых функций. Теорема Поста о полноте системы булевых функций

§ 12. Применение булевых функций к релейно-контактным схемам 111

Идея применения. Две основные задачи теории релейно-контактных схем

§ 13. Релейно-контактные схемы в ЭВМ 115

Двоичный полусумматор. Одноразрядный двоичный сумматор. Шифратор и дешифратор

§ 14. О некоторых других приложениях теории булевых функций 119

Диагностика (распознавание) заболеваний. Распознавание образов

Глава III. Формализованное исчисление высказываний 122

§ 15. Система аксиом и теория формального вывода 122

Начало аксиоматической теории высказываний: первоначальные понятия, система аксиом, правило вывода. Понятие вывода и его свойства. Теорема о дедукции и следствия из неё. Применение теоремы о дедукции. Производные правила вывода

§ 16. Полнота и другие свойства формализованного исчисления высказываний 133

Доказуемость формулы и ее тождественная истинность (синтаксис и семантика). Лемма о выводимости. Полнота формализованного исчисления высказываний. Теорема адекватности. Непротиворечивость формализованного исчисления высказываний. Разрешимость формализованного исчисления высказываний

§ 17. Независимость системы аксиом формализованного исчисления высказываний 141

Понятие независимости. Независимость аксиомы (A1). Независимость аксиомы (A2). Независимость аксиомы (A3). Независимость системы аксиом

§ 18. Основные понятия, связанные с предикатами 146

Понятие предиката. Классификация предикатов. Множество истинности предиката. Равносильность и следование предикатов

§ 19. Логические операции над предикатами 151

Отрицание предиката. Конъюнкция двух предикатов. Дизъюнкция двух предикатов. Свойства отрицания, конъюнкции и дизъюнкции. Импликация и эквивалентность двух предикатов

§ 20. Кванторные операции над предикатами 157

Квантор общности. Квантор существования. Численные кванторы. Ограниченные кванторы. Логический квадрат

§ 21. Формулы логики предикатов 165

Понятие формулы логики предикатов. Классификация формул логики предикатов. Тавтологии логики предикатов

§ 22. Равносильные преобразования формул и логическое следование формул логики предикатов 178

Понятие равносильности формул. Приведенная форма для формул логики предикатов. Предваренная нормальная форма для формул логики предикатов. Логическое следование формул логики предикатов

§ 23. Проблемы разрешения для общезначимости и выполнимости формул 184

Постановка проблемы и ее неразрешимость в общем виде. Решение проблемы для формул на конечных множествах. Пример формулы, выполнимой на бесконечном множестве и невыполнимой ни на каком конечном множестве. Проблема разрешения выполнимости: влияние мощности множества и структуры формулы. Решение проблемы для формул, содержащих только одноместные предикатные переменные. Проблема разрешения общезначимости и мощность множества, на котором рассматривается формула. Решение проблемы для $\forall$ -формул и $\exists$ -формул

§ 24. Применение логики предикатов к логико-математической практике 195

Запись на языке логики предикатов различных предложений. Сравнение логики предикатов и логики высказываний. Строение математических теорем. Методы рассуждений: аристотелева силлогистика. Аристотелева силлогистика и логика предикатов. Теоретико-множественная интерпретация аристотелевой силлогистики. О других методах рассуждений. Принцип полной дизъюнкции в предикатной форме. Метод (полной) математической индукции. Необходимые и достаточные условия. Логика предикатов и алгебра множеств

§ 25. Формализованное исчисление предикатов 222

Первоначальные понятия (язык формализованного исчисления предикатов). Система аксиом исчисления предикатов. Правила вывода (224). Теория формального вывода (224)

§ 26. Аксиоматический метод в математике и аксиоматические теории 226

Понятие аксиоматической теории (226). Как возникают аксиоматические теории (229). Примеры аксиоматических теорий (230). Интерпретации и модели аксиоматической теории (235)

§ 27. Свойства аксиоматических теорий	237

Непротиворечивость (238). Категоричность (240). Независимость системы аксиом (241). Полнота (243)

Глава VI. Формальные аксиоматические теории	247

§ 28. О формальных аксиоматических теориях	248

Об истории идеи формальной аксиоматической теории (249). Понятие формальной аксиоматической теории (251). Язык и метаязык, теоремы и метатеоремы формальной теории (252). Интерпретации и модели формальной теории (253). Семантическая выводимость (255). Метаматематика (свойства формальных аксиоматических теорий) (255). Формализованное исчисление высказываний как формальная аксиоматическая теория (257). Формализация теории аристотелевых силлогизмов (258)

§ 29. Свойства формализованного исчисления предикатов	262

Оправданность аксиоматизации (262). Непротиворечивость формализованного исчисления предикатов (264). Теорема Гёделя о существовании модели (266). Полнота и адекватность формализованного исчисления предикатов (272). Неполнота формализованного исчисления предикатов в абсолютном и узком смыслах (273). Теорема компактности (274)

§ 30. Формальные теории первого порядка	276

Теории первого порядка с равенством (277). О формальных теориях множеств (278). О формальной арифметике (290). О формальных теориях числовых систем (295). О формальной геометрии (302). О формальном математическом анализе (306). Общий взгляд на процесс формализации математической теории (308). О границах аксиоматического метода, метода формализации и логики (310)

Глава VII. Элементы теории алгоритмов	312

§ 31. Интуитивное представление об алгоритмах	312

Алгоритмы вокруг нас (312). Неформальное понятие алгоритма (314). Необходимость уточнения понятия алгоритма (316)

§ 32. Машины Тьюринга	317

Определение машины Тьюринга (317). Применение машин Тьюринга к словам (320). Конструирование машин Тьюринга (322). Вычислимые по Тьюрингу функции (324). Правильная вычислимость функций на машине Тьюринга (327). Композиция машин Тьюринга (329). Тезис Тьюринга (основная гипотеза теории алгоритмов) (330). Машины Тьюринга и современные электронно-вычислительные машины (331)

§ 33. Рекурсивные функции	333

Происхождение рекурсивных функций (333). Основные понятия теории рекурсивных функций и тезис Чёрча (334). Примитивно рекурсивные функции (337). Примитивная рекурсивность предикатов (339). Вычислимость по Тьюрингу примитивно рекурсивных функций (340). Функции Аккермана (342). Оператор минимизации (345). Общерекурсивные и частично рекурсивные функции (347). Вычислимость по Тьюрингу частично рекурсивных функций (347). Частичная рекурсивность функций, вычислимых по Тьюрингу (349)

§ 34. Нормальные алгоритмы Маркова	354

Марковские подстановки (354). Нормальные алгоритмы и их применение к словам (355). Нормально вычислимые функции и принцип нормализации Маркова (356). Совпадение класса всех нормально вычислимых функций с классом всех функций, вычислимых по Тьюрингу (359). Эквивалентность различных теорий алгоритмов (361)

§ 35. Разрешимость и перечислимость множеств	361
§ 36. Неразрешимые алгоритмические проблемы	366
Нумерация алгоритмов (366). Нумерация машин Тьюринга (367). Существование невычислимых по Тьюрингу функций (368). Проблемы распознавания самоприменимости и применимости (369). Алгоритмически неразрешимые проблемы в общей теории алгоритмов (370). Теорема Райса (373). Другие примеры алгоритмической неразрешимости (375)	
§ 37. Теорема Гёделя о неполноте формальной арифметики	376
Формальные аксиоматические теории и натуральные числа (377). Формальная арифметика и ее свойства (379). Теорема Гёделя о неполноте (382). Гёдель и его роль в математической логике XX в. (384)	
Глава VIII. Математическая логика и компьютеры, информатика, искусственный интеллект	385
§ 38. Математическая логика и программное обеспечение компьютеров	386
Теория алгоритмов и математическая логика — фундаментальная основа программирования (386). Описание компьютерных программ с помощью математической логики (387). Описание программирования и анализ его концепций с помощью математической логики (389). Верификация (доказательство правильности) программ с помощью математической логики (393)	
§ 39. Применение компьютеров для доказательства теорем математической логики	397
Программа «Логик-теоретик» и программы, близкие к ней (398). Метод резолюций для доказательства теорем исчисления высказываний и исчисления предикатов (401)	
§ 40. От математической логики к логическому программированию	408
Возникновение языка ПРОЛОГ и его развитие (408). Общая характеристика языка ПРОЛОГ (409). Краткое описание языка ПРОЛОГ и примеры (410). Сферы применения языка ПРОЛОГ (413)	
§ 41. Математическая логика и информатика	414
Общее понятие о базе данных (414). Реляционная база данных и логика запросов в ней (415)	
§ 42. Математическая логика и системы искусственного интеллекта	419
История развития и предмет искусственного интеллекта как науки (420). Представление знаний в системах искусственного интеллекта (422). Экспертные системы (425). Язык ПРОЛОГ в системах искусственного интеллекта (426). Может ли машина мыслить (426).	
Заключение: Всесильна ли логика в познании законов мышления?	428
Список литературы	435

Учебное издание

Игошин Владимир Иванович

Математическая логика и теория алгоритмов

Учебное пособие

2-е издание, стереотипное

Редактор *В. Н. Шакиров*

Технический редактор *Е. Ф. Коржуева*

Компьютерная верстка: *И. М. Чиркин*

Корректоры *Л. С. Рожкова, С. Ю. Свиридова*

Изд. № 102106502. Подписано в печать 03.09.2007. Формат 60×90/16.
Гарнитура «Таймс». Бумага офс. № 1. Печать офсетная. Усл. печ. л. 28,0.
Тираж 1 500 экз. Заказ № 19872.

Издательский центр «Академия». www.academia-moscow.ru

Санитарно-эпидемиологическое заключение № 77.99.02.953.Д.004796.07.04 от 20.07.2004.
117342, Москва, ул. Бутлерова, 17-Б, к. 360. Тел./факс: (495) 334-8337, 330-1092.

Отпечатано в ОАО «Саратовский полиграфкомбинат».
410004, г. Саратов, ул. Чернышевского, 59. www.sarprk.ru