41 к.

Этой книгой издательство „Мир“ продолжает выпуск популярной серии „Современная математика“. В серию включены переводы лучших образцов зарубежной популярной литературы.

Книги серии предназначаются для тех, кто любит математику и хочет заниматься ею самостоятельно. Они будут интересны школьникам старших классов, учителям и студентам, их можно будет использовать в работе школьных математических кружков.

Уже вышло шесть книг этой серии:

О. Оре, Графы и их применение, 1965;

Э. Беккенбах, Р. Беллман, Введение в неравенства, 1965;

А. Нивен, Числа рациональные и иррациональные, 1966;

Р. Неванлинна, Пространство, время и относительность, 1966;

Н. Стинрод, У. Чинн, Первые понятия топологии, 1967;

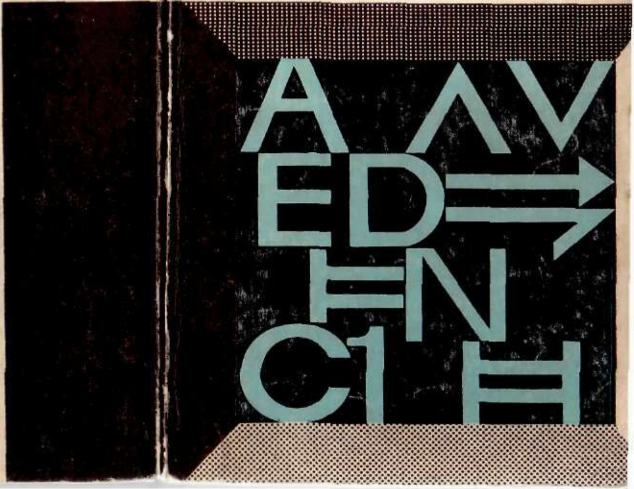
Р. Линдон, Заметки по логике, 1968,

и готовится к изданию седьмая:

Ф. Мостеллер, Р. Рурке, Дж. Томас, Вероятность.

Р. ЛИНДОН

# ЗАМЕТКИ ПО ЛОГИКЕ



ИЗДАТЕЛЬСТВО
«МИР»

VAN NOSTRAND MATHEMATICAL STUDIES

# NOTES ON LOGIC

by

Roger C. Lyndon

*The University of Michigan*

D. VAN NOSTRAND COMPANY, INC.

PRINCETON, NEW JERSEY

Toronto New York London

1966

«СОВРЕМЕННАЯ МАТЕМАТИКА»

*Популярная серия*

Р. ЛИНДОН

# Заметки по логике

*Перевод с английского*
*Ю. А. Гастева*

*Под редакцией*
*И. М. Яглома*

●

ИЗДАТЕЛЬСТВО «МИР»

*Москва 1968*

УДК 510 : 164

В наши дни широкого использования математических методов исследования во многих областях науки и искусства современная логика привлекает все большее внимание исследователей. Однако при этом на первый план зачастую выходит формальный аппарат логики, а не идейная ее сторона. Именно этим идейным аспектам логики, пока незаслуженно остающимся на втором плане, посвящены в основном «Заметки по логике».

Автор избрал внешне свободный стиль изложения и, не углубляясь в технические детали, очень ярко выявил основные идеи логики. Не приводя ни одного сложного и громоздкого доказательства, он тем не менее нигде не ограничился общими описаниями. Очень ценен для начинающего читателя набор задач, которые призваны привить вкус к самостоятельным исследованиям по логике.

Книгу с большим интересом прочтут и те, кто только начинает заниматься математикой (на первом курсе вузов или в старших классах средней школы), и специалисты.

*Редакция литературы по математическим наукам*

Инд. 2-2-3

# От переводчика

Появление в популярной серии «Современная математика» «Заметок по логике» Р. К. Линдона, безусловно, может быть воспринято читателями серии как подарок несколько неожиданный. И не только потому, что книга эта очень уж непохожа на предыдущие выпуски серии,— известно, что все бездарные книги похожи друг на друга, каждая талантливая талантлива по-своему. Дело в том, что «Заметки» при всей своей краткости не только предъявляют известные требования к так называемой общей математической культуре читателя, но предполагают у него наличие некоторых конкретных представлений и даже познаний (правда, совсем скромных) из области теории множеств. При этом книга довольно трудна; каждая из ее трех-пятистраничных главок настолько насыщена идейным и фактическим материалом, что и краткость-то зачастую оказывается иллюзорной. Что и говорить, «Заметки» Линдона не для «трамвайного» чтения. Но кто сказал, что любители математики умеют читать лишь в трамвае, а серьезные занятия — удел одних «специалистов»?

В отличие от подавляющего большинства, в том числе и вполне «популярных», руководств по логике автор «Заметок» основное внимание уделяет не аппарату, а именно идейной стороне вопроса. В наше время логико-математические выкладки — не редкость в книге по лингвистике или, скажем, генетике. Но как часто такая тривиальная «математизация» сводится к наукообразному формальному переоблачению известных истин! Ведь научиться технике элементарных тождественных преобразований алгебры логики не труднее, чем обычным алгебраическим или тригонометрическим преобразованиям. Важнее — и как выясняется, труднее — понять, *что такое логика* (в современном понимании этого слова), извлечь из эффектного многообразия ее впечатляющих результатов целостную картину взаимоотношения между содержательным и формальным аспектами мышления — взаимоотношения, играющего для подлинной математизации любой области знания и для теории познания в целом неизмеримо более важную роль, нежели любые выкладки.

Именно это взаимоотношение между, как говорят логики, семантикой и синтаксисом лежит в центре внимания автора «Заметок». Мастерство, с которым он разъясняет сложные и тонкие концепции, обходясь минимумом техники, но не жертвуя строгостью доказательств в угоду «популярности», весьма поучительно. И хотя «Заметки» представляют собой по существу сокращенный конспект читанного автором систематического курса, они подходят и для самостоятельного ознакомления с новым для читателя материалом, хотя, конечно, особенно полезными и интересными они будут для тех, кто хоть что-нибудь читал или слышал о математической логике (ну хотя бы, скажем, о табличных определениях логических связок). Мерилом усвоения материала может, несомненно, служить *самостоятельное* решение всех (не слишком многочисленных) приводимых автором упражнений.

Как уже говорилось, предполагается, что читатель владеет азбукой теории множеств. Объем этой предполагаемой эрудиции с лихвой перекрывается, например, гл. II и V—VII «Введения в современную математику» Ю. А. Шиха́новича (изд. «Наука», 1965) или еще проще и короче, гл. I книги Р. Р. Столла «Множества. Логика. Аксиоматические теории» (изд. «Просвещение», 1968; начальные параграфы глав этой книги наряду с упоминаемым в списке литературы «Введением в логику» А. Тарского,— пожалуй, самое подходящее предварительное чтение для читателя «Заметок»). Иногда автор позволяет себе привлекать примеры алгебраического содержания; но всякий раз, когда используемые в этих редких примерах понятия





не поясняются тут же в тексте, их можно опустить без существенного ущерба для понимания всего изложения.

В то же время «Заметки» алгебраичны в другом, гораздо более серьезном смысле. Следуя получающей за последние годы все большее распространение традиции (идущей в основном от школ А. Тарского, к которой принадлежит и сам Линдон, и А. И. Мальцева), автор вводит основные логические концепции (в том числе понятия формальной теории и интерпретации) в чисто алгебраических терминах. Поначалу такой алгебраический подход (при котором даже «истина» и «ложь» вводятся как константы в неких абстрактных алгебрах) может показаться читателю суховатым, но зато как ненавязчив автор при «содержательном» истолковании своих конструкций и как естественно и незаметно вживается в это истолкование читатель буквально через десяток страниц. Такая манера изложения может быть условно охарактеризована как классический (базирующийся на содержательной теоретико-множественной основе) аналог конструктивного изложения логики (при котором, как известно, само понятие логического исчисления формулируется в терминах теории алгорифмов). Заметим, впрочем, что трудная проблематика, рассматриваемая на последних страницах «Заметок», изложена на более разговорном уровне, чем остальной материал книги.

Не желая отягощать издание справочным материалом (не случайно в конце концов отсутствующим у автора), мы решили воздержаться при переводе от каких бы то ни было пояснений и дополнений, предоставляя читателю, так сказать, беседовать с автором один на один (работа над переводом дает основание нижеподписавшемуся надеяться, что и для читателя эта беседа будет и полезной, и приятной). Лишь список литературы продолжен некоторыми доступными для русского читателя книгами. Теоретико-множественные термины и символы в соответствии со сказанным не пояснялись. Немногочисленные неточности и опечатки исправлены без специальных оговорок.

В нескольких случаях мы позволили себе удлинить текст за счет пары пояснительных эпитетов, опять-таки не оговаривая это специально. Упоминания (в лингвистических примерах и сравнениях) о русском языке появились, конечно, при переводе. К сожалению, из-за того, что в русском языке слово «импликация» употребляется только как специальный логический термин (в «Заметках», кстати, практически не используемый), нам пришлось отказаться от выразительной игры слов, проводимой Линдоном сквозь весь текст, и перевести авторские semantic implication и syntactical implication совсем непохожими друг на друга терминами «семантическое следование» и «синтаксическая выводимость». Вообще ввиду нереальности проектов всеобщей унификации логической (как и любой другой) терминологии мы даже не пытались согласовать лексикон «Заметок» с другими изданиями по логике и просим читателя все вводимые (курсивом) термины понимать *буквально*, в соответствии с их определениями в тексте (в предметном указателе приведены английские прообразы русских терминов в тех случаях, когда их обратный перевод не вполне однозначен). Обращаем, наконец, внимание читателя на различие в употреблении символов «0» и «1» (в обычном арифметическом смысле) и «**0**» и «**1**» как символов логических констант, а также обычных знаков «0», «1», «2», ..., «$n$», ..., понимаемых содержательно, и их формальных аналогов — «цифр» (арифметических термов) «$\overline{0}$», «$\overline{1}$», «$\overline{2}$», ..., «$\overline{n}$», ..., понимаемых как формальные символы.

*Ю. А. Гастев*

Неверное заключение; мне это отвратительно, как пустая кружка.

*Двенадцатая ночь, II, 3.*

## Предисловие

Эта книга возникла в результате курса лекций для студентов старших курсов и аспирантов, специализирующихся по чистой и прикладной математике, читанного мной в течение 1962/63 г. Я попытался сделать заметки настолько простыми, насколько это допускали требования строгости изложения, построив их в значительной степени в духе идей элементарной абстрактной алгебры. Излагаемый мной материал, как это видно из оглавления, вполне традиционен, так что, кроме исключительных случаев, мне не понадобилось никаких ссылок.

Автор хотел бы специально отметить, сколь многим он обязан многолетнему общению с Альфредом Тарским, и выразить надежду, что некоторые из его идей нашли отражение в этих заметках. Особую благодарность автор выражает Джеймсу Беннету, прочитавшему рукопись.

Анн-Арбор, Мичиган,
1964 г.

*Р. К. Л.*

# Введение

Часто говорят, что логика изучает законы мышления. При этом имеются в виду не столько исторические или психологические закономерности, которым подчиняется процесс мышления, сколько формальные структурные свойства мышления, отражающие, по-видимому, некоторые свойства реальной действительности. Мы не будем вдаваться в обсуждение вопроса о возможности и сущности такой связи между мышлением и действительностью, а прямо приступим к исследованию возможной формальной природы такой связи и ее следствий.

Начнем с примера. Допустим, что из предложения $p$ посредством обычных рассуждений выводится предложение $q$. Если мы знаем, что $p$ на самом деле истинно, то мы заключаем, что $q$ также истинно. Таким образом, не говоря уже о тех практических удобствах, которые дает нам знание отношения «$p$ влечет $q$», открывается возможность использовать это отношение для систематизации и углубления наших знаний и представлений о мире.

В центре нашего внимания будет попытка установить связь фактического, или *семантического, отношения следования*, которое мы будем обозначать через $p \models q$ и которое означает, что из истинности $p$ следует истинность $q$, с чисто формальным *синтаксическим отношением выводимости*, обозначаемым через $p \vdash q$ и заключающимся в том, что $q$ выводимо из $p$ с помощью некоторых четко описанных правил. Если бы нашей основной целью было обучение правилам рассуждений, то мы смогли бы просто сформулировать эти правила и проиллюстрировать затем технику их использования, полагаясь на здравый смысл читателя и предоставляя ему судить о разумности и полезности наших правил. Но наша цель будет в известном смысле противоположной: нас будет главным образом интересовать именно обоснование наших правил и выяснение сферы и границ их применимости; что же касается вопросов техники применения этих правил, то мы попытаемся свести их обсуждение до минимума. Нас интересуют не столько сами по себе дедуктивные правила, сколько взаимосвязь между семантическими и синтаксическими понятиями.

Формальное изучение любого круга вопросов, связанного с нашим повседневным опытом, начинается с замены реальных объектов некоторыми подходящим образом выбираемыми их абстрактными описаниями, идеализациями, выбираемыми таким образом, чтобы в этих идеализациях были отражены именно те свойства исходных объектов, которые мы собираемся изучать. В нашем случае речь пойдет об абстрактных «заместителях» для таких понятий, как мышление, реальная действительность и связь между мышлением и действительностью. Вместо мышления мы будем рассматривать *язык*, точнее говоря, формализованный вариант некоторых аспектов естественного языка. Можно показать, что все чисто формальные аспекты мышления адекватным образом отображаются в таком языке. Вместо реальной действительности мы будем рассматривать так называемую *структуру*, грубо говоря, представляющую собой совокупность предметов, которые могут быть сопоставлены в качестве значений различным выражениям языка. Наконец, роль связи между языком и действительностью будет у нас играть *интерпретация*, т. е. функция, приписывающая некоторым языковым выражениям в качестве их значений некоторые определенные предметы, входящие в данную структуру.

Мы будем по существу пользоваться одним и тем же языком $L$, внося в случае надобности изменения в детали. Все, что мы можем сказать средствами какого-либо одного языка, с достаточными основаниями признаваемого за адекватный, мы, по-видимому, можем выразить и на любом другом таком языке. Однако мы будем рассматривать различные интерпретации языка $L$, связанные с различными структурами $S$. Отчасти это объясняется тем, что мы не знаем, в каком именно из конкретных возможных миров (структур) мы находимся. Еще существеннее то, что нам как логикам, а не естествоиспытателям это попросту безразлично: логика, как принято считать, включает в себя только универсальные принципы, истинные во всех возможных мирах.



## План изложения

Ниже мы дадим точные абстрактные определения следующих понятий: язык $L$, структура $S$ и интерпретация $\varphi$, отображающая $L$ в $S$. Здесь, пожалуй, уместна аналогия с теорией групп, при изучении которой начинают с определения понятий группы и векторного пространства и затем рассматривают представление группы как группы преобразований векторного пространства. Обычная схема изложения теории групп начинается с изучения некоторых элементарных свойств групп, рассматриваемых сами по себе, изолированно от каких-либо иных объектов; затем переходят к изучению представлений групп и в заключение, базируясь на теории представлений, получают дальнейшие сведения о внутренних свойствах групп. Наш план в общих чертах будет таким же. Мы начнем с грамматики (элементарного синтаксиса) языка $L$ и рассмотрим прежде всего такие свойства этого языка, которые связаны с его формальной структурой и не имеют отношения,— если не считать мотивов, по которым выбиралась эта структура, — ни к каким интерпретациям. Затем мы рассмотрим различные интерпретации $L$; отметим заранее, что основной нашей целью на этой стадии будет определение отношения семантического следования $p \models q$, означающего, что $q$ истинно в любой интерпретации, в которой истинно $p$. В заключение мы вернемся к изучению синтаксиса $L$, но уже на более утонченном уровне, в частности к изучению синтаксических отношений $p \vdash q$, с той или иной степенью точности воспроизводящих свойства семантического отношения $p \models q$. Такова наша программа в самых общих чертах; впрочем, мы вовсе не утверждаем, что порядок дальнейшего изложения будет в точности следовать столь схематично намеченному здесь пути.

Мы будем пользоваться словом *теория* в некотором специальном смысле. Теория — это язык $L$ вместе с некоторым множеством $T$ предложений или формул этого языка. На практике теория обычно определяется либо семантически, либо синтаксически. В первом случае $T$ состоит из всех формул языка $L$, истинных в любой интерпретации, входящей в некоторое фиксированное множество интерпретаций. Во втором случае $T$ состоит из всех формул, которые могут быть выведены в соответствии с некоторым фиксированным отношением синтаксического следования из некоторого определенного множества формул, называемых *аксиомами*. В математике теория, связанная первоначально лишь с одной какой-либо структурой, — как, например, теория функций комплексного переменного, — обычно определяется семантически, исходя из этой структуры; теория же, связанная с целым классом структур, — примером может служить теория групп — определяется обычно синтаксически, посредством аксиом. Однако в математике это различие часто смазывается, затушевывается, и фактически эта возможность варьировать и сочетать оба подхода оказывается чрезвычайно удобной.

В большей части последующего изложения мы будем иметь дело с некоторой теорией $T$ в выбранном нами языке $L$ и построим теорию, изучающую эту теорию $T$. В теории, изучающей другие теории, возникает некоторая неопределенность, с которой не приходится сталкиваться в теории групп. Чтобы устранить эту неопределенность, мы будем говорить об изучаемой нами теории как о *предметной теории* $T$, строящейся средствами *предметного языка* $L$; теория же, изучающая предметную теорию, будет именоваться *метатеорией* $T'$, а язык $L'$, средствами которого будет излагаться $T'$, — *метаязыком*. Предметный язык $L$ вообще не будет языком в обычном смысле этого слова; это будет некоторая точно определенная абстрактная конструкция, предназначенная для имитации функций естественно языка; аналогичным образом будет абстрактно определена и теория $T$. Что же касается нашего метаязыка $L'$, то в качестве такового мы будем пользоваться самым обычным математическим жаргоном, представляющим собой смесь русского языка и специальной терминологии и символики. Точно так же дело обстоит с $T'$: здесь мы будем пользоваться постулатами и методами дедукции, обычно применяемыми в математике.





На этом различии предметного языка $L$ и предметной теории $T$, с одной стороны, и метаязыка $L'$ и метатеории $T'$ — с другой, стоит, пожалуй, специально остановиться. Первые мы будем описывать со всей доступной нам абстрактностью и тщательностью. В то же время в метаязыке $L'$ и метатеории $T'$, т. е. в рассуждениях о $L$ и $T$, мы постараемся избежать какой бы то ни было педантичности и вести изложение на содержательном уровне, заботясь лишь о ясности. Мы будем исходить из того, что читатель понимает русский язык и знаком с некоторыми общепринятыми математическими терминами, и будем считать убедительным доказательство какой-либо теоремы логики, если оно проведено с той же степенью строгости, как это принято, скажем, в теории групп.

О соотношении теории и метатеории стоит сказать еще пару слов. Прежде всего, хотя теорию и метатеорию нельзя отождествлять (такое отождествление может привести к недоразумениям, если не вовсе обесценить все рассмотрения), мы должны все же постараться сделать так, чтобы язык $L$ и теорию $T$ можно было соответственно рассматривать как абстракции языков, подобных $L'$, и теорий, подобных $T'$. Это обусловлено естественным желанием сравнить между собой эти языки и теории, причем такое сравнение, как мы увидим ниже, оказывается весьма плодотворным. Правда, против этого можно было бы возразить: изучение свойств некоторого языка $L$ средствами метаязыка $L'$, для которого все соответствующие свойства уже заранее предполагаются известными, есть занятие бесплодное, заводящее в порочный круг. Такого рода возражения, однако, парируются замечанием, что изучение языка средствами языка в математике не более бесполезно, чем в лингвистике, если только в обоих случаях не слишком усложнять вопрос. Когда мы полагаем, что предложение «$p$ и $q$» по определению истинно тогда и только тогда, когда истинно $p$ и истинно $q$, мы, очевидно, вовсе не даем тем самым аналитического определения слова «и». Сказанное относится и к предложенному Тарским специальному определению понятия истинности предложения языка $L$, хотя в этом случае можно утверждать, что такое определение проливает некоторый свет на роль и сущность общего понятия истинности.

Слово *метаматематика* в применении к теории, изучающей математические теории, было введено Гильбертом в связи с его попыткой доказать непротиворечивость некоторой теории $T$ (пользующейся языком $L$), включающей в себя существенную часть классической математики. Идея Гильберта состояла в том, чтобы показать — в результате изучения строения формул теории $T$ самих по себе, — что в $T$ нельзя получить противоречия.

Для того чтобы полученное доказательство такой непротиворечивости $T$ было убедительным, метатеория $T'$ должна обходиться гораздо более скромными средствами. Однако, как следует из одного результата Гёделя, который мы обсудим позднее, такое доказательство непротиворечивости вообще невозможно. Тем не менее во избежание неясностей, с которыми неизбежно связано употребление сильной метатеории, желательно пользоваться метатеорией, по возможности самой слабой из всех пригодных для изучения данной теории. К сожалению, «конструктивная» метатеория, пользующаяся убедительными в общепринятом смысле этого слова средствами, достаточными для изучения большей части синтаксиса языка $L$, оказывается слишком слабой для семантических рассмотрений, требующих свободного использования понятий множества, функции и отношения. Поэтому-то и для упрощения





изложения нам приходится пользоваться в качестве метатеории сильной, но не абсолютно ясно определенной теорией, типа применяемых обычно в математике. Желая поставить дело на точную основу, мы могли бы, следуя предложению Лоренцена, аксиоматизировать нашу метатеорию $T'$ в некоторой — уже конструктивной — метаметатеории $T''$, однако в настоящих заметках мы этого делать не станем.

## Грамматика

Различия между нашим языком $L$ и обычным русским языком, — во всяком случае, в том, что касается их формы, а не содержания, — носят довольно поверхностный характер. Мы будем пользоваться другими символами, и порядок слов в нашем языке будет иным — таким, какой принят в математике; в этом отношении мы отходим от русского или английского языка вряд ли больше, нежели отходит от них, скажем, китайский или немецкий. Более важно то, что правила образования языка $L$ носят абсолютно четкий характер, так что, в частности, грамматический анализ любого выражения этого языка вполне однозначен.

Элементами письменного языка являются «выражения»: буквы, слова, предложения, конечные последовательности предложений. Среди этих выражений имеются выражения, в некотором роде минимальные; это исходные символы или буквы в широком смысле — включая знаки препинания и пробелы между словами. Любое выражение языка можно однозначным образом разложить на буквы; строение же самих букв дальнейшему анализу не подлежит. В английском, русском и других естественных языках имеются более или менее четкие критерии, согласно которым выражения определенного вида признаются грамматически правильными и могут быть классифицированы исходя из разных критериев; они могут подразделяться на различные категории: существительные, глаголы, предложения и т. п. И хотя при построении этой части грамматики обычно руководствуются подразумеваемым смысловым значением выражений языка, в принципе она совершенно от него независима.

Грамматика любого из существующих языков по необходимости носит описательный, аналитический характер — она разлагает выражения на исходные символы как на не поддающиеся дальнейшему разложению компоненты. При построении же нового языка $L$ нам будет удобнее избрать другой путь: мы с самого начала будем исходить из некоторой совокупности символов, а затем уже определим различные категории выражений и свойства выражений в терминах этих исходных символов. Итак, мы будем исходить из некоторого абстрактного множества $S$, элементы которого и будем называть *символами*. Затем мы определяем *выражение* как произвольную конечную последовательность $e=s_1 \ldots s_n$ символов $s_1, \ldots, s_n$ и множество всех выражений будем обозначать через $E$. [Выражение $e$ можно было бы определить как функцию, определенную на множестве целых чисел $i$, где $1 \leqslant i \leqslant n$, со значениями из $S$, так что $e(i)=s_i$.]

Грамматический анализ в значительной степени основан на распознавании какого-либо выражения как произведения или сочленения двух других выражений. Введем в $E$ операцию умножения, определив *произведение* $ef$ двух выражений $e=s_1 \ldots s_m$ и $f=t_1 \ldots t_n$ как $ef=s_1 \ldots s_m t_1 \ldots t_n$. [Если $e$ и $f$ определяются как функции $e(i)=s_i$ и $f(i)=t_i$, то функция $g=ef$ определяется для $1 \leqslant i \leqslant m+n$ следующим образом: $g(i)=e(i)$, если $1 \leqslant i \leqslant n$, и $g(i)=f(i-n)$, если $n+1 \leqslant i \leqslant n+m$.] Очевидно, что наше умножение удовлетворяет *ассоциативному закону*:

$$(ef)g=e(fg) \text{ для всех } e, f \text{ и } g \text{ из } E.$$

Множество $E$, в котором определена операция, подчиняющаяся ассоциативному закону, называется *полугруппой*.

При определении множества $E$ выражений $e=s_1 \ldots \ldots s_n$ мы умышленно не исключали возможности $n=0$; в этом случае говорят о единственном *тривиальном выражении* $e_0$ длины 0. [Единственность $e_0$ особенно очевидна, если считать, что выражению $e_0$ отвечает функция $e$, отображающая в $S$ пустое множество.] Ясно, что тривиальное выражение $e_0$ таково, что

$$ee_0=e_0e=e \text{ для всех } e \text{ из } E.$$

Полугруппу $E$, содержащую элемент $e_0$, такой, что выполняется это последнее правило, называют *полугруппой с единицей*.

Элемент полугруппы называется *простым*, или неразложимым, если он не тривиален и не может быть представлен в виде произведения двух нетривиальных сомножителей; простыми элементами в $E$ являются, очевидно, символы. [Точнее, простыми являются выражения, состоящие из одного символа, а не сами символы, но нам пока незачем принимать во внимание это различие. В дальнейшем мы будем исходить из молчаливого соглашения, что никакой элемент из $S$ не является последовательностью элементов из $S$; например, буква $W$ не принимается за последовательность, состоящую из двух букв $V$.] Очевидно также, что в $E$ выполняется *свойство единственности разложения*: каждое $e$ из $E$ представимо в виде произведения простых множителей $e=s_1 \ldots s_m$, причем если также $e=t_1 \ldots t_n$, где $t_i$ — простые, то $m=n$ и $s_1=t_1, \ldots, s_m=t_m$.

## Упражнения

1. Выясните, существует ли система объектов, которую можно было бы в известном смысле называть языком (скажем, типа азбуки Морзе, языка музыки или живописи), которая (i) не являлась бы полугруппой; (ii) была бы полугруппой, для которой неверно свойство единственности разложения — либо потому, что не каждое выражение разлагается на простые множители, либо потому, что такое разложение не однозначно; (iii) была бы *коммутативной полугруппой*, т. е. полугруппой, для которой справедлив закон $ef=fe$ для всех ее элементов $e$ и $f$.

2. Докажите для полугруппы $E$ следующие теоремы:

(i) из $ef=gh$ следует, что либо для некоторого $k$ имеем $e=gk$ и $h=kf$, либо для некоторого $k$ имеем $g=ek$ и $f=kh$;

(ii) из $ef=fe$ следует, что для некоторого $g$ и для некоторых натуральных чисел $m$ и $n$ имеем $e=g^m$ и $f=g^n$;

(iii) из $e^2f^2=g^2$ следует, что $ef=fe$.

3. Если $E$ и $E'$ — полугруппы, то отображение $\varphi$ из $E$ в $E'$ называется *гомоморфизмом*, если оно сохраняет операцию

умножения, т. е. если $\varphi(ef) = (\varphi e)(\varphi f)$. Полугруппа $E$ называется *свободной*, если она имеет *базис* $S$, т. е. такое подмножество $S$, что любое отображение $S$ в произвольную полугруппу $E'$ может быть единственным образом расширено до гомоморфизма $E$ в $E'$. Докажите, что данное определение эквивалентно тому, что $S$ удовлетворяет свойству единственности разложения на простые множители, роль которых играют элементы базиса.

Теперь мы приступим к классификации выражений по категориям («частям речи»). Начнем мы с символов. Символы языка $L$, с которыми нам в основном придётся иметь дело, мы разобьем на десять категорий. При этом нам совершенно безразлично, что это за символы, — лишь бы эти категории попарно не пересекались; поскольку, однако, нам часто придется говорить об этих символах, мы хотим присвоить различным их категориям какие-либо фиксированные имена. Семь из вводимых категорий содержат каждая по единственному символу; за каждым из этих семи символов мы закрепим постоянное обозначение и некоторое «собственное» русское имя:

символ лжи — $\mathsf{O}$; символ истины — $\mathsf{1}$; символ отрицания — $\mathsf{N}$; символ конъюнкции — $\mathsf{C}$; символ дизъюнкции — $\mathsf{D}$; квантор общности — $\mathsf{A}$; квантор существования — $\mathsf{E}$.

Эти семь символов мы будем называть *связками*. [Заметим, что, например, $\mathsf{O}$ вводится в качестве обозначения некоторого символа лишь потому, что мы хотим иметь возможность говорить об этом символе; при этом для нас совершенно безразлично, какую он имеет форму.]

Остальные три категории мы будем называть следующим образом: $\mathsf{V}$ — класс *переменных*; $\mathsf{F}$ — класс *функциональных символов*; $\mathsf{R}$ — класс *символов отношений*.

Мы будем считать, что каждому функциональному символу $f$ сопоставлено некоторое целое число $n(f) \geqslant 0$, называемое *рангом* $f$, а каждому символу $r$ для отношения — некоторый ранг $n(r) \geqslant 0$. Мы могли бы избрать и другой путь, считая, что $\mathsf{F}$ и $\mathsf{R}$ разбиты на





бесконечное множество подкатегорий: $\mathsf{F}_0$, $\mathsf{F}_1$, ... и $\mathsf{R}_0$, $\mathsf{R}_1$, ... соответственно их рангам.

Забегая вперед, мы укажем хотя бы приблизительно значение, которое мы предполагаем приписать введенным символам. Символ $\mathsf{O}$ можно понимать как обозначение произвольного ложного предложения (например, $2 \neq 2$), символ $\mathsf{1}$ — как обозначение произвольного истинного предложения (скажем, $2=2$). Мы будем читать $\mathsf{N}p$ как «не $p$», $\mathsf{C}pq$ — как «$p$ и $q$»; $\mathsf{D}pq$ — как «$p$ или $q$ (или то и другое)». Если $x$ — переменная, то $\mathsf{A}xp$ означает, что $p$ истинно для всех $x$, а $\mathsf{E}xp$ — что $p$ истинно для некоторого $x$; если, допустим, $p$ есть предложение «$7x > 5y$», то $\mathsf{A}xp$ означает, что $5y$ меньше, чем любое число, умноженное на 7, а $\mathsf{E}xp$ — что $5y < 7x$ для некоторого $x$. Переменные обычно понимаются как индивидные переменные, т. е. как обозначения некоторых индивидов — нерасчленяемых предметов — в отличие от множеств, функций и т. п. Примерами функциональных символов рангов 1 и 2 являются в обычных обозначениях символ $\sqrt{\phantom{x}}$ в выражении $\sqrt{x}$ и символ $+$ в выражении $x+y$. Функциональный символ ранга 0, или индивидная константа, не зависит ни от каких аргументов и обозначает поэтому конкретный предмет; примерами могут служить имеющие один и тот же смысл символы $\pi$ и 3,14159... . Примеры символов отношений рангов 1 и 2: Pos в записи $\mathrm{Pos}(x)$, означающей «$x$ положительно», и $<$ в записи $x < y$. О символах отношений ранга 0 предполагается, что значения их истинности не зависят ни от каких аргументов; они не часто встречаются в обычных рассуждениях, разве что в обозначениях вида: Допущение $C_3$ или Гипотеза $H_7$.

## Термы

Мы будем рассматривать (кроме символов) лишь две основные категории выражений: термы и формулы. Термы будут играть роль существительных и местоимений и интерпретироваться как наименования входящих в какую-либо структуру предметов. Такое истолкование получают прежде всего переменные, которые и причисляются поэтому к термам. Далее мы будем интерпретировать функциональный символ $f$ ранга $n$ как функцию $n$ аргументов, входящих в данную структуру, значения которой также принадлежат этой структуре. Если $t_1, \ldots, t_n$ — термы, являющиеся именами некоторых предметов из структуры, то выражение $ft_1 \ldots t_n$ мы будем понимать как терм, служащий именем значения функции, именуемой $f$, для этих $n$ значений аргументов. О термах не будет предполагаться ничего сверх того, что вытекает из этих условий.

Более точно, мы определяем множество $T$ *термов* как минимальное из всех множеств $U$ выражений языка $L$, такое, что

(1) $\mathsf{V} \subseteq U$,
(2) если $f$ принадлежит $\mathsf{F}_n$, а $t_1, \ldots, t_n$ принадлежат $U$, то $ft_1 \ldots t_n$ принадлежит $U$.

Чтобы показать законность этого определения, мы должны доказать, что среди всех множеств $U$, удовлетворяющих условиям (1) и (2), действительно имеется минимальное множество $T$. Прежде всего, множества, удовлетворяющие (1) и (2), существуют; примером является множество $E$ всех выражений. Заметим далее, что если имеется некоторое семейство $\mathcal{F}$ множеств $U$, удовлетворяющих (1) и (2), а $U_0$ есть общая часть множеств из этого семейства, то $U_0$ также удовлетворяет (1) и (2). Таким образом, если мы возьмем в качестве $\mathcal{F}$ семейство множеств, удовлетворяющих (1) и (2), то $U_0$ будет множеством, удовлетворяющим (1) и (2) и содержащимся в каждом другом множестве, удовлетворяющем этим условиям.

## Упражнения

**1.** Исходя из допущения, что существуют в точности одна переменная $x$ и один функциональный символ $f$ ранга 1, дайте точное описание множеств термов.

**2.** То же, если $n(f)=2$.





**3.** Переменная $x$ добавляет к терму один аргумент; обозначим это обстоятельство через $A(x)=1$. Функциональный символ $f$ ранга $n$ поглощает $n$ аргументов, давая взамен один — в аналогичных обозначениях имеем $A(f)=1-n$. Докажите, что если $e=s_1 \ldots s_m$ — терм, то $A(e)=A(s_1)+\ldots+A(s_m)=1$, и выразите термы $e$ через частичные суммы $A(s_1 \ldots s_i)$, $1 \leqslant i \leqslant m$.

**4.** Используя упражнение 3, докажите, что равенство $e=fg$, где $e$ и $f$ — термы, возможно лишь в том случае, когда $g$ — тривиальное выражение.

**5.** Докажите, что если $ft_1 \ldots t_m=gs_1 \ldots s_n$ (где $f$ и $g$ — функциональные символы, а $t_i$ и $s_j$ — термы) есть терм, то $f=g$, $m=n$ и $t_1=s_1, \ldots, t_m=s_m$.

**6.** Считая, что, взглянув на символ, можно решить, принадлежит ли он $\mathsf{V}$ или $\mathsf{F}_n$ (для некоторого $n$), опишите эффективный метод проверки, позволяющий решить для произвольного данного выражения, является ли оно термом.

По определению, *абстрактная алгебра* состоит из некоторого непустого множества $A$, являющегося ее *областью*, вместе с множеством *операций* $w_i$ рангов $n(w_i)$, перенумерованных посредством элементов некоторого множества $I$. Здесь операция $w$ ранга $n$ — это просто функция $n$ аргументов из $A$ со значениями из $A$. Две алгебры $A$ и $A'$ *подобны*, если множества их операций перенумерованы одним и тем же множеством $I$ и если соответствующие операции имеют один и тот же ранг: $n(w_i)=n(w'_i)$ для всех $i$ из $I$. Отображение $\varphi$ из алгебры $A$ в подобную ей алгебру $A'$ есть *гомоморфизм*, если для каждого $i$ из $I$ и всех элементов $a_1, \ldots, a_{n(w_i)}$ из $A$ имеет место

$$\varphi\left[w_i\left(a_1, \ldots, a_{n(w_i)}\right)\right]=w'_i\left(\varphi a_1, \ldots, \varphi a_{n(w_i)}\right).$$

Алгебра $A$ по определению *свободна* (относительно своего класса подобия) с *базисом* $B$, если $B$ является некоторым подмножеством $A$ и каждое отображение из $B$ в произвольную алгебру $A'$, подобную алгебре $A$, можно единственным образом расширить до гомоморфизма.

Мы делаем множество $T$ термов *алгеброй термов*, перенумерованной множеством $\mathsf{F}$, определяя операции

$w(f)$ следующим образом: для всех $f$ из $\mathbf{F}_n$ и всех $t_1, \ldots, t_n$ из $T$ полагаем

$$w(f)(t_1, \ldots, t_n) = ft_1 \ldots t_n.$$

Можно показать, что $T$ — свободная алгебра с базисом $\mathbf{V}$.

### Упражнение

Докажите последнее утверждение.

Здесь мы пользуемся кратким обозначением $ft_1 \ldots t_n$; однако, кроме специально оговоренных случаев, будем пользоваться и обычным обозначением $f(t_1, \ldots, t_n)$. Заметим, что запятые, скобки и многоточия не только не являются составной частью языка $L$, но даже именами для выражений из $L$; они являются лишь составной частью чисто условной процедуры именования некоторой части $L$.

## Формулы и предложения

Формулы языка $L$ — это выражения, которые мы в дальнейшем будем интерпретировать как некоторые утверждения. Предложения — это формулы, интерпретация которых не зависит от интерпретации входящих в них переменных.

Из множества $F$ формул мы выделим в качестве базиса так называемые *атомарные формулы* — выражения вида $rt_1 \ldots t_n$, где $r$ принадлежит $\mathbf{R}_n$. Затем мы определим множество $F$ формул как минимальное множество $F$, такое, что:

(1) каждая атомарная формула принадлежит $F$;

(2) $\mathbf{O}$ и $\mathbf{1}$ принадлежат $F$; если $p$ и $q$ принадлежат $F$, то $\mathbf{N}p$, $\mathbf{C}pq$ и $\mathbf{D}pq$ принадлежат $F$; если $p$ принадлежат $F$, а $x$ принадлежат $\mathbf{V}$, то $\mathbf{A}xp$ и $\mathbf{E}xp$ принадлежат $F$.





### Упражнения

Аналоги упражнений 1—6 предыдущего раздела.

Множеству $F$ формул может быть придан вид алгебры формул — это делается почти так же, как выше для случая алгебры термов. Наличие кванторов существенно осложняет дело, но даже если исключить кванторы из рассмотрения, мы получим чрезвычайно интересную алгебру, которую ниже и рассмотрим.

Ближайшая наша цель — дать определение понятия предложения. Но для этого нам прежде всего следует уяснить и описать в синтаксических терминах, как зависит интерпретация какой-либо формулы от интерпретации ее переменных. Когда в школьном учебнике видят формулу

$$x^2 - y^2 = (x+y)(x-y),$$

ее обычно понимают как утверждение об истинности некоторого равенства, которое мы могли бы записать как

$$\mathbf{A}x\mathbf{A}y\,[x^2 - y^2 = (x+y)(x-y)];$$

иначе говоря, мы понимаем ее как безусловно истинное высказывание, так же как, скажем, $\mathbf{A}x\mathbf{A}y[x^2 + y^2 = (x+y)^2]$ безусловно ложно. С другой стороны, про формулу типа $x^2+7x+5=0$ нельзя сказать, что она выражает — вне зависимости от контекста — какое-то определенное утверждение: для некоторых $x$ она истинна, для большинства ложна. Эта неопределенность, очевидно, обусловлена вхождением в эту формулу переменной $x$, не снабженной никаким квантором или каким-либо другим указанием, позволяющим судить о том, какие именно значения $x$ следует здесь рассматривать. Грубо говоря, предложение — это формула, каждое вхождение в которую любой переменной $x$ управляется квантором $\mathbf{A}x$ или $\mathbf{E}x$ (или, как говорят, связано этим квантором).

Уточним теперь эту формулировку. Выражение $e$ может входить как *часть* в другое выражение $f=aeb$ более чем один раз; будем называть упорядоченную тройку вида $(a, e, b)$, такую, что $f=aeb$, *вхождением*

$e$ в $f$. Если $f$ в свою очередь входит в какое-нибудь другое выражение $g$, $g=cfd$, то вхождение $(ca, e, bd)$ выражения $e$ в $g$ называют частью данного вхождения.

Сказанное позволяет нам теперь определить вхождение переменной $x$ в выражение $e$ как *связанное* в $e$, если это вхождение есть часть вхождения некоторой формулы $\mathsf{A}xp$ или $\mathsf{E}xp$ в $e$. Вхождение, не являющееся связанным, называют *свободным*. *Предложение* — это по определению формула, не содержащая свободных вхождений ни одной переменной.

Мы уже говорили, что вполне определенные утверждения выражаются не произвольными формулами, а лишь такими, которые мы назвали предложениями. В большинстве случаев мы и будем поэтому ограничиваться рассмотрением предложений, так как формулы, не являющиеся предложениями, нас просто не будут интересовать. Поскольку, однако, сложное предложение может быть построено из компонент, которые сами не являются предложениями, а всего лишь формулами, непосредственное определение понятия предложения без промежуточного понятия формулы представляется малоестественным. Это станет особенно очевидным, когда нам придется доказывать какое-нибудь свойство $P$, относящееся к предложениям: в таких случаях обычно доказывают некоторое более широкое свойство $P'$ применительно ко всем формулам, из чего уже следует выполнимость $P$ для всех предложений.

## Интерпретации и структуры

Когда говорят об интерпретации $\varphi$ языка $L$, то понимают под этим, кратко говоря, сопоставление термам $t$ из $L$ некоторых объектов $\varphi t$, входящих в некоторую область $A$, причем исходные термы можно понимать при этом как наименования сопоставленных при данной интерпретации предметов из $A$. Интерпретация сопоставляет каждому функциональному символу $f$ ранга $n$ некоторую функцию $\varphi f$ ранга $n$, переводящую $n$-ки предметов из $A$ в элементы $A$, а каждому символу отношения $r$ ранга $n$ — некоторое отношение $\varphi r$ ранга $n$, определенное на $A$. Непустую *область* $A$ вместе с определенными на ней функциями $\varphi f$, составляющими в совокупности множество $\mathsf{F}$, и отношениями $\varphi r$, составляющими множество $\mathsf{R}$, мы будем называть *структурой*. Понятие это есть несущественное обобщение определенного выше понятия алебры.

Нашей целью, когда мы вводим понятие интерпретации, является сопоставление каждой формуле $p$ некоторого утверждения относительно структуры $A$, могущего быть либо истинным, либо ложным. Самый простой путь состоит в том, что в качестве $\varphi p$ мы просто выбираем значение — истину или ложь — этого утверждения. Поскольку незачем — да это было бы и затруднительно — разъяснять, что именно мы понимаем под истиной и ложью, мы выберем вместо них два «нейтральных» объекта, которые и будут играть для нас роль истинности и ложности предложений; в этих ролях у нас будут выступать соответственно числа 1 и 0. Будем называть 0 и 1 *истинностными значениями* и обозначать множество, состоящее из этих двух истинностных значений, через $\mathsf{B}=\{0, 1\}$. Тогда для произвольной формулы $p$ мы будем выбирать $\varphi p$ из $\mathsf{B}$. В соответствии с этим нам будет удобно потребовать, чтобы для символа отношения $r$ ранга $n$ в качестве $\varphi r$ выбиралось не множество $n$-ок, а функция ранга $n$ из $A$ в $\mathsf{B}$.

Дадим теперь точное определение. *Интерпретация* $\varphi$ языка $L$ с *областью* $A$ ($A$ непуста) — это прежде всего функция, определенная на $\mathsf{F} \cup \mathsf{R} \cup T \cup F$ и имеющая следующие значения:

(i) если $f$ принадлежит $\mathsf{F}_n$, то $\varphi f$ есть функция из $A^n$ в $A$;

(ii) если $r$ принадлежит $\mathsf{R}_n$, то $\varphi r$ есть функция из $A^n$ в $\mathsf{B}$;

(iii) если $t$ принадлежит $T$, то $\varphi t$ принадлежит $A$;

(iv) если $p$ принадлежит $F$, то $\varphi p$ принадлежит $\mathsf{B}$.

Далее требуется, чтобы интерпретация удовлетворяла следующим условиям:

(1) если $f$ принадлежит $\mathsf{F}_n$, а $t_1, \ldots, t_n$ принадлежат $T$, то
$\varphi(ft_1 \ldots t_n) = (\varphi f)(\varphi t_1, \ldots, \varphi t_n)$;

(2) если $r$ принадлежит $\mathsf{R}_n$, а $t_1, \ldots, t_n$ принадлежат $T$, то
$\varphi(rt_1 \ldots t_n) = (\varphi r)(\varphi t_1, \ldots, \varphi t_n)$;

(3) $\varphi\mathsf{0} = 0$, $\varphi\mathsf{1} = 1$; для любых $p$ и $q$ из $F$
$\varphi(\mathsf{N}p) = 1 - \varphi p$, $\varphi(\mathsf{C}pq) = \mathrm{Min}(\varphi p, \varphi q)$,
$\varphi(\mathsf{D}pq) = \mathrm{Max}(\varphi p, \varphi q)$;

(4) пусть $x$ принадлежит $\mathsf{V}$, $p$ принадлежит $F$, а $I(\varphi, x)$ определяется как множество всех интерпретаций $\varphi'$, совпадающих с $\varphi$ на $\mathsf{F} \cup \mathsf{R} \cup \mathsf{V}$, кроме, быть может, значения аргумента $x$; в таком случае $\varphi(\mathsf{A}xp) = 1$ тогда и только тогда, когда $\varphi' p = 1$ для всех $\varphi'$ из $I(\varphi, x)$, и $\varphi(\mathsf{E}xp) = 1$ тогда и только тогда, когда $\varphi' p = 1$ для некоторой $\varphi'$ из $I(\varphi, x)$.

Для разъяснения пункта (3) заметим, что $\varphi\mathsf{N}p = 1$ равносильно тому, что $\varphi p$ не есть 1; что $\varphi\mathsf{C}pq = 1$ равносильно тому, что $\varphi p = 1$ и $\varphi q = 1$; что наконец, $\varphi\mathsf{D}pq = 1$ равносильно тому, что $\varphi p = 1$ или $\varphi q = 1$. Для пояснения (4) отметим (мы пользуемся весьма неформальными обозначениями), что $\varphi(\mathsf{A}xp(x, y, \ldots)) = 1$ должно означать, что $(\varphi p)(a, \varphi y, \ldots)$ для всех $a$ из $A$, т. е. что если взять $\varphi'$ из $I(\varphi, x)$, такую, что $\varphi' x = a$, то $(\varphi' p)(\varphi' x, \varphi' y, \ldots) = 1$ (короче, $\varphi' p = 1$). Значение $\varphi(\mathsf{E}xp) = 1$ разъясняется аналогично.

Определение, которое мы дали понятию интерпретации, представляется в высшей степени естественным. Но против него можно выдвинуть одно возражение: в пункте (4) нашего определения интерпретации уже используется совокупность интерпретаций. Чтобы избавиться от этого явного порочного круга, мы дадим сейчас несколько другое определение — более аккуратное, но зато и более сложное.





Пусть фиксирована некоторая структура $S$, т. е. фиксированы $A$ и $\varphi_0$, определенная на $\mathsf{F} \cup \mathsf{R}$ в соответствии с условиями (i) и (ii). Пусть $J$ — множество всех расширений $\varphi_0$ до функции $\varphi$, определенной на $\mathsf{F} \cup \mathsf{R} \cup T$ и удовлетворяющей условиям (iii) и (1). Теперь мы определяем функцию, сопоставляющую каждой формуле $p$ из $F$ некоторое подмножество $J(p)$ множества $J$ следующим образом:

(2′) если $rt_1 \ldots t_n$ — атомарная формула, то $\varphi$ принадлежит $J(rt_1 \ldots t_n)$ тогда и только тогда, когда $(\varphi r)(\varphi t_1, \ldots, \varphi t_n) = 1$;

(3′) $J(\mathsf{0}) = \varnothing$ (пустое множество), $J(\mathsf{1}) = J$, $J(\mathsf{N}p) = J - J(p)$ (дополнение), $J(\mathsf{C}pq) = J(p) \cap J(q)$ (пересечение), $J(\mathsf{D}pq) = J(p) \cup J(q)$ (объединение);

(4′) $J(\mathsf{A}xp)$ — множество всех $\varphi$ из $J$, таких, что $J(\varphi, x) \subseteq J(p)$; $J(\mathsf{E}xp)$ — множество всех $\varphi$ из $J$, таких, что $J(\varphi, x) \cap J(p) \neq \varnothing$, где $J(\varphi, x)$ состоит из всех $\varphi'$, совпадающих с $\varphi$ всюду, кроме, быть может, значения аргумента $x$.

Теперь мы расширяем каждую $\varphi$ из $J$ до функции, определенной как на $F$, так и на $\mathsf{F} \cup \mathsf{R} \cup T$, полагая $\varphi p = 1$ тогда и только тогда, когда $\varphi$ принадлежит $J(p)$. Легко видеть, что функции $\varphi$ из $J$, расширенные таким образом, совпадают с интерпретациями — в смысле условий (i)—(iv) и (1)—(4) — со структурой $S$.

## Упражнения

1. Если рассматривать структуру $S$ как алгебру с областью $A$ и операциями $\varphi f$, перенумерованными множеством $\mathsf{F}$, то условия (i), (iii) и (1) означают, что $\varphi$ осуществляет гомоморфизм алгебры $T$ термов в $S$. Исходя из того, что $T$ есть свободная алгебра, докажите, что произвольную функцию $\varphi_0$, определенную на $\mathsf{V} \cup \mathsf{F}$, такую, что $\varphi_0 \mathsf{V} \subseteq A$, и удовлетворяющую условию (i), можно однозначно расширить до функции $\varphi$, определенной на $T \cup \mathsf{F}$ и удовлетворяющей (i), (iii) и (1).

2. Докажите, что, аналогично, произвольная функция $\varphi_0$, определенная на множестве атомарных формул и принимающая значения в $\mathsf{B}$, допускает единственное расширение до функции

$\varphi$, определенной на множестве всех бескванторных формул и удовлетворяющей условию (3).

3. Докажите, что произвольная функция $\varphi_0$, определенная на $\mathsf{V} \cup \mathsf{F} \cup \mathsf{R}$ и принимающая значения в соответствии с условиями (i), (ii) и (iii), однозначно расширяема до интерпретации.

Принимая во внимание утверждение, высказанное в упражнении 3, часто интерпретацией называют просто функцию $\varphi$, определенную на $\mathsf{V} \cup \mathsf{F} \cup \mathsf{R}$, подразумевая при этом тривиальное расширение на $T \cup F$. Структура данной интерпретации может тогда быть отождествлена с ограничением $\varphi$ на $\mathsf{F} \cup \mathsf{R}$.

## Зависимость и подстановка

Представляется довольно очевидным, что значение $\varphi t$ терма $t$ при интерпретации $\varphi$ зависит только от значений $\varphi s$, которые $\varphi$ приписывает символам $s$, входящим в $t$. Сформулируем, однако, строго это предложение и докажем его.

Теорема. *Пусть $t$ — терм, а $\varphi$ и $\varphi'$ — две интерпретации, совпадающие для каждого входящего в $t$ символа. Тогда $\varphi t = \varphi' t$.*

Для доказательства этого утверждения рассмотрим множество $U$ всех термов, для которых утверждение справедливо; поскольку $U \subseteq T$, остается показать, что $T \subseteq U$. Обратившись к определению множества $T$ термов, заметим прежде всего, что $\mathsf{V} \subseteq U$, так что остается лишь показать, что если $f$ принадлежит $\mathsf{F}_n$, а $t_1, \ldots, t_n$ принадлежат $U$, то и $t = ft_1 \ldots t_n$ принадлежит $U$. Если $\varphi$ и $\varphi'$ совпадают для любых входящих в $t$ символов, то, конечно, $\varphi f = \varphi' f$ и, кроме того, $\varphi$ и $\varphi'$ совпадают для всех символов, входящих в $t_1, \ldots, t_n$. Поскольку $t_1, \ldots, t_n$ принадлежат $U$, то $\varphi t_1 = \varphi' t_1, \ldots, \varphi t_n = \varphi' t_n$. Из пункта (2) определения интерпретации получаем, что

$$\varphi(ft_1 \ldots t_n) = (\varphi f)(\varphi t_1, \ldots, \varphi t_n)$$

и

$$\varphi'(ft_1 \ldots t_n) = (\varphi' f)(\varphi' t_1, \ldots, \varphi' t_n),$$





откуда

$$\varphi t = \varphi' t.$$

Аналогичный результат, относящийся к формулам, выглядит следующим образом:

Теорема. *Пусть $p$ — формула, а $\varphi$ и $\varphi'$ — две интерпретации, совпадающие для каждого входящего в $p$ символа, за исключением, быть может, переменных, не входящих в $p$ свободно. Тогда $\varphi p = \varphi' p$.*

Для доказательства рассмотрим множество $U$ формул, для которых утверждение теоремы справедливо. Доказательство того, что $\mathsf{0}$, $\mathsf{1}$, $\mathsf{N}p$, $\mathsf{C}pq$ и $\mathsf{D}pq$ принадлежат $U$, если $p$ и $q$ принадлежат $U$, не представляет собой ничего нового. Остается доказать, что если $p$ принадлежит $U$, то $\mathsf{A}xp$ и $\mathsf{E}xp$ также принадлежат $U$; рассмотрим случай $\mathsf{E}xp$ (для $\mathsf{A}xp$ доказательство проводится в точности так же). Ввиду симметричности утверждения относительно $\varphi$ и $\varphi'$ достаточно доказать, например, что $\varphi\mathsf{E}xp = 1$ влечет $\varphi'\mathsf{E}xp = 1$. Далее, $\varphi\mathsf{E}xp = 1$ влечет $\psi p = 1$, где $\psi$ — интерпретация, отличающаяся от $\varphi$ (на множестве $\mathsf{V} \cup \mathsf{F} \cup \mathsf{R}$) разве что для значения аргумента $x$. Построим $\psi'$, отличающуюся от $\varphi'$, быть может, лишь для значения аргумента $x$, положив $\psi' x = \psi x$, что возможно в силу упражнений из предыдущего раздела. Тогда $\psi$ и $\psi'$ будут совпадать для всех $f$ из $\mathsf{F}$ и $r$ из $\mathsf{R}$, входящих в $p$, и для всех $v$ из $\mathsf{V}$, свободно входящих в $\mathsf{E}xp$, а также для $x$. Таким образом, $\psi$ и $\psi'$ удовлетворяют утверждению теоремы по отношению к $p$ и $\psi p = \psi' p$. Следовательно, $\psi' p = 1$ и $\varphi'\mathsf{E}xp = 1$.

Следующее видоизменение первой из теорем настоящего раздела (доказательство здесь несложно и предоставляется читателю в качестве упражнения) демонстрирует понятие подстановки в его простейшей форме:

Теорема. *Пусть $t$ и $u$ — термы, $x$ — переменная, $t'$ — терм, получающийся в результате замены $x$ на $u$ в каждом вхождении $x$ в $t$. Если $\varphi$ и $\varphi'$ — две интерпретации, совпадающие для всех входящих в $t$ символов, кроме, быть может, $x$, такие, что $\varphi x = \varphi' u$, то $\varphi t = \varphi' t'$.*

В описанной ситуации мы будем писать $t = t(x)$ и $t' = t(u)$; смысл этих записей очевиден.

Для формул дело обстоит несколько сложнее; если, например, $f(x) = \int_1^x xy\,dy$, то формула $f(y) = \int_1^y y^2\,dy$, полученная заменой $x$ (во всех его свободных вхождениях) на $y$, не определяет ту же самую функцию. Нас будут интересовать поэтому лишь такие случаи, когда в формуле $p'$, получающейся в результате подстановки $u$ в формулу $p$ вместо всех свободных вхождений $x$, не возникает при подстановке связанных вхождений переменной $u$. В таких случаях мы будем писать $p = p(x)$ и $p' = p(u)$ и при использовании этого обозначения всегда неявно будем исходить из допущения, что сформулированное здесь условие выполнено. [Таким образом, подстановка $u$ в $p$ — в описываемом здесь ограниченном смысле — может быть произведена не во всех случаях.]

Теорема. *Если $\varphi$ и $\varphi'$ — две интерпретации, совпадающие для всех символов из* $\mathsf{F} \cup \mathsf{R}$, *входящих в $p(x)$, и всех переменных, входящих свободно в $p(x)$, кроме, быть может, $x$, причем $\varphi x = \varphi' u$, то $\varphi p(x) = \varphi' p(u)$.*

Для доказательства рассмотрим случай, когда $p(x)$ имеет вид $\mathsf{E}yq$. Если $x = y$, то $x$ не входит свободно в $p(x)$, так что $p(x) = p(u)$ и требуемое заключение следует из предыдущей теоремы. Допустив, что $x \neq y$, мы получим $p(x) = \mathsf{E}yq(x)$ и $p(u) = \mathsf{E}yq(u)$ при условии, что $y$ не входит в $u$. Пусть $\psi$ и $\psi'$ — две такие интерпретации, что $\psi$ совпадает с $\varphi$, кроме, быть может, значения аргумента $y$, а $\psi'$ совпадает с $\varphi'$, также кроме, быть может, значения $y$, причем $\psi y = \psi' y$. Так как $y$ не входит в $u$, то $\psi' u = \varphi' u$ и, следовательно, $\psi x = \varphi x = \varphi' u = \psi' u$. По предположению индукции имеем $\psi q(x) = \psi' q(u)$, из чего вытекает, что существование такой $\psi$, что $\psi q(x) = 1$, равносильно существованию такой $\psi'$, что $\psi' q(u) = 1$, так что условия $\varphi \mathsf{E}yq(x) = 1$ и $\varphi' \mathsf{E}yq(u) = 1$ оказываются эквивалентными.





Отметим важное следствие последней теоремы.

Следствие. *Если $p$ — некоторое предложение, то $\varphi p$ имеет одно и то же значение для всех интерпретаций $\varphi$, имеющих одну и ту же структуру; иными словами, $\varphi p$ определяет лишь значения $\varphi$ для элементов* $\mathsf{F} \cup \mathsf{R}$, *но не для элементов* $\mathsf{V}$.

## Семантическое следование

Определим отношение *семантического следования* $p \models q$ между двумя формулами $p$ и $q$ языка $L$, имеющее место тогда и только тогда, когда для любой интерпретации $\varphi$ из $\varphi p = 1$ следует $\varphi q = 1$. Аналогично для множеств формул $P$ и $Q$ отношение $P \models Q$ означает по определению, что $\varphi P = 1$ влечет $\varphi Q = 1$ для всех $\varphi$.

Если $p \models q$ и $q \models p$, мы пишем $p \mathrel{=\!|\!=} q$ и называем $p$ и $q$ *семантически эквивалентными.*

Если $\varnothing \models q$, т. е. если $\varphi q = 1$ для любой интерпретации $\varphi$, то мы будем писать просто $\models q$ и говорить, что $q$ *общезначима*, или (тождественно) *истинна.*

Если $P \models \mathsf{O}$, т. е. если ни для какой интерпретации не имеет места $\varphi P = 1$, мы будем говорить, что множество $\varphi$ формул $P$ *семантически противоречиво*; в противном же случае $P$ *семантически непротиворечиво.* Если $\varphi P = 1$, то интерпретацию $\varphi$ (а иногда и соответствующую ей структуру) называют обычно *моделью* (для) $P$. Таким образом, множество $P$ формул по определению непротиворечиво, если для него существует модель.

Введем теперь в качестве сокращения для записи выражения $\mathsf{DN}$ обозначение $\mathsf{J}$; иначе говоря, $\mathsf{J}pq = \mathsf{DN}pq$ для любых формул $p$ и $q$. Вместо записи $\mathsf{J}pq$ мы будем также пользоваться более обычным обозначением $p \supset q$. Заметим, что $\varphi \mathsf{J}pq = 1$ всегда, за исключением того случая, когда $\varphi p = 1$ и в то же время $\varphi q = 0$. Таким образом, синтаксическая операция $\mathsf{J}$ над парами формул выражает отношение семантического следования в следующем смысле:

Теорема. *Для произвольных формул $p$ и $q$ утверждения $\models p \supset q$ и $p \models q$ равносильны.*

Важно подчеркнуть, что символ $\models$ обозначает некоторое отношение между формулами (подобно тому как знак $\geqslant$ в записи «$x \geqslant y$» выражает отношение между числами), в то время как символ $\mathsf{J}$ обозначает операцию над формулами, результатом которой в свою очередь является формула (подобно, например, операции получения разности двух чисел $x-y$). Таким образом, сформулированная здесь теорема выражает факт, аналогичный тому, что $x \geqslant y$ равносильно $x-y \geqslant 0$. Важно, в частности, уяснить, что утверждение $p \supset q$ часто играет роль краткого сообщения о синтаксически определенном эквиваленте семантического отношения $p \models q$.

Когда мы рассматриваем какую-нибудь теорию $T$, определяемую семантически посредством указания некоторого класса $I_0$ интерпретаций, мы, строго говоря, для указания того факта, что $\varphi P=1$ влечет $\varphi Q=1$ для всех интерпретаций $\varphi$ из $I_0$, будем писать $P \models_{I_0} Q$ и вообще снабжать индексом $I_0$ обозначения всех зависящих от этого класса $I_0$ понятий. На практике мы, однако, будем обычно опускать такие индексы.

## Пропозициональная логика

Теперь мы, наконец, имеем в своем распоряжении все понятия, которые могут понадобиться при дальнейшем изложении. Вначале, однако, рассмотрим несколько более простую ситуацию, возникающую в результате удаления из языка $L$ символов $\mathsf{A}$ и $\mathsf{E}$. При этом наш язык упрощается также за счет удаления из него переменных, функциональных символов и всех символов отношений рангов, больших 0. Получающийся язык $L$ называется *пропозициональным языком*. Изучение таких языков представляет немалый самостоятельный интерес и позволяет в то же время на сравнительно простом материале подойти к изучению языков более общего типа; впрочем, следовало бы предупредить читателя заранее, что результаты, относящиеся к пропозициональным языкам, не только значительно проще, но зачастую имеют характер, совершенно противоположный соответствующим результатам, относящимся к более сложным языкам.





В применении к случаю, когда $L$ — пропозициональный язык, мы слегка модифицируем наши определения. *Символами* языка $L$ являются пять *связок* $\mathsf{0}$, $\mathsf{1}$, $\mathsf{N}$, $\mathsf{C}$ и $\mathsf{D}$, а также множество $\mathsf{R}_0$ *символов отношений* ранга 0. Никаких термов здесь нет. *Атомарные формулы* — это элементы $\mathsf{R}_0$. Множество $F$ *формул* определяется как наименьшее множество, такое, что $\mathsf{R}_0 \subseteq F$, что $\mathsf{0}$ и $\mathsf{1}$ принадлежат $F$ и что если $p$ и $q$ принадлежат $F$, то $\mathsf{N}p$, $\mathsf{C}pq$ и $\mathsf{D}pq$ также принадлежат $F$. *Предложение* в данном случае — в точности то же самое, что формула.

Поскольку у нас сейчас нет никаких термов, ни к чему оказывается и область интерпретации: понятия *интерпретации* и *структуры* теперь попросту совпадают; в данном случае эти понятия сводятся к понятию функции $\varphi$, отображающей $\mathsf{R}_0$ в $\mathbf{B}$ и удовлетворяющей следующим условиям:

$$\varphi\mathsf{0}=0, \quad \varphi\mathsf{1}=1, \quad \varphi\mathsf{N}p=1-\varphi p,$$
$$\varphi\mathsf{C}pq=\mathrm{Min}(\varphi p, \varphi q), \quad \varphi\mathsf{D}pq=\mathrm{Max}(\varphi p, \varphi q).$$

Определения семантического следования и общезначимости прежние.

Проблема чисто синтаксической характеризации отношения семантического следования $p \models q$ для пропозициональных языков оказывается легко решаемой. Прежде всего из того обстоятельства, что $p \models q$ равносильно $\models \mathsf{J}pq$, вытекает, что нам нужно научиться характеризовать общезначимость формул. Пусть $p$ — произвольно выбранная формула, а $r_1, \ldots, r_n$ — конечное множество входящих в $p$ символов отношений. Поскольку значение $\varphi p$ зависит лишь от $n$ значений $\varphi r_1, \ldots, \varphi r_n$, то $p$ будет общезначимой тогда и только тогда, когда $\varphi_i p=1$ для каждой из $2^n$ интерпретаций $\varphi_i$, приписывающих символам $r_1, \ldots, r_n$ значения $\mathsf{0}$ и $\mathsf{1}$ во всех возможных комбинациях. Пусть $\varphi_i^* p$ — формула, получаемая из $p$ заменой каждого $r_j$ на $\mathsf{0}$, если $\varphi_i r_j=0$, и на $\mathsf{1}$, если $\varphi_i r_j=1$, где $\varphi_i$ — любая из упомянутых интерпретаций. Легко показать, что $\varphi_i$

сопоставляет формулам $p$ и $\varphi_i^* p$ одно и то же значение. Таким образом, наша проблема сводится к выяснению вопроса, сопоставляет ли $\varphi_i$ значение 1 формуле $\varphi_i^* p$. Но так как $\varphi_i^* p$ не содержит символов отношений, нам нужно лишь научиться решать вопрос об общезначимости формул $q$, не содержащих символов отношений. Этот же вопрос в свою очередь может быть сведен к аналогичному вопросу для эквивалентной $q$ и более короткой, чем она, формулы $q'$, получаемой из $q$ путем подстановки одного из следующих видов:

1 вместо $\mathrm{N0}$; 0 вместо $\mathrm{N1}$;

0 вместо $\mathrm{C00}$, $\mathrm{C01}$ и $\mathrm{C10}$; 1 вместо $\mathrm{C11}$;

0 вместо $\mathrm{D00}$; 1 вместо $\mathrm{D01}$, $\mathrm{D10}$ и $\mathrm{D11}$,

причем подстановки эти производятся до тех пор, пока не выясняется, что $q$ эквивалентна либо **0**, либо **1**. Очевидно, что $q$ общезначима тогда и только тогда, когда конечный результат таких последовательных подстановок эквивалентен **1**.

Из приведенного рассуждения легко извлечь описание процесса, проводимого исключительно в терминах синтаксиса языка $L$, без какого бы то ни было обращения к понятиям общезначимости или эквивалентности, который приводил бы к решению вопроса о том, является ли данная формула $p$ общезначимой. Таким образом, — при любом разумном понимании слова «разрешимый» — мы доказали следующую теорему:

Теорема. *Какова бы ни была формула пропозиционального языка, вопрос о том, общезначима ли она, разрешим.*

## Алгебра высказываний

Теперь мы превратим множество $F$ формул в некоторую алгебру — *алгебру формул*, имеющую две операции ранга 0, т. е. константы, одну операцию ранга 1 и две операции ранга 2. Эти операции, обозначаемые 0, 1, $\neg$, $\wedge$ и $\vee$, определяются следующим образом:

$$\mathbf{0}=0,\quad \mathbf{1}=1,\quad \neg p=\mathrm{N}p,\quad p\wedge q=\mathrm{C}pq,\quad p\vee q=\mathrm{D}pq.$$

Множество **B** истинностных значений мы также превратим в алгебру — *алгебру истинностных значений*. Операции в этой алгебре будут обозначаться так же, как в алгебре формул. 0 и 1 получат те же определения, остальные же операции определяются так:

$$\neg x=1-x,\quad x\wedge y=\mathrm{Min}(x,\ y),\quad x\vee y=\mathrm{Max}(x,\ y).$$

Теперь интерпретация $\varphi$ оказывается просто гомоморфизмом, отображающим $F$ в **B**. Сказанное позволяет нам применить к изучению языка $L$ обычные алгебраические методы.

Если $\varphi$ есть некоторое отображение множества $A$ в множество $A'$, мы будем говорить, что на $A$ определено бинарное отношение $x\equiv y$ *равнообразности* отображения $\varphi$, причем $x\equiv y$ для тех и только тех пар $x$ и $y$, для которых $\varphi x=\varphi y$. Бинарное отношение есть по определению (абстрактное) *отношение эквивалентности*, если оно:

*рефлексивно:* $x\equiv x$ для всех $x$;
*симметрично:* $x\equiv y$ влечет $y\equiv x$ для всех $x$ и $y$;
*транзитивно:* $x\equiv y$ и $y\equiv z$ влечет $x\equiv z$ для всех $x$, $y$ и $z$.

Равнообразность любого отображения множества $A$ в $A'$ является отношением эквивалентности. Если на некотором множестве $A$ задано отношение эквивалентности $x\equiv y$, мы определим *класс, порожденный* элементом $x$ из $A$, как множество всех таких $y$, что $x\equiv y$; класс, порожденный элементом $x$, мы будем обозначать через $[x]$, а совокупность всех таких классов для данного множества $A$ — через $[A]$. Совокупность $P$ непустых подмножеств множества $A$ есть по определению *разбиение*, если каждый элемент множества $A$ входит в точности в один член этой совокупности $P$. Если $x\equiv y$ есть отношение эквивалентности на множестве $A$, то $[A]$ есть разбиение $A$.

Если задано некоторое разбиение $P$ множества $A$, то *каноническое отображение* $\varkappa$ множества $A$ на $P$ сопоставляет каждому $x$ из $A$ единственный элемент $\varkappa(x)$ из $P$, содержащий $x$; в этом случае $P$ является разбиением, индуцируемым отношением равнообразности отображения $\varkappa$. Если задано некоторое отображение $\varphi$ множества $A$ в $A'$, а $[A]$ есть разбиение, индуцируемое отношением равнообразности отображения $\varphi$, то существует единственная взаимно-однозначная функция $\varphi'$, отображающая $[A]$ в $A'$, такая, что для всех $x$ $\varphi x = \varphi'[x]$.

Если на $A$ задано семейство отношений эквивалентности $x \equiv_i y$, где $i$ пробегает некоторое множество индексов $I$, то *пересечение* всех этих отношений, обозначаемое просто $x \equiv y$ и равносильное по определению тому, что $x \equiv_i y$ для всех $i$ из $I$, также является отношением эквивалентности.

Если $A$ и $A'$ — алгебры, а $\varphi$ — гомоморфизм алгебры $A$ в $A'$, то отношение равнообразности гомоморфизма $\varphi$ есть *конгруэнция* (или *отношение конгруэнтности*), т. е. эквивалентность, обладающая так называемым свойством подставимости во все определенные на $A$ операции: если $w$ — операция ранга $n$, то для всех $x_1, \ldots, x_n$ и $y_1, \ldots, y_n$ из $A$

$$x_1 \equiv y_1 \text{ и } \ldots \text{ и } x_n \equiv y_n \text{ влечет}$$
$$w(x_1, \ldots, x_n) \equiv w(y_1, \ldots, y_n).$$

Если $[A]$ — разбиение множества $A$, индуцируемое некоторой конгруэнцией, то мы можем превратить $[A]$ в алгебру, так называемую *факторалгебру* множества $A$ по отношению $\equiv$, определяя операции $w$ на $[A]$, исходя из операций, определенных на $A$, посредством следующих условий:

$$w([x_1], \ldots, [x_n]) = [w(x_1, \ldots, x_n)]$$
$$\text{для всех } x_1, \ldots, x_n \text{ из } A.$$

Сказанное позволяет перенести на конгруэнции все результаты, полученные ранее для отношений эквивалентности.





Обращаясь, в частности, к алгебре формул, мы видим, что отношение $p \mathrel{|{=}|} q$ на $F$ есть пересечение всех конгруэнций $\varphi p = \varphi q$, связанных с интерпретациями $\varphi$, и потому само является конгруэнцией. Факторалгебру $[F]$ алгебры $F$ по отношению $p \mathrel{|{=}|} q$ называют *алгеброй Линденбаума* языка $L$.

Когда имеется некоторая семантика, различение синонимичных формул, имеющих одинаковые значения при всех интерпретациях, оказывается излишним. Если объединить вместе с $p$ все формулы, семантически эквивалентные $p$, мы получаем элемент $[p]$ алгебры Линденбаума. По ряду соображений $[p]$ естественно рассматривать как общее значение всех этих различных, но синонимичных формул и называть $[p]$ *высказыванием*, а алгебру Линденбаума $[F]$ — *алгеброй высказываний.* В качестве примера заметим, что при $p \neq q$ две формулы $p \wedge q$ и $q \wedge p$ различны, хотя и имеют одно и тоже значение: $p \wedge q \mathrel{|{=}|} q \wedge p$. Следовательно, $[p] \wedge [q]$ и $[q] \wedge [p]$ — это один и тот же элемент факторалгебры $[F]$ и в алгебре высказываний мы имеем закон: $x \wedge y = y \wedge x$ для всех $x$ и $y$ из $[F]$.

## Дизъюнктивная форма

Алгебра высказываний $[F]$ проявляет определенное сходство с обычной алгеброй; в нашем случае операция $\wedge$ играет роль умножения, а операция $\vee$ — роль сложения. Так, закон $x \wedge y = y \wedge x$ есть аналог закона $xy = yx$ обычной алгебры. В обычной алгебре значение произведения не зависит от порядка сомножителей или расстановки скобок, так что произведение $n$ сомножителей $x_1, \ldots, x_n$ мы обозначаем просто через $\prod\limits_{1}^{n} x_i$. В алгебре высказываний элемент $p$, построенный посредством одной лишь операции $\wedge$ из элементов $x_1, \ldots, x_n$, не зависит не только от их порядка или группировки, но и от количества вхождений каждого $x_i$ — лишь бы было хоть одно вхождение. Для обозначения конъюнкции $x_1, \ldots, x_n$ мы пишем, как в обычной алгебре, $p = \bigwedge_1^n x_i$, причем если $n=0$, то мы полагаем $p=1$. Точно так же по аналогии с обычным алгебраическим обозначением $p = \sum_1^n x_i$ мы будем обозначать дизъюнкцию элементов $x_1 \ldots, x_n$, т. е. любой элемент $p$, образованный исходя из элементов $x_i$ посредством одной лишь операции $\vee$ и такой, что каждый член $x_i$ входит в него хотя бы один раз, через $p = \bigvee_1^n x_i$. При $n=0$ мы положим по определению $p = \bigvee_1^n x_i = 0$.

В обычной алгебре имеется понятие многочлена; это, если не обращать внимания на коэффициенты, сумма произведений. В нашей алгебре мы определим *многочлен* от $x_1, \ldots, x_n$ как дизъюнкцию конъюнкций членов $x_i$ и их отрицаний $\rightarrow x_i$, т. е. как элемент вида $p = \bigvee_i \bigwedge_j s_{ij}$, где каждое $s_{ij}$ есть некоторое $x_k$ или $\rightarrow x_k$. Покажем, что каждый элемент алгебры $[F]$ можно представить в виде некоторого многочлена от $x_1, \ldots, x_n$ и что, если принять некоторые подходящие ограничения, такое представление единственно.

Выше мы говорили не только об элементах алгебры $[F]$, но и о представлениях для этих элементов, не уточняя, впрочем, пока этого термина. Чтобы разъяснить его, естественнее и удобнее всего обратиться к алгебре $F$, элементы которой как раз и являются представлениями для элементов алгебры $[F]$. Дадим теперь точное определение и докажем высказанные выше утверждения, пользуясь введенными терминами.

Формула $p$ алгебры $F$ записана в *дизъюнктивной форме*, если:

(1) никакая подформула формулы $p$, начинающаяся с символа $\mathsf{N}$, не содержит другого вхождения этого символа, а также вхождений символов $\mathsf{0}$, $\mathsf{1}$, $\mathsf{C}$ и $\mathsf{D}$;





(2) никакая подформула формулы $p$, начинающаяся с символа $\mathsf{C}$, не содержит символов $\mathsf{0}$, $\mathsf{1}$ и $\mathsf{D}$;

(3) никакая подформула формулы $p$, начинающаяся с символа $\mathsf{D}$, не содержит символов $\mathsf{0}$ и $\mathsf{1}$.

Теорема. *Каждая формула эквивалентна некоторой формуле, записанной в дизъюнктивной форме.*

Покажем вначале, что любая формула $p$ эквивалентна $\mathsf{0}$ или $\mathsf{1}$ или же формуле, не содержащей ни $\mathsf{0}$, ни $\mathsf{1}$. Если $p$ содержит $\mathsf{0}$ или $\mathsf{1}$, то, используя правила

$$\mathsf{N0} \mathrel{|=|} \mathsf{1}, \quad \mathsf{C0}x \mathrel{|=|} \mathsf{C}x\mathsf{0} \mathrel{|=|} \mathsf{0}, \quad \mathsf{D0}x \mathrel{|=|} \mathsf{D}x\mathsf{0} \mathrel{|=|} x,$$
$$\mathsf{N1} \mathrel{|=|} \mathsf{0}, \quad \mathsf{C1}x \mathrel{|=|} \mathsf{C}x\mathsf{1} \mathrel{|=|} x, \quad \mathsf{D1}x \mathrel{|=|} \mathsf{D}x\mathsf{1} \mathrel{|=|} \mathsf{1}$$

и возможность эквивалентной замены $x$ на $y$ при условии $x \mathrel{|=|} y$, мы можем заменить $p$ более короткой эквивалентной формулой. Продолжая и далее таким же образом, мы в конце концов придем к некоторой формуле $p'$, эквивалентной $p$, которая либо есть $\mathsf{0}$ или $\mathsf{1}$, либо не содержит ни $\mathsf{0}$, ни $\mathsf{1}$.

Допустив далее, что $p$ не содержит ни $\mathsf{0}$, ни $\mathsf{1}$, мы покажем, что $p$ эквивалентна некоторой формуле, не содержащей ни $\mathsf{0}$, ни $\mathsf{1}$ и не содержащей частей вида $\mathsf{NN}$, $\mathsf{NC}$ и $\mathsf{ND}$. В самом деле, если $p$ содержит часть любого из указанных видов, то с помощью одного из правил

$$\mathsf{NN}x \mathrel{|=|} x, \quad \mathsf{NC}xy \mathrel{|=|} \mathsf{DN}x\mathsf{N}y, \quad \mathsf{ND}xy \mathrel{|=|} \mathsf{CN}x\mathsf{N}y$$

мы можем заменить $p$ такой эквивалентной ей формулой $p'$, что число вхождений в нее символов $\mathsf{N}$, $\mathsf{C}$ и $\mathsf{D}$ (не считая вхождений $\mathsf{N}$, которыми начинались, быть может, некоторые не содержащие других связок подформулы исходной формулы) меньше, чем в $p$. В конце концов мы придем таким путем к некоторой формуле $p'$, в которую $\mathsf{N}$ входит только в составе подформул $\mathsf{N}r$, где $r$ — атомарная формула.

Наконец, приняв, что $p$ не содержит частей вида $\mathsf{0}$, $\mathsf{1}$, $\mathsf{NN}$, $\mathsf{NC}$ и $\mathsf{ND}$, мы покажем, что $p$

эквивалентна некоторой формуле, которая обладает тем же свойством и ни одна из подформул которой, начинающаяся с $\mathsf{C}$, не содержит $\mathsf{D}$. В самом деле, правила

$$\mathsf{CD}xyz \mathrel{|{=}|} \mathsf{DC}xz\mathsf{C}yz, \quad \mathsf{C}x\mathsf{D}yz \mathrel{|{=}|} \mathsf{DC}xy\mathsf{C}xz$$

позволяют уменьшать число вхождений $\mathsf{D}$ в подформулы, начинающиеся с $\mathsf{C}$, до тех пор, пока мы не получим такой формулы $p'$. Очевидно, что такая $p'$ и будет формулой, записанной в дизъюнктивной форме.

Формула $p$, по определению, записана в *приведенной дизъюнктивной форме*, если она записана в дизъюнктивной форме и сверх того

(4) каждая подформула формулы $p$, начинающаяся с $\mathsf{C}$, содержит не более одного вхождения каждой атомарной формулы.

Теорема. *Каждая формула эквивалентна некоторой формуле, записанной в приведенной дизъюнктивной форме.*

Если $q$ — подформула формулы $p$, начинающаяся символом $\mathsf{C}$ и построенная, следовательно, посредством одной лишь операции $\mathsf{C}$, примененной к подформулам $r_i$ и $\mathsf{N}r_i$, где $r_i$ — атомарная формула, то по правилам

$$\mathsf{C}xy \mathrel{|{=}|} \mathsf{C}yx, \quad \mathsf{C}x\mathsf{C}yz \mathrel{|{=}|} \mathsf{CC}xyz$$

мы можем как угодно переставлять подформулы $r_i$ и $\mathsf{N}r_i$. Если $q$ содержит два вхождения какой-либо атомарной формулы $r$, то мы можем считать, что $q$ содержит часть одного из следующих видов: $\mathsf{C}rr$, $\mathsf{C}r\mathsf{N}r$, $\mathsf{CN}rr$, $\mathsf{CN}r\mathsf{N}r$. По одному из правил

$$\mathsf{C}xx \mathrel{|{=}|} x, \quad \mathsf{C}x\mathsf{N}x \mathrel{|{=}|} \mathsf{CN}xx \mathrel{|{=}|} 0$$

мы можем заменить такую часть на эквивалентную ей часть вида $r$, $\mathsf{N}r$ или $0$. Поскольку эта процедура приводит нас к формуле $p'$, эквивалентной формуле $p$ и имеющей меньшую чем $p$ длину, то отсюда по индукции и получается утверждение теоремы.





Формула $p$ по определению записана в *совершенной дизъюнктивной форме* относительно некоторого упорядоченного набора $r_1, \ldots, r_n$ различных атомарных формул, если она имеет следующий вид. Если $n=0$, то $p=0$ или $p=1$. Если $n>0$, то либо $p=0$, либо существует такое целое $m\geqslant 1$, что $p$ имеет вид

$$p = \mathsf{D}q_1\mathsf{D}q_2 \ldots \mathsf{D}q_{m-2}\mathsf{D}q_{m-1}q_m,$$

где каждая подформула $q_i$ в свою очередь имеет вид

$$q_i = \mathsf{C}s_{i1}\mathsf{C}s_{i2} \ldots \mathsf{C}s_{i,\,n-2}\mathsf{C}s_{i,\,n-1}s_{in},$$

а каждая $s_{ij}$ есть $r_j$ или $\mathsf{N}r_j$. Кроме того, если $1\leqslant i<h\leqslant m$, то существует некоторое такое $k$ $(1\leqslant k\leqslant n)$, что $s_{i1}=s_{h1}, \ldots, s_{i,\,k-1}=s_{h,\,k-1}$, в то время как $s_{ik}=r_i$ и $s_{hk}=\mathsf{N}r_i$.

Теорема. *Если формула $p$ не содержит никаких атомарных формул, кроме $r_1, \ldots, r_n$, то $p$ эквивалентна некоторой формуле, записанной в совершенной дизъюнктивной форме относительно $r_1, \ldots, r_n$.*

Мы можем считать, что $p$, записанная в дизъюнктивной форме, построена лишь с помощью символа $\mathsf{D}$ из частей $q_i$, не содержащих $\mathsf{D}$. По правилам

$$\mathsf{D}x\mathsf{N}x \mathrel{|{=}|} 1, \quad \mathsf{C}x1 \mathrel{|{=}|} x, \quad \mathsf{C}x\mathsf{D}yz \mathrel{|{=}|} \mathsf{DC}xy\mathsf{C}xz$$

мы можем заменить $q_i$ на $\mathsf{DC}q_ir_j\mathsf{C}q_i\mathsf{N}r_j$; иными словами, мы можем заменить $q_i$ двумя дизъюнктивными членами: $q_i'=\mathsf{C}q_ir_j$ и $q_i''=\mathsf{C}q_i\mathsf{N}r_j$. Таким путем мы можем добиться, чтобы каждая подформула $q_i$ содержала каждую $r_j$. Как и раньше, мы можем далее добиться, чтобы каждая $q_i$ содержала $r_1, \ldots, r_n$ в определенном порядке, причем так, что ни один из этих символов не будет входить в $q_i$ более чем один раз. Тогда $q_i$ будет иметь требуемую форму.

По правилам

$$\mathsf{D}xx \mathrel{|{=}|} x, \quad \mathsf{D}xy \mathrel{|{=}|} \mathsf{D}yx, \quad \mathsf{D}x\mathsf{D}yz \mathrel{|{=}|} \mathsf{DD}xyz$$

мы можем аналогичным образом расположить вхождения $q_i$ в $p$ так, чтобы они следовали в некотором заданном («лексикографическом») порядке, сгруппированные заданным образом и при этом так, чтобы ни одно из них не входило в $p$ более чем один раз. Тогда $p$ будет записана в совершенной дизъюнктивной форме.

Теорема. *Если $p$ записана в приведенной дизъюнктивной форме, то $p \models 0$ тогда и только тогда, когда $p = 0$.*

Допустив, что $p \neq 0$, мы должны будем показать, что в этом случае для некоторой интерпретации $\varphi$ будет $\varphi p = 1$. Если $p = 1$, то этим свойством будет обладать любая интерпретация $\varphi$. Если же $p \neq 1$, то $p$ есть дизъюнкция членов $q_i$, содержащих одни лишь связки $\mathsf{C}$ и $\mathsf{N}$, и достаточно найти такую $\varphi$, что некоторая $\varphi q_i = 1$. Заметим, что $q_i$ построена из некоторых $r_j$ и $\mathsf{N}r_j$ лишь с помощью связки $\mathsf{C}$ и не содержит ни одной $r_j$ дважды. Пусть $J$ — множество таких $j$, что каждая $q_i$ содержит $\mathsf{N}r_j$. Поскольку атомарные формулы составляют базис $F$ (алгебры формул), отображение $\varphi$ множества $\mathsf{R}_0$ в $\mathsf{B}$, определяемое соотношениями $\varphi r_j = 0$, если $j \in J$, и $\varphi r_j = 1$, если $j \notin J$, может быть расширено до некоторой интерпретации $\varphi$. Так как $q_i$ построена с помощью одной лишь связки $\mathsf{C}$ из частей, имеющих вид $\mathsf{N}r_j$, если $j \in J$, и вид $r_h$, если $h \notin J$, и поскольку для таких частей $\varphi \mathsf{N}r_j = 1$ и $\varphi r_h = 1$, то мы получаем $\varphi q_i = 1$, что и требовалось.

Теорема. *Если формулы $p$ и $p'$ записаны в совершенной дизъюнктивной форме относительно $r_1, \ldots, r_h$, то $p \models p'$ тогда и только тогда, когда $p = p'$.*

Утверждение теоремы тривиально при $n = 0$. Если же $n \neq 0$, то, допустив, что $p \neq p'$, мы получим, что множество $q_i$, входящих в $p$, не совпадает с множеством $q_i$, входящих в $p'$, и можем принять ввиду симметричности ролей $p$ и $p'$, что, например, некоторая $q_i$ входит в $p$, но не входит в $p'$. Если мы построим $\varphi$, как указывалось выше, то будет верно $\varphi q_i = 1$ и, следовательно, $\varphi p = 1$. Если какая-либо $q_h$ входит в $p'$, то, согласно принятому допущению, $q_h \neq q_i$ и для некоторого $k$ один из членов $s_{ik}$, $s_{hk}$ есть $r_k$, а другой





$\mathsf{N}r_k$. Поскольку $\varphi s_{ik} = 1$, то $\varphi s_{hk} = 0$, и так как $q_h$ построена из $s_{hj}$ с помощью одной лишь связки $\mathsf{C}$, то $\varphi q_h = 0$. Наконец, поскольку $p'$ построена с помощью одной лишь связки $\mathsf{D}$ из различных $q_h$, таких, что $\varphi q_h = 0$, мы приходим к выводу, что $\varphi p' = 0$.

## Булева алгебра

Рассмотрим детальнее алгебраическую структуру алгебры высказываний $[F]$. Мы уже видели, что в $[F]$ выполнен закон $x \wedge y = y \wedge x$, а в предыдущем разделе перечислили еще несколько законов, имеющих место для $[F]$. Можно поставить перед собой задачу описать $[F]$ посредством указания всех имеющих место для $[F]$ законов. Задача эта решается просто: множество законов, которым удовлетворяет $[F]$, есть в точности то же множество законов, которым удовлетворяет $\mathsf{B}$. Это следует из определения $[F]$ в терминах множества всех гомоморфизмов, отображающих $F$ в $\mathsf{B}$.

### Упражнение

Докажите это утверждение.

Алгебра, удовлетворяющая всем этим законам, называется *булевой алгеброй.* Булева алгебра $A$ есть, по определению, *свободная булева алгебра с базисом $B$*, если $B$ есть такое подмножество $A$, что каждое отображение $B$ в некоторую булеву алгебру $A'$ может быть единственным образом расширено до гомоморфизма алгебры $A$ в $A'$. Например $[F]$ есть свободная булева алгебра с базисом $\mathsf{R}_0$, а $\mathsf{B}$ — свободная булева алгебра, базисом которой является пустое множество.

### Упражнение

Докажите эти утверждения.

К понятию булевой алгебры очень часто приходят и другим путем, несколько отличным от описанного. Пусть $E$ — произвольное множество, а $A$ — семейство всех подмножеств $x$ множества $E$. Мы превращаем $A$ в алгебру, считая за 0 пустое множество, за 1 — все множество $E$ и для любых $x$ и $y$ из $A$, определяя $\rightarrow x$ как дополнение $E - x$ множества $x$, $x \wedge y$ — как пересечение $x \cap y$ и $x \vee y$ — как объединение $x \cup y$. Тогда $A$ есть *алгебра всех подмножеств* множества $E$. Если $A'$ — произвольное подсемейство семейства $A$, *замкнутое* относительно определенных здесь операций (т. е. 0 и 1 принадлежат $A'$ и для любых $x$ и $y$ из $A'$ $\neg x$, $x \wedge y$, $x \vee y$ также принадлежат $A'$), то $A'$ тоже будет алгеброй с теми же операциями (рассматриваемыми теперь, конечно, только для элементов множества $A'$). Мы будем называть $A'$ просто *алгеброй подмножеств* множества $E$.

Теорема. *Произвольная алгебра подмножеств любого множества есть булева алгебра.*

Мы докажем это утверждение для алгебры $A$ всех подмножеств некоторого множества $E$. Для произвольного элемента $e$ множества $E$ определим отображение $\varphi_e$ множества $A$ в $B$, полагая $\varphi_e x = 1$ тогда, когда $e \in x$. Легко видеть, что каждое $\varphi_e$ есть гомоморфизм и что $x = y$ равносильно $\varphi_e x = \varphi_e y$ для любого $e$ из $E$. Пусть в $B$ выполняется некоторый закон $H(a_1, \ldots, a_n) = K(a_1, \ldots, a_n)$. Если $x_1, \ldots, x_n$ — элементы множества $A$, то для каждого $e$ из $E$

$$\varphi_e H(x_1, \ldots, x_n) = H(\varphi_e x_1, \ldots, \varphi_e x_n) = \\ = K(\varphi_e x_1, \ldots, \varphi_e x_n) = \varphi_e K(x_1, \ldots, x_n),$$

так что $H(x_1, \ldots, x_n) = K(x_1, \ldots, x_n)$. Следовательно, данный закон справедлив и для $A$.

Теорема. *Алгебра высказываний [F] изоморфна некоторой алгебре множеств.*

Пусть $E$ — множество всех гомоморфизмов множества $F$ в $\mathbf{B}$. Каждому элементу $[p]$ алгебры $[F]$ мы можем сопоставить множество $J[p]$ всех таких гомоморфизмов $\varphi$, что $\varphi p = 1$. Простые соображения, показывающие, что $J$ есть гомоморфизм, уже приводились выше в связи с определением понятия интерпретации; что же касается взаимной однозначности отображения $J$ (т. е. того, что $J[p] = J[q]$ влечет $p = q$), то она обусловливается уже определением $[F]$ как факторалгебры алгебры $F$.





Класс всех булевых алгебр можно описать более явным образом — как класс алгебр, удовлетворяющих некоторому конечному числу законов.

Теорема. *Алгебра $A$ с операциями 0, 1, $\neg x$, $x \wedge y$ и $x \vee y$ есть булева алгебра, если она удовлетворяет каждому из следующих законов.*

$$\neg 0 = 1, \quad 0 \wedge x = 0, \quad 0 \vee x = x, \quad \neg 1 = 0,$$
$$1 \wedge x = x, \quad 1 \vee x = 1,$$
$$\neg\neg x = x, \quad \neg(x \wedge y) = \neg x \vee \neg y,$$
$$\neg(x \vee y) = \neg x \wedge \neg y,$$
$$(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z),$$
$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z),$$
$$x \wedge x = x, \quad x \wedge y = y \wedge x, \quad (x \wedge y) \wedge z = x \wedge (y \wedge z),$$
$$x \vee x = x, \quad x \vee y = y \vee x, \quad (x \vee z) \vee z = x \vee (y \vee z),$$
$$x \wedge \neg x = 0, \quad x \vee \neg x = 1.$$

Прежде всего легко проверить, что все эти законы выполняются в двухэлементной алгебре $\mathbf{B}$, а следовательно, и в булевой алгебре. Далее, введем на $F$ отношение $p \equiv q$, равносильное по определению тому, что равенство $p = q$ вытекает из выполнения на $F$ всех перечисленных законов. Достаточно будет показать, что если $p \mid\!= q$, то $p \equiv q$. Заметим, что перечисленные в утверждении теоремы законы суть с точностью до несущественного изменения порядка перечисления именно те законы, которые использовались выше для преобразования произвольной формулы $p$ в эквивалентную ей формулу, записанную в совершенной дизъюнктивной форме. Если $p$ и $q$ — две формулы, не содержащие никаких символов отношений, кроме $r_1, \ldots, r_n$, а $p'$ и $q'$ — их совершенные дизъюнктивные формы относительно этих символов, то $p \equiv p'$ и $q \equiv q'$. Допустим теперь, что $p \mid\!= q$; тогда, как было показано выше, $p' = q'$. Поскольку отношение $\equiv$ есть, очевидно, отношение эквивалентности, то $p \equiv q$.

### Упражнения

1. Среди законов, входящих в выписанное в утверждении последней теоремы множество, есть законы, выводимые из других законов этого же множества; упростите это множество.

2. Каждая булева алгебра $A$ изоморфна некоторой алгебре подмножеств множества $J(A)$ гомоморфизмов $A$ в $\mathbb{B}$ [теорема Стоуна]. Докажите это утверждение для случая конечной алгебры $A$ и покажите, что $A$ — свободная булева алгебра.

3. Если $A$ — конечная булева алгебра, то она изоморфна алгебре всех подмножеств множества $J(A)$; если же $A$ бесконечна, то это необязательно так. Докажите оба эти утверждения.

[Указание: алгебра всех подмножеств непустого множества имеет минимальные элементы, или *атомы* $x$, обладающие тем свойством, что для любого $y$ имеет место либо $x \wedge y = x$, либо $x \wedge y = 0$; покажите, что свободная алгебра с бесконечным базисом не имеет атомов.]

Сказанное выше об алгебре Линденбаума сохраняет силу и для языка $L$, не ограниченного рамками пропозиционального языка; однако рассмотрение $[F]$ как булевой алгебры не дает полного представления об $[F]$, поскольку такое рассмотрение не принимает в расчет роли переменных и кванторов. В целях преодоления этого недостатка было предложено два довольно близких обобщения понятия булевой алгебры: *цилиндрические алгебры*, введенные в рассмотрение Тарским и его школой, и *полиадические алгебры* Халмоша. В обоих типах алгебр имеется бесконечное множество операторов цилиндрификации $C_x$, интерпретируемых следующим образом: $C_x[p] = [\mathsf{E}xp]$. В полиадических алгебрах имеются также операторы подстановки, посредством которых одна переменная заменяется на другую; в цилиндрических алгебрах, где имеются гиперплоскости $[x = y]$, для такой замены оказывается полезным использовать то обстоятельство, что

$$[\mathsf{E}x\,(p\,(x) \wedge x = y)] = [p\,(y)].$$

### Упражнение

Можно рассматривать $[p(x, y, z)]$ как геометрическое место точек, удовлетворяющих условию $p(x, y, z)$, в пространстве точек $(x, y, z)$; покажите, что $C_z[p(x, y, z)]$ — прямой цилиндр, образуемый кривой $[p(x, y, z)]$.





## Варианты пропозициональной логики

Известно несколько разновидностей обычной, *классической, логики*. Некоторые из этих разновидностей обязаны своим возникновением чистой любознательности или желанию получить более широкий взгляд на классическую логику. Большинство же этих разновидностей представляет собой попытки преодолеть некоторое несоответствие классической логики нашим интуитивным представлениям о «логике». Как правило, эти построения не ограничены рамками пропозициональной логики, так что мы вводим здесь это ограничение исключительно ради простоты изложения.

*Другие двузначные логики.* Классическая логика двузначна в том смысле, что множество $\mathbb{B}$ ее истинностных значений состоит из двух элементов. Какова природа этих двух элементов, совершенно несущественно, так что можно видоизменять пропозициональную логику, выбирая связки, соответствующие какому-либо множеству операций, отличному от множества, состоящего из элементов 0, 1, $\to x$, $x \wedge y$ и $x \vee y$.

Надо заметить, что в известном смысле ничего принципиально нового мы таким образом не получим; дело в том, что уже введенное нами множество операций *функционально полно*: любая операция конечного ранга, определенная на $\mathbb{B}$, выразима в терминах данных операций. Выразительные возможности языка $L$ нельзя расширить никаким усовершенствованием его формальной структуры. Разумеется, сузить эти выразительные возможности — вполне реальное дело. Исследование систем, получающихся в результате такого сужения выразительных средств, представляет зачастую большой интерес; примером может служить весьма важная теория, единственной связкой которой является $\mathsf{J}$.

### Упражнения

1. Докажите функциональную полноту классической пропозициональной логики.

[Указание: воспользуйтесь совершенной дизъюнктивной формой.]

4 Зак. 1253

2. Докажите, что 0, 1, $+$ и $\times$ образуют функционально полное множество, если под $+$ и $\times$ понимать сложение и умножение по модулю 2, т. е. эти операции отличаются от обычного сложения и умножения чисел только тем, что $1+1=0$.

3. Покажите, что множество, состоящее из одной-единственной связки Шеффера $\mathsf{S}pq = \mathsf{CN}p\mathsf{N}q$, является функционально полным.

4. Покажите, что связка $\mathsf{J}$ не образует функционально полного множества; исследуйте логику, имеющую $\mathsf{J}$ в качестве единственной связки.

*Многозначные логики.* Пусть вместо $\mathbf{B}$ в рассмотрение вводится некоторое множество $C$ действительных чисел $x$, $0 \leqslant x \leqslant 1$, для которых можно определить те же операции, что и в $\mathbf{B}$. Естественно принять точку зрения, согласно которой этим истинностным значениям $x$ соответствуют различные степени неопределенности, хотя, конечно, такой пример, как $\varphi p = {}^1/_2$ влечет $\varphi(p \vee \neg p) = {}^1/_2$, не слишком хорошо согласуется с такой интерпретацией.

### Упражнения

1. Какие законы булевой алгебры остаются в силе при замене $\mathbf{B}$ на $C = \{0, {}^1/_2, 1\}$?

2. Образуют ли обычные пять операций функционально полное множество на этом $C$?

3. Разрешимы ли описанные выше многозначные логики?

*Теория вероятностей.* Теория вероятностей в ее простейшей форме представляет собой нечто вроде многозначной логики, в которой каждой формуле $p$ приписывается в качестве ее вероятности некоторое число $x$, где $0 \leqslant x \leqslant 1$, обозначаемое через $Pr(p)$. Обычно это делается следующим образом. Предполагается, что каждое подмножество множества $J$ всех интерпретаций или событий имеет некоторую меру. Тогда в качестве $Pr(p)$ выбирается мера множества $J(p)$ всех таких интерпретаций $\varphi$, для которых $\varphi p = 1$. В таком случае вероятность как функция, выражающая меру, удовлетворяет соотношению

$$Pr(p \vee q) = Pr(p) + Pr(q) - Pr(p \wedge q).$$





Таким образом, теория вероятностей отличается от логики в узком смысле этого слова тем, что $Pr(p \vee q)$ определяется не только через $Pr(p)$ и $Pr(q)$.

*Модальная логика.* Назначение различных систем модальной логики состоит в том, чтобы включить в пропозициональную логику так называемые модальности, к числу которых относятся, например, *необходимость* и *возможность*. Обычно вводят связку $\blacksquare$, полагая по определению, что $\blacksquare p$ означает, что высказывание $p$ необходимо истинно; тогда $\blacklozenge p \to \blacksquare \to p$ означает возможность $p$, а связка $p \prec q = \blacksquare (p \supset q)$ выражает так называемую строгую импликацию. Строгая импликация была введена Льюисом с целью избавиться от того недостатка обычной связки $p \supset q$ — так называемой материальной импликации, — который проявляется в признании истинными таких, например, импликаций, как (лед горяч) $\supset$ (трава зелена). Весьма любопытная семантика для модальной логики была недавно предложена Крипке; состоит она в общих словах в следующем. С каждой интерпретацией $\varphi$ (в обычном смысле) связывается множество $K(\varphi)$ других интерпретаций $\varphi$, имеющих ту же самую область; если $\varphi$ воспринимать как некоторый реальный мир, то элементы этого множества суть возможные миры. Тогда значение символа $\blacksquare$ определяется условием: $\varphi(\blacksquare p) = 1$ равносильно $\varphi p = 1$ для всех $\varphi$ из $K(\varphi)$. Формальная близость с соответствующим условием для $\varphi(\mathsf{A}xp) = 1$ очевидна; в известном смысле можно сказать, что при таком понимании модальностей функциональные символы и символы отношений связываются кванторами общности.

*Интуиционистская логика.* Из всех видоизменений классической логики наиболее важной является интуиционистская логика. Интуиционизм представляет собой детально разработанное философское направление, выражающее серьезную критику методов рассуждений, принятых в классической математике, и провозглашающее необходимость ограничения методов математических рассуждений, в особенности относящихся к бесконечным множествам, некоторыми в определенном смысле конструктивными и интуитивно ясными принципами. В качестве самого грубого примера предложение $\mathsf{E}xp(x)$ о натуральных числах можно интерпретировать как утверждение о том, что можно указать некоторое натуральное число $n$, о котором можно доказать, что оно обладает свойством $p$. Формальное отрицание такого утверждения, имеющее вид $\mathsf{A}x\neg p(x)$, конструктивно можно понимать только как утверждение о возможности доказать для каждого натурального $n$, что $n$ не обладает указанным свойством $p$. Но может, конечно, оказаться, что ни одно из этих предложений не является истинным в таком конструктивном смысле. Последовательные интуиционисты не признают универсальной общезначимости формулы $p\vee\neg p$, выражающей так называемый *закон исключенного третьего*. Интуиционистское пропозициональное исчисление было аксиоматизировано Гейтингом; одна из аксиоматизаций интуиционистской логики отличается от обычной аксиоматизации классической пропозициональной логики как раз исключением из числа аксиом формулы, выражающей закон исключенного третьего.

Мы не будем здесь вдаваться в обсуждение синтаксиса и дедуктивной теории интуиционистской логики, но опишем предложенное Тарским семантическое определение общезначимости для интуиционистской пропозициональной логики. Язык $L$ — тот же, что и в классической теории, но, переходя к семантике, мы вместо $\mathbf{B}$ возьмем некоторую совокупность $C$ подмножеств какого-нибудь топологического пространства $E$. Для простоты мы в качестве $E$ выберем обычную плоскость.

Пусть $U$ — некоторое подмножество $E$. Определим *внутренность* $U^*$ множества $U$ как множество, состоящее из всех таких точек $x$ пространства $E$, для которых $U$ целиком содержит внутренность некоторого круга положительного радиуса с центром в $x$. Множество $U$ называется *открытым*, если $U=U^*$. Теперь мы можем определить $C$ как множество всех открытых подмножеств плоскости $E$.

Пустое множество $0=\varnothing$ и вся плоскость $1=E$ — открытые множества. Кроме того, если $U$ и $V$ — открытые множества, то множества $U\cap V$ и $U\cup V$ также открыты, так что мы можем положить по определению $U\wedge V=U\cap V$ и $U\vee V=U\cup V$. Если $U$ открыто, то его дополнение $E-U$ не обязательно является открытым; определим $\neg U$ как $(E-U)^*$, т. е. как максимальное открытое множество, не пересекающееся с $U$. Последнее обстоятельство обеспечивает выполнимость $U\wedge\neg U=0$ — закона, от которого, в отличие от закона исключенного третьего, мы вовсе не собираемся отказываться. Чтобы показать, что закон исключенного третьего при нашей семантике неверен, возьмем в качестве $U$ открытую нижнюю полуплоскость: $U=[(x,y):y<0]$. Тогда $E-U$ есть замкнутая полуплоскость: $E-U=[(x,y):y\geqslant 0]$, так что $\neg U=(E-U)^*$ — открытая верхняя полуплоскость: $[(x,y):y>0]$. Очевидно, что $U\vee\neg U\neq 1$.

### Упражнения

1. Исследуйте отношения между множествами $U$, $\neg U$, $\neg\neg U$, ... для произвольного множества $U$.

2. Какое утверждение о множествах $U$ и $V$ выражается уравнением $\mathsf{J}UV=1$? (Здесь, как и выше, принято $\mathsf{J}=\mathsf{DN}$.)

3. Покажите, что если взять в качестве $E$ топологическое пространство, каждое подпространство которого совпадает со своей внутренностью (т. е. $U=U^*$ для всех $U\subseteq E$), то приведенные выше определения приводят к классической пропозициональной логике.

## Разрешимость и аксиоматизируемость

В качестве нашей главной задачи мы выбрали выше задачу нахождения синтаксического определения для отношения семантического следования. Ввиду того что $p\models q$ равносильно $\models\mathsf{J}pq$, мы можем вместо этой задачи рассматривать равносильную ей, состоящую в том, чтобы охарактеризовать синтаксическими средствами множество $T$ общезначимых формул некоторой теории, описанной в семантических терминах. При этом, если не вдаваться в подробности, могут возникнуть три различные ситуации, которые мы и проиллюстрируем на трех важных примерах.

*Пропозициональная логика.* В данном случае $L$ — это пропозициональный язык, а теория $T$ охватывает все общезначимые формулы языка $L$. Мы видели уже, что эта теория является в некотором (самом сильном из всех разумных) смысле разрешимой: имеется чисто механический способ проверки, приложимый к любой формуле, пользуясь которым, мы можем ответить на вопрос, принадлежит ли эта формула $T$. В силу этого обстоятельства дедуктивная аксиоматизация $T$ является в некотором смысле излишней роскошью, хотя выписать множество аксиом и правил вывода, посредством которых можно вывести все формулы из $T$ и только эти формулы, оказывается совсем нетрудным. Такая аксиоматизация является составной частью аксиоматизации логики предикатов, которую мы рассмотрим ниже.

*Логика предикатов.* Под *логикой предикатов* мы понимаем теорию $T$, включающую в себя все общезначимые формулы языка $L$ в полном его объеме (как мы его описывали вначале). Предположим, что $L$ имеет хотя бы один функциональный символ ранга, не низшего чем 1, или же один символ отношения ранга, не низшего чем 2. Тогда теория $T$ ни в каком из разумных смыслов этого слова не является разрешимой; кратким доказательством теоремы, устанавливающей этот результат (теорема эта, доказанная Чёрчем, основывается на результатах Гёделя), мы закончим нашу книгу. В то же время ниже нам удастся, следуя Гёделю, показать, что существует в высшей степени удовлетворительная аксиоматизация теории $T$ посредством аксиом и правил вывода, пользуясь которыми, можно доказать в точности все формулы, входящие в $T$.

*Арифметика.* Допустим теперь, что наш полный язык $L$ содержит конкретные символы $=$, $0$, $1$, $+$ и $\times$. Мы ограничимся рассмотрением интерпретаций нашей теории на единственной структуре $N$, областью которой является множество натуральных чисел $0, 1, 2 \ldots$, причем выбранные символы получают свои обычные интерпретации. Под *арифметикой* мы будем понимать





теорию, состоящую из всех формул языка $L$, общезначимых при каждой интерпретации на такой стандартной структуре. Основной результат Гёделя состоит в том, что арифметика не только не является разрешимой, но и неаксиоматизируема. Таким образом, по отношению к арифметике наша основная цель, состоящая в получении синтаксического определения общезначимости, обречена на неудачу, и нам остается лишь надеяться, что в результате этой неудачи мы станем мудрее.

Мы пока не будем давать точного определения, что значит, что некоторое множество *разрешимо*; достаточно знать, что любое множество, о котором можно утверждать, что оно разрешимо в интуитивном понимании этого слова, остается таковым и в рамках соответствующего определения. Отметим, что все предложенные до сих пор определения этого понятия оказались эквивалентными между собой; одно из них мы сформулируем ниже, когда нам без него уже действительно нельзя будет обойтись. Что же касается *аксиоматизируемости*, то определение этого понятия легко дать в терминах разрешимости. Это достигается, например, следующим образом. Задается некоторое множество формул, называемых по определению *аксиомами*, и некоторое отношение конечного ранга между формулами, в силу которого некоторая формула называется следующей из некоторых других формул по определенным *правилам вывода*. Конечная последовательность формул называется *доказательством*, если каждая формула из этой последовательности либо является аксиомой, либо следует из предыдущих формул последовательности по правилам вывода: доказательство есть доказательство последней формулы в такой последовательности. Формула, для которой существует доказательство, называется *теоремой*. Мы будем требовать, чтобы свойство быть аксиомой и отношение следования по правилам вывода были разрешимыми. Тогда свойство быть теоремой также будет разрешимым: из определения понятия доказательства прежде всего вытекает, что для любой заданной конечной последовательности формул имеется простой способ проверки, является ли она доказательством. В то же время аксиоматизируемая теория, включающая все теоремы, вовсе не обязательно разрешима: поиски доказательства для какой-либо конкретной формулы, если они остались безрезультатными, не дают возможности прийти к заключению, существует ли вообще такое доказательство.

Совсем тривиальное рассуждение показывает, что разрешимая теория непременно является аксиоматизируемой: на худой конец, аксиоматизация может быть достигнута объявлением всех формул теории аксиомами (при этом нам не понадобятся никакие правила вывода). С другой стороны, мы уже отмечали, что логика предикатов аксиоматизируема, но не разрешима. Мы отмечали также, что арифметика даже и не аксиоматизируема.

С разрешимостью связано понятие полноты. Теория $T$ называется *полной*, если для каждого предложения $p$ либо само $p$, либо $\neg p$ принадлежит $T$. Если аксиоматизируемая теория $T$ полна и непротиворечива, то она разрешима. Чтобы убедиться в этом, допустим, что $T$ аксиоматизируема, полна и непротиворечива, и возьмем произвольное предложение $p$. Из предположения об аксиоматизируемости следует, что формулы языка $L$ можно перенумеровать с помощью натуральных чисел, из чего в свою очередь нетрудно получить и пересчет $s_1, s_2, \ldots$ всех конечных последовательностей формул. Поскольку свойство быть доказательством разрешимо, мы можем «просеять» перечень $s_1, s_2, \ldots$, оставив в нем только формулы, являющиеся доказательствами, а поскольку это просеивание можно продолжать, двигаясь по этому перечню как угодно далеко, то в результате мы получим пересчет $p_1, p_2, \ldots$ всех доказательств. Так как $T$ по предположению полна, то либо $p$, либо $\neg p$ принадлежит $T$. А так как $T$ аксиоматизируема, то для той из этих формул, которая входит в $T$, существует доказательство. Таким образом, для некоторого натурального $n$ предложение $p_n$ будет — и это можно усмотреть из вида $p_n$ — доказательством для $p$ или для $\neg p$. Если $p_n$ есть





доказательство для $p$, то $p$ есть теорема, т. е. $p \in T$. Если $p_n$ есть доказательство для $\neg p$, то $\neg p \in T$, а поскольку $T$ по предположению непротиворечива, то мы заключаем, что тогда $p$ не принадлежит $T'$. Описанная процедура, как легко понять, позволяет решить в принципе для любой формулы $p$, принадлежит ли она теории $T$.

Теория $T$, определенная семантическим образом исходя из некоторой определенной структуры — скажем, арифметика, не имеющая никаких функциональных символов и символов отношений, кроме 0, 1, $=$, $+$ и $\times$, — тривиальным образом полна и непротиворечива. Следовательно, для таких теорий понятия разрешимости и аксиоматизируемости совпадают.

## Разрешимые теории

Для сколько-нибудь сложной математической теории разрешимость является скорее исключением из общего правила. И все же для некоторых важных математических теорий удается доказать их разрешимость. Большинство доказательств разрешимости для теорий, язык которых содержит кванторы, проводится методом, которой получил название метода *исключения кванторов.* Мы проиллюстрируем этот метод на примерах двух довольно простых теорий.

*Плотный линейный порядок.* Мы начнем с семантического описания теории $T$ плотного линейного порядка. Пусть $L$ есть язык, включающий связки **0**, **1**, **N**, **C**, **D**, **A** и **E** и бесконечное множество **V** переменных, не содержащий никаких функциональных символов и никаких символов отношений, кроме $=$, $<$ и $\leqslant$. Мы ограничимся рассмотрением интерпретаций нашей теории в области $R$ действительных чисел, на которой используемые в $T$ символы отношений имеют свой обычный смысл. Теория $T$ — это множество всех формул, общезначимых при каждой такой интерпретации. Разрешающий метод, который мы опишем, предложен Лэнгфордом; исчерпывающее обоснование дал Роджерс.

Мы покажем, что каждая формула вида $p=\mathsf{E}vq$, где $q$ не содержит кванторов, эквивалентна некоторой бескванторной формуле $p'$, не содержащей других переменных, кроме тех, которые входят в $p$ свободно. Поскольку $\mathsf{A}vq \models\dashv \neg\mathsf{E}v\neg q$, то то же самое справедливо и для формул вида $p=\mathsf{A}vq$. Применяя повторно это преобразование, мы сможем заменить любую формулу $p$ эквивалентной ей бескванторной формулой $p'$, не содержащей никаких переменных, кроме тех, что входят свободно в $p$. Если, в частности, $p$ есть предложение, то $p'$ вообще не содержит никаких переменных, а следовательно, не содержит никаких символов, кроме $\mathsf{0}$, $\mathsf{1}$, $\mathsf{N}$, $\mathsf{C}$ и $\mathsf{D}$. Мы уже видели, что любая такая формула пропозициональной логики тривиальным образом сводится к эквивалентной форме $\mathsf{0}$ или $\mathsf{1}$. Таким образом решается вопрос о проверке на истинность любого предложения; общезначимость же формулы $p$, не являющейся предложением, равносильна истинности некоторого предложения вида $\mathsf{A}x_1\ldots\mathsf{A}x_n p$

Пусть теперь $p=\mathsf{E}vq$, где $q$ не содержит кванторов; ясно, что мы можем записать $q$, пользуясь только символами $=$ и $<$ (без символа $\leqslant$). Мы можем допустить, что $q$ записана в дизъюнктивной форме, т. е. имеет вид $q=\bigvee q_i$, где каждая $q_i$ есть $q_i=\bigwedge q_{ij}$, а каждая $q_{ij}$ имеет одну из следующих форм: $x=y$, $x<y$, $\neg(x=y)$ или $\neg(x<y)$. Заменим $x\neq y$ на $x<y\vee y<x$, а $x\nless y$ — на $x=y\vee y<x$, после чего преобразуем полученное выражение согласно дистрибутивному закону $r\wedge(s\vee t)\models\dashv(r\wedge t)\vee(r\wedge s)$. Мы получим таким образом формулу, эквивалентную формуле $q$ и записанную в дизъюнктивной форме, где каждая подформула $q_{ij}$ имеет вид $x=y$ или $x<y$. Ясно, что формула вида $p=\mathsf{E}v(\bigvee q_i)$ эквивалентна формуле $\bigvee vq_i$, так что вместо $q$ мы можем рассматривать $q_i$ — иными словами, допустить, что $q=\bigwedge q_j$, где каждая $q_j$ имеет вид $x=y$ или $x<y$. Ввиду того что если $r$ не содержит $v$, то $\mathsf{E}v(r\wedge s)\models\dashv r\wedge\mathsf{E}vs$, мы можем теперь вместо $p$ рассматривать формулу $p'\wedge\mathsf{E}v\bigwedge q_j$, где каждая подформула $q_j$ содержит $v$. Таким образом, мы можем считать, что $p$ имеет вид $\mathsf{E}v\bigwedge q_j$, где каждое $q_j$ имеет вид $v=x$, $x<v$ или $v<x$.





Очевидно, что вхождение в $p$ подформулы вида $v=v$ можно попросту опустить, а наличие вхождений вида $v<v$ означает, что $p$ неверна. Если в $p$ входит подформула вида $v=x$, где $x$ отлично от $v$, то $p$ можно представить в виде $p=\mathsf{E}v[v=x\wedge r(v,x)]$, что, очевидно, эквивалентно $p'=r(x,x)$. Теперь остается рассмотреть лишь тот случай, когда $q$ представляет собой конъюнкцию формул $x_1<v,\ldots,x_m<v$ и $v<y_1,\ldots$ $\ldots, v<y_n$, причем все $x_i$ и $y_j$ отличны от $v$. В этом случае $p$, очевидно, эквивалентна $p'$ — конъюнкции всех формул $x_i<y_j$ $(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n)$. Этим замечанием завершается доказательство разрешимости теории $T$.

Теория $T$ была определена нами семантически, в связи с действительными числами; ясно, однако, что в точности те же рассуждения проходят и для рациональных чисел или даже для множества рациональных чисел, заключенных строго между 0 и 1, знаменателями которых являются степени числа 2. В самом деле, в нашем рассуждении нам понадобилось лишь конечное множество допущений о действительных числах, выразимых посредством некоторого множества $A$ предложений языка $L$, так что рассуждение это справедливо по отношению к любой теории, включающей $A$. Но $A$ есть не что иное, как множество аксиом для $T$ — в том смысле, что $T$ совпадает с множеством всех семантических следствий из $A$. Чтобы убедиться в этом, заметим прежде всего, что так как $A$ есть часть $T$, то то же самое справедливо и по отношению к множеству всех следствий из $A$; с другой стороны, если какая-нибудь формула $p$ принадлежит $T$, то с помощью одних только формул из $A$ мы можем показать, что $p$ эквивалентна $\mathsf{1}$ — иными словами, можем получить $p$ как следствие из $A$. Если бы мы с самого начала определяли $T$ посредством множества $A$ аксиом — что, пожалуй, было бы более естественным, — то могли бы заранее и не знать, что $T$ полна; но доказательство разрешимости показывает фактически, что каждое предложение эквивалентно — если принять $A$ — либо $\mathsf{0}$, либо $\mathsf{1}$, так что либо само это предложение, либо его отрицание входит в $T$, что и означает полноту $T$.

Если вместо множества всех действительных чисел взять его подмножество, состоящее, например, из таких действительных чисел $x$, что $5 \leqslant x \leqslant 8$, то мы получим некоторую новую теорию — обозначим ее через $T'$, — также являющуюся разрешимой. В самом деле, если пополнить язык $L$ двумя новыми символами 5 и 8, то в точности тем же методом, что и выше, доказывается разрешимость получающейся в результате теории $T''$, из чего в свою очередь следует, что подтеория $T'$ теории $T''$ также разрешима.

### Упражнения

1. Докажите разрешимость $T'$.
2. Составьте множество $A$ аксиом для $T$ и множество $A'$ аксиом для $T'$.

*Теория равенства.* Пусть $L$ включает в себя все связки, бесконечное множество переменных и единственный символ отношения $=$ и не содержит никаких функциональных символов. *Теорией равенства* $T$ будем, по определению, называть множество всех формул, истинных при всех интерпретациях, в которых символ $=$ понимается в своем обычном смысле — как обозначение равенства (тождества). Ясно, что $T$ не может быть полна, так как для каждого $n>1$ предложение $C_n$

$$\mathsf{E}x_1 \ldots \mathsf{E}x_n \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j,$$

утверждающее, что некоторая структура содержит по крайней мере $n$ элементов, истинно при одних интерпретациях и ложно при других. Поэтому если мы попытаемся воспользоваться методом исключения кванторов, то нам придется расширить язык $L$ таким образом, чтобы предложение $C_n$ можно было записать без кванторов. Расширим $L$ до некоторого языка $L'$ за счет добавления бесконечного множества символов отношений $c_2, c_3, \ldots$ ранга 0, а множество $T$ расширим до $T'$ — множества формул, истинных при всех интерпретациях, в которых символ $=$ интерпретируется как равенство, а каждый из символов $c_n$ — как $C_n$.





Исключая, как и выше, кванторы, с той лишь разницей, что теперь мы воспользуемся совершенной дизъюнктивной формой, сведем случай произвольной формулы $p$ к случаю формулы $p = \mathsf{E}vq$, где $q$ есть конъюнкция некоторого числа равенств $v = x_i$ и $x_i = x_j (i<j)$ и отрицаний остальных равенств такого вида для набора различных переменных $v$, $x_1, \ldots, x_n$. При этом может, в частности, оказаться, что $q$ содержит каждое равенство $v = x_i$ или $x_i = x_j$. Пусть $r = \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j$. Очевидно, что формула

$$p = \bigwedge \mathsf{E}v (r \wedge v \neq x_1 \wedge \ \ldots \ \wedge v \neq x_n)$$

эквивалентна формуле $p' = r \wedge c_{n+1}$.

Этим завершается процедура исключения кванторов, и мы видим, что каждое предложение языка $L'$ эквивалентно относительно $T'$ некоторому выражению, образованному при помощи связок из $c_n$. Легко показать, что в таком случае предложение $p$ должно выражать, что мощность $n$ соответствующей области принадлежит некоторому множеству $U$, являющемуся объединением конечного числа непересекающихся интервалов вида $[n : a \leqslant n \leqslant b]$ или $[n : a \leqslant n]$. Очевидно, что $p$ истинно тогда и только тогда, когда $U$ состоит из одного-единственного интервала $[n : 1 \leqslant n]$. Из этого, в частности, следует, что в языке $L'$ нет таких предложений, которые выполнялись бы для всех структур, имеющих конечную область, и только для этих структур.

Обращаясь теперь к теории $T$, мы видим, что она также разрешима: имеется алгорифм, переводящий произвольное предложение языка $L$ в эквивалентное ему относительно данной теории предложение, имеющее вид пропозициональной комбинации предложений вида $C_n$.

Как и в случае теории плотного линейного порядка, мы можем извлечь из наших рассуждений множество $A$ аксиом для теории $T$. Таковыми будут предложения, утверждающие, что отношение, обозначаемое посредством символа $=$, рефлексивно, симметрично и транзитивно:

$$\mathsf{A}x\,(x=x),\quad \mathsf{A}x\mathsf{A}y\,(x=y\supset y=x),$$
$$\mathsf{A}x\mathsf{A}y\mathsf{A}z\,(x=y\wedge y=z\supset x=z).$$

Стоит отметить, что, поскольку этим аксиомам удовлетворяет произвольное отношение эквивалентности, то, очевидно, средствами языка $L$ невозможно выразить условия, которые позволили бы выделить равенство из всех отношений эквивалентности.

### Упражнения

1. Проведите во всех деталях доказательство разрешимости теории равенства.

2. Существует ли бесконечное множество $P$ предложений, такое, что $\varphi P=1$ выражает бесконечность области интерпретации $\varphi$? Существует ли такое множество $P$, что $\varphi P=1$ выражает конечность области?

*Другие разрешимые теории.* Упомянем еще лишь о двух разрешимых теориях. Для каждой из этих теорий доказательство разрешимости методом исключения кванторов представляет известную трудность и связано с учетом специальных свойств соответствующей теории. Первая из этих теорий — теория абелевых групп, формулируемая на языке, включающем символ $=$ и символ для групповой операции. Разрешающая процедура для этой теории, предложенная Шмелёвой, приводит к тому же результату, что и для теории равенства, хотя и значительно более сложным путем. Другой — и, пожалуй, самый важный — пример разрешающей процедуры предложен Тарским для теории действительных чисел, язык которой содержит символы для равенства, сложения и умножения. Теория эта, конечно, полна, и разрешающий метод дает возможность получить систему аксиом; полезно отметить, что любое свойство действительных чисел, выразимое средствами указанного языка, справедливо и для всех других моделей вещественно-замкнутых полей, удовлетворяющих этим аксиомам. Результат Тарского, относящийся к теории действительных чисел, легко переносится на теорию комплексных чисел; аппарат аналитической геометрии сразу же приводит и к разрешающему методу для евклидовой геометрии.





Чтобы понять, насколько близко арифметика действительных чисел подходит к границе между разрешимостью и неразрешимостью, заметим, что каждое натуральное число $n$ может быть охарактеризовано в этой теории посредством формулы

$$p_n(x)=\mathsf{A}y\,[xy=y+\ \dots\ +y]\quad (n\ \text{слагаемых});$$

в то же время, если бы существовала формула $p(x)$, характеризующая в точности весь натуральный ряд, то в нашу теорию можно было бы перевести любое предложение арифметики натуральных чисел и неразрешимость рассматриваемой нами ограниченной арифметики действительных чисел вытекала бы из неразрешимости арифметики натуральных чисел.

*Неразрешимые теории.* Известен ряд результатов о неразрешимости, доказательства которых не зависят от (или, быть может, проще) гёделевского доказательства неразрешимости арифметики. Результаты Поста и Тьюринга устанавливают неразрешимость следующей проблемы: узнать по произвольной совокупности данных, поданных на вход некоторой идеализированной вычислительной машины, закончится ли процесс вычисления. С этим результатом связана неразрешимость проблемы тождества слов для полугрупп: существуют такие термы $t_1, s_1, \dots, t_n, s_n$ и $u$ в языке теории полугрупп с символами $=$ и умножения, что множество термов $w$, для которых верна формула $t_1=s_1\wedge\dots\wedge t_n=s_n\supset w=u$, неразрешимо. На этих результатах основаны, прямо или косвенно, многие другие результаты о неразрешимости. Одним из наиболее трудных таких результатов явилось предложенное Новиковым и Буном доказательство неразрешимости знаменитой проблемы тождества слов для групп, не поддававшейся решению в течение многих лет.

## Аксиоматизация логики предикатов

Последующие разделы настоящих заметок будут посвящены двум основным вопросам: во-первых, мы докажем аксиоматизируемость логики предикатов и, во-вторых, наметим доказательство неаксиоматизируемости арифметики, из чего в свою очередь следует неразрешимость как самой арифметики, так и логики предикатов. Разумеется, по ходу дела мы будем касаться и других результатов, связанных с двумя упомянутыми.

Под *логикой предикатов* мы понимаем теорию $T$ всех формул некоторого языка $L$, описанного в начале книги, истинных при любой интерпретации. Мы дадим две, несколько отличные друг от друга, аксиоматизации этой теории. Первая из них — это обычная аксиоматизация, совпадающая в основном с той, что была использована Расселом и Уайтхедом. Утверждение о том, что аксиомы и правила этой аксиоматизации действительно дают синтаксическую характеристику определенной семантическим образом теории $T$, называют обычно теоремой Гёделя о полноте; поскольку, однако, мы пользуемся термином «полнота» в другом смысле, мы будем называть это предложение теоремой адекватности. Доказательство этой теоремы, которое мы приведем, — это предложенное Генкиным усовершенствование доказательства Гёделя. Вторая аксиоматизация, принадлежащая Генцену, несколько менее известна, но зато является в некотором смысле более естественной, не говоря уже о том, что она удобнее для практического использования. Мы изложим доказательство адекватности системы Генцена, следуя Расёвой и Сикорскому.

В качестве связок языка $L$ нам будет удобно ограничиться символами $\mathsf{0}$, $\mathsf{J}$ и $\mathsf{A}$, рассматривая остальные символы как сокращения, например $\neg p$ вместо $p \supset \mathsf{0}$ и $\mathsf{E}x$ вместо $\neg \mathsf{A}x \neg$. Мы будем предполагать, что в $L$ входят связки $\mathsf{0}$, $\mathsf{J}$, $\mathsf{A}$, бесконечное множество $\mathsf{V}$ переменных и некоторая совершенно произвольная совокупность функциональных символов и символов отношений различных рангов.





Опишем теперь первую из упомянутых аксиоматизаций. *Аксиомы* задаются посредством пяти схем, каждая из которых охватывает все формулы определенного вида. Схемы аксиом имеют следующий вид:

A1. $p \supset (q \supset p)$;
A2. $[p \supset (q \supset r)] \supset [(p \supset q) \supset (p \supset r)]$;
A3. $[(p \supset \mathsf{0}) \supset \mathsf{0}] \supset p$;
A4. $\mathsf{A}x(p \supset q) \supset (p \supset \mathsf{A}xq)$, где $x$ не содержится свободно в $p$;
A5. $\mathsf{A}xp(x) \supset p(t)$.

Заметим, что обозначение, использованное в схеме A5, следует понимать в том смысле, что $p(x)$ есть некоторая формула, а $p(t)$ — формула, получающаяся из $p(x)$ в результате замены переменной $x$ термом $t$ во всех свободных вхождениях переменной $x$, причем никакое вхождение терма $t$ в формулу $p(t)$, являющееся таковым в результате этой замены, не содержит связанных вхождений никаких переменных.

Имеются два *правила вывода*. Первое из них, *Modus ponens* (MP), представляет собой тернарное отношение, имеющее место между двумя формулами, называемыми *посылками*, и третьей формулой, называемой *заключением*, тогда и только тогда, когда посылки имеют вид $p$ и $p \supset q$, а заключение есть $q$. Второе правило — *правило обобщения* (GN) — связывает единственную посылку с некоторым заключением тогда и только тогда, когда эта посылка имеет вид $p(x)$, а заключение — вид $\mathsf{A}yp(y)$. Мы будем схематически записывать эти правила следующим образом:

$$\frac{p \mid p \supset q}{q} \quad (\mathrm{MP}); \qquad \frac{p(x)}{\mathsf{A}yp(y)} \quad (\mathrm{GN}).$$

*Выводом* из множества $P$ формул как посылок некоторой формулы $q$ как заключения мы будем называть конечную последовательность $D=(d_1, \ldots, d_n)$ формул, такую, что каждая $d_i$ есть либо аксиома, либо принадлежит $P$, либо является заключением по какому-либо правилу вывода из одной из предшествующих в этой последовательности формул $d_j$, $d_h$ как посылок и такова, что $d_n$ есть $q$, причем если имеет место применение GN, то переменная $x$ не входит свободно ни в какую из формул, принадлежащих $P$. Запись $P \vdash q$ означает, что существует вывод формулы $q$ из $P$ (или из какого-нибудь подмножества множества $P$). [Замечание в скобках в предыдущей фразе преследует чисто технические цели: с его помощью мы избавляемся от искусственного ограничения на использование правила GN, которое иначе пришлось бы вводить, имея в виду, что все — кроме, быть может, конечного числа — переменные могут входить свободно в формулы, принадлежащие множеству $P$.]

*Доказательством* формулы $q$ называется вывод $q$ из пустого множества формул; отметим, что при этом определении сформулированное выше (при определении понятия вывода) ограничение на использование правила GN отпадает. В случае когда для формулы $q$ существует доказательство, мы будем называть $q$ *теоремой* и записывать это обстоятельство символически в виде $\vdash q$

Если $P \vdash \mathsf{O}$, мы будем называть множество формул $P$ *дедуктивно несовместным*, или *дедуктивно противоречивым*; в противном случае $P$ называется *дедуктивно совместным*, или *дедуктивно непротиворечивым*.

Сейчас мы приведем три простых следствия из аксиом и правил вывода. Мы могли бы их без всякого ущерба просто присоединить к списку аксиом и правил, но предпочитаем привести их доказательства в качестве иллюстраций данных нами определений понятий вывода и доказательства.

Т е о р е м а. *Для всех формул $p$ имеет место* $\vdash p \supset p$

Приведем схему доказательства $D = (d_1, \ldots, d_5)$ всех таких формул $p \supset p$; справа для каждой строки указано, каким именно образом эта строка удовлетворяет условиям, фигурирующим в определении понятия доказательства. Вот эта схема:

| | | |
|---|---|---|
| $d_1$ | $p \supset (p \supset p)$ | A1 |
| $d_2$ | $p \supset ((p \supset p) \supset p)$ | A1 |
| $d_3$ | $[p \supset ((p \supset p) \supset p)] \supset [(p \supset (p \supset p)) \supset (p \supset p)]$ | A2 |
| $d_4$ | $(p \supset (p \supset p)) \supset (p \supset p)$ | $d_2$, $d_3$, MP |
| $d_5$ | $p \supset p$ | $d_1$, $d_4$, MP |





Т е о р е м а. *Для любых формул $p$ и $q$ имеет место* $\vdash (q \supset \mathsf{O}) \supset (q \supset p)$.

Приводим доказательство:

| | | |
|---|---|---|
| $d_1$ | $((p \supset \mathsf{O}) \supset \mathsf{O}) \supset p$ | A3 |
| $d_2$ | $[((p \supset \mathsf{O}) \supset \mathsf{O} \supset p] \supset [\mathsf{O} \supset [((p \supset \mathsf{O}) \supset \mathsf{O}) \supset p]]$ | A1 |
| $d_3$ | $\mathsf{O} \supset [((p \supset \mathsf{O}) \supset \mathsf{O}) \supset p]$ | $d_1$, $d_2$, MP |
| $d_4$ | $[\mathsf{O} \supset [((p \supset \mathsf{O}) \supset \mathsf{O}) \supset p]] \supset [[\mathsf{O} \supset ((p \supset \mathsf{O}) \supset \mathsf{O})] \supset (\mathsf{O} \supset p)]$ | A2 |
| $d_5$ | $[\mathsf{O} \supset ((p \supset \mathsf{O}) \supset \mathsf{O})] \supset (\mathsf{O} \supset p)$ | $d_3$, $d_4$, MP |
| $d_6$ | $\mathsf{O} \supset ((p \supset \mathsf{O}) \supset \mathsf{O})$ | A1 |
| $d_7$ | $\mathsf{O} \supset p$ | $d_5$, $d_6$, MP |
| $d_8$ | $(\mathsf{O} \supset p) \supset (q \supset (\mathsf{O} \supset p))$ | A1 |
| $d_9$ | $q \supset (\mathsf{O} \supset p)$ | $d_7$, $d_8$, MP |
| $d_{10}$ | $(q \supset (\mathsf{O} \supset p)) \supset ((q \supset \mathsf{O}) \supset (q \supset p))$ | A2 |
| $d_{11}$ | $(q \supset \mathsf{O}) \supset (q \supset p)$ | $d_9$, $d_{10}$, MP |

Т е о р е м а. *Для всех формул $p$ имеет место*

$$\rightarrow \rightarrow \mathsf{A}x \rightarrow \rightarrow p \vdash \mathsf{A}xp.$$

Мы будем иногда пользоваться, кроме основных, и другими связками, определяя их в терминах $\mathsf{O}$, $\mathsf{J}$ и $\mathsf{A}$; например, $\rightarrow p$ мы будем писать в качестве сокращения для $p \supset \mathsf{O}$, а $\mathsf{E}xp$ — как сокращение для $\rightarrow \mathsf{A}x \rightarrow p$. В этих обозначениях вывод, о существовании которого говорится в утверждении этой теоремы, записывается в виде

$$\rightarrow \mathsf{E}x \rightarrow p \vdash \mathsf{A}xp.$$

Утверждение это следует из рассмотрения следующей схемы вывода:

| | | |
|---|---|---|
| $d_1$ | $\rightarrow \rightarrow \mathsf{A}x \rightarrow \rightarrow p$ | Посылка |
| $d_2$ | $(\rightarrow \rightarrow \mathsf{A}x \rightarrow \rightarrow p) \supset (\mathsf{A}x \rightarrow \rightarrow p)$ | A3 |
| $d_3$ | $\mathsf{A}x \rightarrow \rightarrow p$ | $d_1$, $d_2$, MP |
| $d_4$ | $\mathsf{A}x \rightarrow \rightarrow p \supset \rightarrow \rightarrow p$ | A5 |
| $d_5$ | $\rightarrow \rightarrow p$ | $d_3$, $d_4$, MP |
| $d_6$ | $\rightarrow \rightarrow p \supset p$ | A3 |
| $d_7$ | $p$ | $d_5$, $d_6$, MP |
| $d_8$ | $\mathsf{A}xp$ | $d_7$, GN |

Для обоснования последней строки вывода, заключающегося в ссылке на правило GN, существенно то обстоятельство, что переменная $x$ не входит свободно в единственную посылку нашего вывода — формулу $\to\to \mathsf{A}x \to \to p$.

Не совсем удобным является то обстоятельство, что если $D_1$ есть вывод $q$ из $P$, а $D_2$ — вывод $s$ из $\{q\} \cup R$, то последовательность $D$ формул, получающаяся приписыванием $D_2$ к $D_1$, не обязательно является выводом $s$ из $P \cup R$. Дело в том, что правило GN может применяться в $D_1$ (или в $D_2$) к некоторой переменной, входящей свободно в какую-нибудь из формул множества $\{q\} \cup R$ (соответственно множества $P$) и не входящей в то же время свободно ни в одну из формул множества $P$ (соответственно $\{q\} \cup R$). Тем не менее отношение $\vdash$ транзитивно в смысле, устанавливаемом следующей теоремой.

Теорема. *Если $P \vdash Q$ и $Q \cup R \vdash S$, то $P \cup R \vdash S$.*

Утверждение теоремы легко следует из того частного ее случая, когда $P$ и $R$ — конечные множества формул; что же касается множества $Q$, то оно в соответствии с определением вывода в любом случае состоит из одной формулы $q$, и, аналогично, $S$ состоит из единственной формулы $s$. Пусть теперь $D_1$ есть вывод $q$ из $P$, а $D_2$ — вывод $s$ из $\{q\} \cup R$. В конечное множество $P \cup \{q\} \cup R$ формул может входить свободно лишь конечное число переменных, поэтому множество $\mathsf{V}'$ остальных переменных бесконечно. Допустим теперь, что $D_1$ содержит некоторый вывод посредством GN некоторой формулы $\mathsf{A}yp(y)$ из $p(x)$, так что $x$ не входит свободно ни в какую из принадлежащих $P$ формул. Тогда некоторая подпоследовательность $E$ последовательности $D_1$, оканчивающаяся этим выводом, представляет собой вывод $\mathsf{A}yp(y)$ из $P$. Если мы теперь образуем из $E$ новую последовательность $E'$, заменяя каждое свободное вхождение переменной $x$ вхождением некоторой новой переменной $x'$ из $\mathsf{V}'$, и присоединим $E'$ к $D_1$, то получим вывод $D_1'$ формулы $q$ из $P$, наличие в котором формулы $\mathsf{A}yp(y)$ обосновывается ссылкой на применение правила GN к формуле $p(x')$, где $x'$ принадлежит множеству $\mathsf{V}'$.

Повторное применение этой конструкции приведет нас в конце концов к выводу $D_1''$ формулы $q$ из $P$, в котором правило GN применяется к формуле $\mathsf{A}yp(y)$ лишь для переменных $x$, принадлежащих множеству $\mathsf{V}'$. Аналогично мы можем преобразовать $D_2$ в некоторый вывод $D_2''$, обладающий тем свойством, что GN применяется в нем к формулам $p(x)$ только для переменных $x$, не входящих свободно в множество $P \cup \{q\} \cup R$. Если мы теперь припишем $D_2''$ вслед за $D_1''$, то получим некоторую последовательность $D_2''$, все применения в которой правила GN будут удовлетворять ограничению, фигурирующему в определении вывода, так что $D''$ будет представлять собой вывод $s$ из $P$, что и требовалось.

## Упражнения

1. Покажите на примере, что произведение $D$ двух выводов $D_1$ и $D_2$, удовлетворяющих предположениям, сформулированным в ходе доказательства предыдущей теоремы, не обязательно являются выводом.

2. Завершите доказательство теоремы, показав, что ее утверждение для общего случая следует из частного случая, разобранного в приведенном выше доказательстве.

Еще одно замечание того же рода, которым мы воспользуемся ниже, состоит в том, что если $P$ есть множество формул, записанных на языке $L$, $q$ — формула, записанная на том же языке, а $L'$ — язык, получающийся в результате расширения $L$ за счет присоединения некоторых новых символов, то отношение $P \vdash q$ имеет место относительно $L$ тогда и только тогда, когда оно имеет место относительно $L'$. Это замечание представляет собой простой шаг в направлении к более глубокой теореме Крэйга, о которой мы поговорим позднее.

Отметим также, что поскольку вопросы о том, является ли некоторая данная формула аксиомой и следует ли данная формула из других данных формул по какому-либо правилу вывода, очевидным образом разрешимы, то разрешимым оказывается и вопрос, является ли некоторая данная последовательность формул выводом данной формулы $q$ из данного множества $P$ формул.

### Упражнения

1. Докажите первое из только что высказанных утверждений.

2. Дайте точное описание метода, позволяющего по произвольно заданным множеству $P$ формул, формуле $q$ и последовательности $p_1, \ldots, p_n$ формул определить, является ли эта последовательность выводом $q$ из $P$.

## Оправданность аксиоматизации

Теорема. *Если $P \vdash q$, то $P \models q$.*

Эта теорема утверждает попросту, что мы не были слишком щедры в выборе аксиом и правил вывода; ее доказательство, к которому мы обратимся чуть ниже, не сложно. Обратное же утверждение — о том, что мы при этом выборе не проявили излишней скромности, — далеко не так очевидно, и доказательство его, которое мы дадим позднее, представляет значительно бо́льшие трудности.

Чтобы доказать высказанное утверждение посредством индукции по длине формулы, мы должны доказать два следующих утверждения: во-первых, что каждая аксиома истинна и, во-вторых, что если посылки вывода по одному из правил в каком-либо выводе из некоторой совокупности $P$ формул являются семантическими следствиями из $P$, то и заключение есть семантическое следствие из $P$.

Непосредственно очевидна истинность любой аксиомы, получающейся по одной из схем A1, A2, A3.

Обращаясь к схеме A4, мы должны доказать, что если $\varphi$ есть произвольная интерпретация, а $x$ — переменная, не входящая свободно в $p$, то $\varphi[\mathsf{A}x(p\supset q)]=1$





влечет $\varphi[p\supset \mathsf{A}xq]=1$. Иными словами, предполагая $\varphi[\mathsf{A}x(p\supset q)]=1$ и $\varphi p=1$, мы должны показать, что $\varphi\mathsf{A}xq=1$. Пусть $\varphi'$ — произвольная интерпретация, совпадающая с $\varphi$ на множестве $\mathsf{V}\cup\mathsf{R}\cup\mathsf{F}$, за исключением, быть может, $x$; тогда мы должны показать, что $\varphi'q=1$. Из $\varphi[\mathsf{A}x(p\supset q)]=1$ мы получаем $\varphi'(p\supset q)=1$. Так как $x$ не входит свободно в $p$, то $\varphi'p=\varphi p$; поэтому из $\varphi p=1$ следует $\varphi'p=1$. Но теперь из $\varphi'(p\supset q)=1$ и $\varphi'p=1$ мы получаем $\varphi'q=1$.

Рассмотрим теперь A5. Из $\varphi[\mathsf{A}xp(x)]=1$ мы должны вывести $\varphi p(t)=1$. Существует интерпретация $\varphi'$, совпадающая с $\varphi$ на множестве $\mathsf{V}\cup\mathsf{F}\cup\mathsf{R}$, за исключением, быть может, $x$, где $\varphi'x=\varphi t$. По доказанной ранее теореме о подстановке $\varphi'p(x)=\varphi p(t)$. Но $\varphi\mathsf{A}xp(x)=1$ влечет $\varphi'p(x)=1$, откуда $\varphi p(t)=1$.

Рассмотрение *Modus ponens* не представляет трудностей. Если $\varphi p=1$ и $\varphi(p\supset q)=1$ для любой интерпретации $\varphi$, такой, что $\varphi P=1$, то $\varphi q=1$ для любой такой $\varphi$.

Обращаясь к правилу обобщения, предположим, что $P\models p(x)$, где $x$ не входит свободно ни в одну из формул, принадлежащих $P$. Мы должны показать, что $\varphi P=1$ влечет $\varphi\mathsf{A}yp(y)=1$. Пусть интерпретация $\varphi'$ совпадает с $\varphi$ на $\mathsf{V}\cup\mathsf{F}\cup\mathsf{R}$, за исключением, быть может, $x$. Так как $x$ не входит свободно ни в одну из составляющих $P$ формул, то $\varphi'P=\varphi P=1$ и $\varphi'p(x)=1$. Отсюда видно, что $\varphi\mathsf{A}xp(x)=1$ и, согласно теореме о подстановке, $\varphi\mathsf{A}yp(y)=\varphi\mathsf{A}xp(x)=1$.

Следствие. *Любая теорема истинна: если $\vdash p$, то $\models p$.*

Следствие. *Если множество формул имеет модель, то оно дедуктивно непротиворечиво.*

### Упражнение

Постройте примеры, показывающие, что условие на переменную $x$ в A4 и условие на $x$ в применении правила GN в выводе нельзя опустить.

## Теорема дедукции

Теорема дедукции представляет собой первый серьезный шаг, приближающий нас к доказательству адекватности выбранной аксиоматизации. Связка $\supset$ была определена выше таким образом, что $\models p \supset q$ оказалось равносильно $p \models q$. Мы хотим теперь получить дедуктивный аналог этого факта — доказать, что $\vdash p \supset q$ равносильно $p \vdash q$. Половина сказанного составляет содержание правила *Modus ponens*: если $\vdash p \supset q$, то $p \vdash q$. Вторая половина, т. е. то, что из $p \vdash q$ следует $\vdash p \supset q$, и составляет основное содержание теоремы дедукции.

Теорема дедукции. *Пусть $P$ — множество формул, а $q$ и $r$ — формулы. Тогда $P \vdash q \supset r$ тогда и только тогда, когда $P, q \vdash r$.*

То, что $P \vdash q \supset r$ влечет $P, q \vdash r$, непосредственно следует из правила MP и транзитивности импликации. Из данного вывода $q \supset r$ из $P$ мы получаем вывод $r$ из $P \cup \{q\}$, добавляя к исходному выводу две заключительные строки $q$ и $r$ и обосновывая включение первой из них в вывод тем, что она посылка, а второй — тем, что она является заключением по MP из двух предшествующих строк вывода: $q \supset r$ и $q$.

Чтобы доказать обратное утверждение, предположим, что имеется вывод $D = (d_1, \ldots, d_n)$ формулы $d_n = r$ из $P \cup \{q\}$. Пусть $D'$ — последовательность $(d'_1, \ldots, d'_n)$, где каждая формула $d'_i = q \supset d_i$ и, в частности, $d'_n = q \supset r$. Определенная таким образом последовательность $D'$ не является еще непременно выводом формулы $q \supset r$ из посылок $P$, но мы покажем, как преобразовать ее в такой вывод посредством вставки дополнительных строк перед каждой формулой $d'_i$. Чтобы провести доказательство по индукции, мы допустим, что нам уже удалось проделать такую процедуру для последовательности $d'_1, \ldots, d'_{i-1}$. Разберем теперь различные возможные случаи.





Случай 1. Если $d_i = q$, то $d'_i = q \supset q$; такая формула является, как было показано выше, теоремой, и ее доказательство можно вставить в $D'$ перед ней.

Случай 2. Если $d_i$ есть аксиома или одна из формул, принадлежащих $P$, мы вставляем перед ней в $D'$ две строки: $e = d_i$ и $f = d_i \supset (q \supset d_i)$. Теперь $e$ обосновывается ссылкой на то, что она является аксиомой или членом $P$, $f$ есть аксиома, получающаяся по схеме A2, а $d'_i = q \supset d_i$ следует из $e$ и $f$ по правилу MP.

Случай 3. Пусть формула $d_i$ следует из двух предшествующих ей в выводе строк $d_j$ и $d_k = d_j \supset d_i$ по правилу MP. В этом случае перед $d_i$ вставляется две строки: $e = d'_k \supset (d'_j \supset d'_i)$ и $f = d'_j \supset d'_i$. Тогда

$$e = [q \supset (d_j \supset d_i)] \supset [(q \supset d_j) \supset (q \supset d_i)]$$

есть такая аксиома, получающаяся по схеме A2, а $f$ следует из $d'_k$ и $e$ по MP. Наконец, $d'_i$ следует из $d'_j$ и $f$ по MP.

Случай 4. Пусть $d_i$ следует из некоторой более ранней строки $d_j$ вывода по правилу GN, т. е. $d_j = p(x)$ и $d_i = \mathsf{A}y\,p(y)$, где $x$ не входит свободно ни в одну из формул множества $P \cup \{q\}$. Вставляем перед $d_i$ две строки: $e = \mathsf{A}y(q \supset p(y))$ и $f = \mathsf{A}y(q \supset p(y)) \supset (q \supset \mathsf{A}y\,p(y))$. Тогда $e$ следует из $d'_j = q \supset p(x)$ по GN, так как $x$ не входит свободно в $P \cup \{q\}$, а $f$ получается по схеме A5 (при условии, что $y$ не входит свободно в $q$), а из $e$ и $f$ по MP следует $d'_i = q \supset \mathsf{A}x\,p(x)$. [Если же $y$ входит свободно в $q$, то мы можем доказать $q \supset \mathsf{A}z\,p(z)$ для некоторой новой переменной $z$, после чего, уже доказав предварительно $\mathsf{A}z\,p(z) \supset \mathsf{A}y\,p(y)$, мы легко получаем $d'_i$.]

### Упражнения

1. Восстановите подробности, опущенные в конце доказательства для случая 4.

2. Ценой незначительных усложнений в определениях формулы и интерпретации удается достичь некоторых преимуществ

в аксиоматизации, пользуясь двумя разными множествами символов для связанных и для свободных переменных; никаких существенных усложнений в разборе случая 4 теоремы дедукции при этом не возникает. Укажите, каким именно образом придется видоизменить при этом ход рассуждений.

## Теорема о непротиворечивости

Мы увидим позднее, что следующая теорема, которую мы назовем теоремой о непротиворечивости, есть по сути дела просто некоторая переформулировка теоремы адекватности.

Теорема о непротиворечивости. *Множество формул дедуктивно непротиворечиво тогда и только тогда, когда оно имеет модель.*

Первое утверждение этой теоремы уже доказано в качестве следствия из теоремы об оправданности аксиоматизации. Остается, таким образом, по любому данному (дедуктивно) непротиворечивому множеству $P$ формул языка $L$ найти такую интерпретацию $\varphi$, что $\varphi P=1$. При построении интерпретации мы должны обходиться имеющимися у нас в наличии выразительными средствами, т. е. языком $L$ и множеством $P$ формул. В общих словах, элементами структуры должны служить термы языка $L$, функциями — операции алгебры термов, а отношения на структуре должны быть определены таким образом, чтобы им соответствовали формулы из множества $P$. Такое построение интерпретации для языка $L$ средствами самого этого языка до некоторой степени напоминает представление некоторой абстрактной группы посредством подстановок, определенных на области, состоящей в точности из тех же элементов, что и исходная группа.

При выполнении этой задачи мы можем столкнуться с двумя трудностями. Прежде всего, множество термов языка $L$ может оказаться просто слишком малым, чтобы из него можно было выделить множество всех термов, образующих область такой интерпретации $\varphi$, что $\varphi P=1$. Может, например, оказаться, что $\mathsf{E}xp(x)$ принадлежит $P$, хотя $\rightharpoondown p(t)$ для любого терма $t$ из $L$ также принадлежит $P$. Чтобы преодолеть эту трудность, мы расширим язык $L$, присоединив к нему новые термы. Затем само множество $P$ формул может оказаться недостаточным для описания нужной нам структуры, связанной с множеством термов. Вполне может, например, случиться так, что для некоторой атомарной формулы $p$ ни сама $p$, ни $\rightharpoondown p$ не принадлежат $P$. Чтобы преодолеть это препятствие, приходится расширять $P$ до некоторого охватывающего его множества, также непротиворечивого. Ниже мы покажем, как конкретно преодолеваются обе эти трудности в отдельности, а затем и обе сразу. После этого мы сможем спокойно приступить к построению интерпретации $\varphi$.

Перейдем теперь к доказательству теоремы. Рассмотрим два условия, относящихся к множеству $P$ формул языка $L$:

(1) для каждой формулы $p$ из $L$ имеет место либо $p$, либо $\rightharpoondown p$, но не то и другое одновременно;
(2) если формула $\mathsf{E}xp(x)$ принадлежит $P$, то в $L$ найдется такой терм $t$, что $p(t)$ также принадлежит $P$.

Лемма. *Каждое непротиворечивое множество $P$ формул языка $L$ содержится в некотором непротиворечивом множестве $P'$ формул языка $L$, удовлетворяющем условию* (1).

Мы будем исходить из предположения, что множество всех формул языка $L$ вполне упорядочено, свободно пользуясь в случае надобности аксиомой выбора или же явным образом постулируя лемму Цорна, эквивалентную аксиоме выбора:

*Пусть $F$ есть система подмножеств $Q$ некоторого множества $S$, обладающая тем свойством, что если $G\subseteq F$ есть цепь, — т. е. для любых множеств $Q_1$ и $Q_2$ из $G$ имеет место $Q_1\subseteq Q_2$ или $Q_2\subseteq Q_1$, — то объединение всех множеств $Q$ из $G$ принадлежит $F$. Тогда в $F$ имеется максимальный элемент, т. е. такой элемент $M$, что $M\subseteq Q$ влечет $M=Q$ для произвольного множества $Q$ из $F$.*

Чтобы воспользоваться леммой Цорна, мы в качестве $F$ возьмем систему всех непротиворечивых множеств $Q$ формул языка $L$, таких, что $P \subseteq Q$. Объединение $U$ множеств из любой цепи $G \subseteq F$ содержит, очевидно, множество $P$. Покажем, что $U$ непротиворечиво. Если бы $U$ было противоречивым, — т. е. если бы было $U \vdash 0$, — то для некоторого конечного множества формул $p_1, \ldots, p_n$ из $U$ имело бы место $p_1, \ldots, p_n \vdash 0$. Так как $U$ есть объединение множеств $Q$ из $G$, то каждая $p_i$ принадлежит некоторому $Q_i$ из $G$; так как $G$ есть цепь, то некоторое из этих $Q_i (1 \leqslant i \leqslant n)$ содержит все остальные $Q_j$ $(1 \leqslant j \leqslant n,\ j \neq i)$; поэтому все $p_1, \ldots, p_n$ принадлежат этому $Q_i$. Но тогда $Q_i \vdash 0$ вопреки предположению о непротиворечивости всех $Q$ из $F$. Мы показали, таким образом, что $U$ принадлежит $G$, так что условие леммы Цорна выполнено. Следовательно, $F$ содержит максимальное множество $P'$.

Чтобы доказать теперь (1), допустим существование такой формулы $p$, что ни $p$, ни $\neg p$ не принадлежат $P'$. Так как $P'$ есть максимальное из непротиворечивых множеств, содержащих $P$, мы заключаем, что $P' \cup \{p\} \vdash 0$ и $P' \cup \{\neg p\} \vdash 0$. По теореме дедукции $P' \vdash \neg p$ и $P' \vdash \neg\neg p$. Но из $\neg p = p \supset 0$ и $\neg\neg p = (p \supset 0) \supset 0$ мы по правилу MP получим $0$, откуда $P' \vdash 0$ вопреки предположению.

Под расширением $L'$ языка $L$ ниже понимается язык, отличающийся от $L$ лишь тем, что он имеет, быть может, более широкое множество переменных.

Лемма. *Каково бы ни было непротиворечивое множество $P$ формул языка $L$, существует непротиворечивое множество $P'$ формул расширения $L'$ языка $L$, содержащее $P$ и такое, что для любой формулы вида $\mathsf{E}xq(x)$ из $P$ найдется некоторая формула $q(t)$ в $P'$.*

Для каждой формулы $p = \mathsf{E}xq(x)$ из $P$ мы присоединим к $L$ новую перменную $v_p$, а к $P$ — новую формулу $q(v_p)$. Такая процедура приводит, очевидно, к некоторому множеству $P'$ формул языка $L'$, такому, что $P \subseteq P'$ и что для любой формулы $\mathsf{E}xq(x)$ из $P$ в $P'$





найдется некоторая формула $q(v)$. Заметим, что для доказательства непротиворечивости $P'$ достаточно рассмотреть случай конечного числа присоединенных формул, а следовательно, случай, когда присоединяется лишь одна-единственная формула. Нам нужно показать, что если $P$ непротиворечиво, $\mathsf{E}xq(x)$ принадлежит $P$, а $v$ не входит в $P$, то множество $P \cup \{q(v)\}$ также непротиворечиво.

Допустим, что $P, q(v) \vdash 0$. Тогда по теореме дедукции $P \vdash \neg q(v)$. Так как $v$ не входит в $P$, по правилу GN мы получаем $P \vdash \mathsf{A}x \neg q(x)$. Но $P$ содержит $\mathsf{E}xq(x)$, т. е. $\neg \mathsf{A}x \neg q(x) = (\mathsf{A}x \neg q(x)) \supset 0$. По MP мы получаем отсюда $P \vdash 0$, что противоречит сделанному предположению.

Лемма. *Каково бы ни было непротиворечивое множество $P$ формул языка $L$, существует непротиворечивое множество $P'$ формул некоторого расширения $L'$ языка $L$, содержащее $P$, причем $P'$ и $L'$ удовлетворяют условиям* (1) *и* (2).

Построим следующим образом последовательность языков $L_1, L_2, \ldots$ и последовательность множеств формул $P_1, Q_1, P_2, Q_2, \ldots$. Начнем с $L_1 = L$ и $P_1 = P$. Пусть теперь нам дано непротиворечивое множество $P_n$ формул языка $L_n$. По первой лемме найдется множество $Q_n$ формул языка $L_n$, непротиворечивое, содержащее $P_n$ и удовлетворяющее условию (1). По второй лемме найдутся расширение $L_{n+1}$ языка $L_n$ и непротиворечивое множество $P_{n+1}$ формул языка $L_{n+1}$, содержащее $Q_n$ и такое, что для любой формулы вида $\mathsf{E}xq(x)$ из $P_n$ в $P_{n+1}$ найдется некоторая формула $q(t)$. Обозначим теперь через $L'$ язык, символами которого служат символы всех $L_n$, а через $P'$ — множество формул этого языка $L'$, являющееся объединением всех множеств $P_n$.

Очевидно, что $P'$ содержит $P$ и, как объединение цепи непротиворечивых множеств, непротиворечиво. Пусть $p$ есть произвольная формула языка $L'$; тогда $p$ является формулой какого-то из языков $L_n$ и, поскольку $P_n$ удовлетворяет условию (1), либо $p$, либо $\neg p$ принадлежит $P_n$. Но в таком случае либо $p$, либо

$\rightarrow p$ принадлежит множеству $P'$. Значит, множество $P'$ и язык $L'$ удовлетворяют условию (1). Если $p = \mathbf{E} xq(x)$ принадлежит $P'$, то она принадлежит некоторому $P_n$. Значит, для некоторого $v$ из $L_{n+1}$ формула $q(v)$ принадлежит $Q_{n+1}$. Но тогда для некоторого $v$ из $L'$ формула $q(v)$ принадлежит $P_{n+1}$, а, значит, и $L'$, и условие (2) выполнено.

Чтобы завершить доказательство теоремы о непротиворечивости, нам теперь нужно указать такую интерпретацию $\varphi$ языка $L$, что $\varphi P = 1$. Очевидно, что мы можем заменить $P$ и $L$ соответственно на некоторые $P'$ и $L'$, фигурирующие в формулировке предыдущей леммы, и, следовательно, считать выполненными условия (1) и (2).

В качестве области интерпретации $\varphi$ мы возьмем множество $T$ всех термов языка $L$. Если $f$ — функциональный символ ранга $n$, то мы определим функцию $\varphi f$, полагая

$$(\varphi f)(t_1, \ldots, t_n) = ft_1 \ldots t_n$$

для любых $t_1, \ldots, t_n$ из $T$. Если $x$ принадлежит $V$, мы положим по определению $\varphi x = x$. Теперь по индукции получаем, что $\varphi t = t$ для всех $t$ из $T$. Если $r$ — символ отношения ранга $n$, то мы определим функцию $\varphi r$, положив $(\varphi r)(t_1, \ldots, t_n) = 1$ тогда и только тогда, когда $rt_1 \ldots t_n$ принадлежит $P$. Этим завершается определение $\varphi$, и остается только показать, что $\varphi P = 1$.

Покажем посредством индукции по числу связок в формуле $p$, что $\varphi p = 1$ тогда и только тогда, когда $p \in P$. Это утверждение непосредственно следует из определения интерпретации, если $p$ — атомарная формула, и тривиально, если $p$ есть $\mathbf{O}$. Пусть $p = q \supset r$. Допустим сначала, что $\varphi p = 1$; тогда $\varphi q = 0$ или $\varphi r = 1$. По предположению индукции $\varphi q = 0$ влечет, что $q$ не принадлежит $P$, так что в силу условия (1) $\rightarrow q \in P$. Мы видели ранее, что $(q \supset \mathbf{O}) \vdash (q \supset r)$, т. е. $\rightarrow q \vdash (q \supset r)$; поэтому из $\rightarrow q \in P$ мы получаем $P \vdash q \supset r$. Как и ранее, из этого следует, что $\rightarrow (q \supset r)$ не принадлежит $P$, а значит, $(q \supset r) \in P$. Если $\varphi r = 1$, то мы, рассуждая точно так же, получим, что $r \in P$, и в силу $r \vdash (q \supset r)$, что $P \vdash q \supset r$ и $(q \supset r) \in P$. В любом случае оказывается, что $p$ принадлежит $P$. Для доказательства обратного утверждения предположим, что $p \in P$. Из $\varphi q = 1$ мы должны получить $\varphi r = 1$, т. е. из $q \in P$ получить $r \in P$. По МР $(q \supset r) \in P$ и $q \in P$ дает $P \vdash r$, откуда $r \in P$.

Остается рассмотреть случай $p = \mathbf{A} xq(x)$. Допустим сначала, что $p$ не принадлежит $P$. Мы видели, что $\rightarrow \mathbf{E} x \rightarrow q(x) \vdash \mathbf{A} xq(x)$, из чего вытекает, что $\rightarrow \mathbf{E} x \rightarrow q(x)$ не принадлежит $P$, а, значит, в силу условия (1) $\mathbf{E} x \rightarrow q(x) \in P$. В силу (2) отсюда следует, что $\rightarrow q(t) \in P$ для некоторого $t$, из чего в свою очередь в силу (1) вытекает, что $q(t) \notin P$. По предположению индукции отсюда следует, что $\varphi q(t) = 0$, откуда уже наконец получаем $\varphi p = \varphi \mathbf{A} xq(x) = 0$, что и требовалось.

Предположим теперь, что $p = \mathbf{A} xq(x)$ и $\varphi p = 0$. Тогда для некоторой интерпретации $\varphi'$, совпадающей с $\varphi$ на множестве $\mathbf{V} \cup \mathbf{F} \cup \mathbf{R}$ — за исключением, быть может, $x$, — имеем $\varphi' q(x) = 0$. Значит, $\varphi' x = t$ — элемент множества $T$. Пусть $q'(x)$ получается из $q(x)$ посредством такого переименования связанных переменных, что в результате в $q'(x)$ не входит связанно никакая переменная, входящая в $t$; в таком случае мы можем, подставив $t$ вместо $x$ в эту формулу, получить $q'(t)$. Так как $\varphi'$ совпадает с $\varphi$, за исключением, быть может, их значения для $x$, а $\varphi'(x) = t = \varphi t$, то в силу теоремы о подстановке $\varphi' q'(x) = \varphi q'(t)$. Теперь уже совсем просто показать, что $\varphi' q'(x) = \varphi' q(x)$, а также что $\mathbf{A} xq(x) \vdash \mathbf{A} xq'(x)$. Из первого равенства мы получаем $\varphi' q'(x) = \varphi' q(x) = 0$, откуда $\varphi q'(t) = 0$ и в силу предположения индукции $q'(t) \notin P$. Из второй выводимости с помощью схемы аксиом A5 и правила МР мы получаем $\mathbf{A} xp(x) \vdash q'(t)$. Так как $q'(t) \notin P$, то в силу условия (1) $\mathbf{A} xq(x)$ также не принадлежит $P$, что и требовалось доказать.

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 рассмотрений показать, что в данной теории нельзя доказать, скажем, формулу $\mathbf{0}$. Область применимости этого метода, однако, также невелика. Мы увидим ниже, что 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 сколько-либо сложных математических теорий базируется в конечном счете на интуиции и опыте.

## Теорема адекватности и теорема компактности

Теорема адекватности. *$P\vdash q$ равносильно $P\models q$ для произвольного множества $P$ формул и любой формулы $q$.*

Взяв $\mathbf{0}$ в качестве $q$, мы получим теорему о непротиворечивости. Для доказательства теоремы адекватности нам в силу теоремы об оправданности аксиоматизации достаточно показать, что $P\models q$ влечет $P\vdash q$. Из предположения $P\models q$ немедленно следует $P, \rightarrow p\models \mathbf{0}$, откуда по теореме о непротиворечивости в свою очередь следует $P, \rightarrow q\vdash \mathbf{0}$. Отсюда по теореме дедукции получаем $P\vdash \rightarrow\rightarrow q$. Теперь с помощью аксиомы $((q\supset \mathbf{0})\supset \mathbf{0})\supset q$, т. е. $\rightarrow\rightarrow q\supset q$, и MP мы получаем $P\vdash q$.

Нам уже приходилось пользоваться тривиальным соображением, непосредственно вытекающим из определения понятия вывода, что $P\vdash q$ равносильно $P_0\vdash q$, где $P_0$ — некоторое конечное подмножество множества $P$ формул. Теорема адекватности позволяет получить из этого тривиального соображения теорему семантического содержания, уже отнюдь не столь очевидную.

Теорема компактности. *Если $P\models q$, то для некоторого конечного подмножества $P_0$ множества $P$ $P_0\models q$.*

Следствие. *Множество $P$ имеет модель в том и только том случае, когда каждое его конечное подмножество имеет модель.*

Термин «компактность» заимствован из топологии; выбор его мотивируется достаточно прозрачными аналогиями. Пусть $E$ — множество всех интерпретаций языка $L$. [Предполагается, что область каждой из этих интерпретаций является подмножеством некоторого фиксированного достаточно обширного множества.] Подмножество $U$ множества $E$ называется *замкнутым*, если для некоторого множества $P$ формул $\varphi\in U$ тогда и только тогда, когда $\varphi P=1$. Множество $E$ вместе с системой всех своих замкнутых подмножеств образует *топологическое пространство*. Пространство $E$ называется *компактным*, если оно обладает по отношению к замкнутым множествам свойством конечного пересечения: если $F$ есть произвольная совокупность замкнутых множеств, такая, что пересечение любого конечного числа членов этой совокупности непусто, то пересечение всех множеств из $F$

также непусто. Теперь видно, что теорема компактности — точнее, ее следствие, которое, как легко видеть, эквивалентно самой теореме, — утверждает, что пространство $E$ интерпретаций компактно.

Совсем недавно мы убедились, что в теории равенства нет такого предложения, которое выполнялось бы на всех конечных структурах, и притом только на них. Из теоремы компактности аналогичный результат довольно легко получается и для других теорий. Пусть, например, $T$ есть теория групп с символами для равенства и группового умножения, и пусть предложение $q$ верно для всех бесконечных групп. Тогда верно, что $P \models q$, где $P$ состоит из предложений $p_2$, $p_3, \ldots$, а каждое $p_n$ утверждает существование по крайней мере $n$ элементов. Из теоремы компактности следует, что в таком случае $q$ следует из некоторого конечного подмножества $P_0$ множества $P$, а поэтому $p_n \models q$ для некоторого $n$. Таким образом, предложение, истинное для всех бесконечных групп, оказывается истинным и для всех конечных групп достаточно большого порядка.

### Упражнения

1. Исследуйте более детально множество $E$ как топологическое пространство.

2. Если $E$ есть пространство всех интерпретаций, а $F$ — множество всех формул языка $L$, то между множеством $S(E)$ всех подмножеств множества $E$ и множеством $S(F)$ всех подмножеств множества $F$ можно установить два соответствия: если $U \subseteq E$, то $\alpha U$ по определению есть множество всех таких $p$ из $F$, что $\varphi p = 1$ для всех $\varphi$ из $U$; если $V \subseteq F$, то $\beta V$ по определению есть множество всех таких $\varphi$ из $E$, что $\varphi p = 1$ для всех $p$ из $V$. Как связаны между собой эти два отображения? В частности, как $\beta\alpha U$ относится к $U$, а $\alpha\beta V$ — к $V$? Что означают равенства $\beta\alpha U = U$ и $\alpha\beta V = V$? Что можно сказать о $\alpha\beta\alpha U$? о $\beta\alpha\beta V$?

3. Будем исходить из допущения, что каждый не равный константе многочлен с коэффициентами из некоторого данного поля имеет корень из некоторого более обширного поля. С помощью теоремы компактности докажите, что существует некоторое поле содержащее рациональные числа и такое, что любой непостоянный многочлен с рациональными коэффициентами имеет корень, принадлежащий этому полю.





4. Найдите другие применения теоремы компактности к известным математическим проблемам. [По поводу этой проблематики и связанного с ней круга идей см. упомянутую в списке литературы книгу А. Робинсона.]

## Логика предикатов с равенством

Обозначим через $=$ один из символов бинарных отношений языка $L$ и будем пользоваться вместо обозначения $=ts$ обычной записью $t = s$. Пусть $I_0$ есть множество всех *собственных интерпретаций* $\varphi$, т. е. таких интерпретаций, при которых $=$ интерпретируется как обычное равенство на области интерпретации $\varphi$; иными словами, для собственной интерпретации $\varphi$ запись $\varphi(t = s) = 1$ равносильна $\varphi t = \varphi s$. Мы будем говорить, что множество $P$ формул *собственно влечет* формулу $q$, и писать $P \models_{I_0} q$, если $\varphi P = 1$ влечет $\varphi q = 1$ для всех $\varphi$ из $I_0$. Если $\models_{I_0} q$, то мы будем называть формулу $q$ *собственно истинной*; мы будем также говорить, что множество формул $P$ *собственно противоречиво*, если $P \models_{I_0} 0$, и что $P$ *собственно непротиворечиво* в противном случае. Нам предстоит аксиоматизировать теорию $T_{I_0}$ всех собственно истинных формул.

Добавим в качестве аксиом к множеству $A$ аксиом все формулы, получающиеся по следующим схемам (множество всех таких формул мы будем обозначать через $I$):

I1. $t = t$;

I2. $t = s \supset s = t$;

I3. $t = s \wedge s = u \supset t = u$;

I4. $t_i = t_i' \supset f t_1 \ldots t_{i-1} t_i t_{i+1} \ldots t_n = f t_1 \ldots t_{i-1} t_i' t_{i+1} \ldots t_n$ для любого $f$ из $\mathsf{F}_n$ и любого $i$, $1 \leqslant i \leqslant n$;

I5. $t_i = t_i' \supset (r t_1 \ldots t_{i-1} t_i t_{i+1} \ldots t_n \supset r t_1 \ldots t_{i-1} t_i' t_{i+1} \ldots t_n)$ для любого $r$ из $\mathsf{R}_n$ и любого $i$, $1 \leqslant i \leqslant n$.

Упражнение

Покажите, что без аксиом I2 и I3 в этом списке можно обойтись (т. е. получить их из остальных аксиом).

Правила вывода остаются прежними, а отношение $P \vdash_{I_0} q$ определяется в точности так же, как $P \vdash q$, только с множеством $A \cup I$ аксиом вместо $A$. Очевидно, что $P \vdash_{I_0} q$ равносильно $P \cup I \vdash q$.

Теорема адекватности для логики предикатов с равенством. *Для любого множества $P$ формул и любой формулы $q$ $P \vdash_{I_0} q$ равносильно $P \models_{I_0} q$.*

Легко видеть, что аксиомы множества $I$ являются собственно истинными, так что $P \vdash_{I_0} q$ влечет $P \models_{I_0} q$. Чтобы доказать обратное утверждение, надо показать, что если множество $P$ собственно непротиворечиво, то оно имеет собственную модель. Допустим, что $P$ собственно непротиворечиво. Тогда $P \cup I$ непротиворечиво и по теореме о непротиворечивости имеет модель (в обычном смысле) $\varphi$, областью которой служит некоторое множество $A$. Из равенства $\varphi I = 1$ мы заключаем, что $\varphi(=)$ есть некоторое отношение эквивалентности $\equiv$ на $A$ и что это отношение подстановочно относительно всех функций $\varphi f$ и отношений $\varphi r$ на $A$. Отсюда следует, что на фактормножестве $[A]$ множества $A$ по отношению $\equiv$ существуют однозначно определенные функции $\psi f$ и отношения $\psi r$, такие, что, каковы бы ни были $a_1, \ldots, a_n \in A$, для всех $f$ из $\mathsf{F}_n$

$$(\psi f)([a_1], \ldots, [a_n]) = [(\varphi f)(a_1, \ldots, a_n)]$$

и для всех $r$ из $\mathsf{R}_n$

$$(\psi r)([a_1], \ldots, [a_n]) = (\varphi r)(a_1, \ldots, a_n).$$

Определим теперь новую интерпретацию $\psi$ с областью $[A]$, полагая $\psi x = [\varphi x]$ для $x \in \mathsf{V}$, а $\psi f$ для $f \in \mathsf{F}$ и $\psi r$ для $r \in \mathsf{R}$ — как выше. Из определения $\psi f$ следует по индукции, что $\psi t = [\varphi t]$ для всех термов $t$. Из определения $\psi r$ сразу вытекает, что $\psi p = \varphi p$ для атомарных формул $p$, а затем по индукции, что и $\psi p = \varphi p$ для произвольных $p$. В частности, мы получаем, что $\psi P = \varphi P = 1$, откуда следует, что $\psi$ есть модель множества $P$.





Остается показать, что $\psi$ есть собственная интерпретация. Пусть $\psi(t=s) = 1$. Тогда и $\varphi(t=s) = 1$, из чего видно, что $\varphi t$ и $\varphi s$ находятся в отношении $\varphi(=)$, т. е. $\varphi t \equiv \varphi s$. Но в таком случае $\varphi t$ и $\varphi s$ входят в один и тот же класс эквивалентности: $[\varphi t] = [\varphi s]$. Так как $\psi t = [\varphi t]$ и $\psi s = [\varphi s]$, то $\psi t = \psi s$. Из всего сказанного видно, что интерпретация $\psi(=)$ отношения $=$ при интерпретации $\psi$ есть равенство на $[A]$, из чего и следует, что $\psi$ — собственная интерпретация, а значит, и собственная модель.

## Теорема Лёвенгейма — Сколема

Теорема. *Пусть $P$ — множество формул языка $L$ с символом равенства, и пусть $n$ — мощность множества входящих в $P$ символов. Если $P$ имеет бесконечную собственную модель, а $m$ есть произвольная бесконечная мощность, $m \geqslant n$, то $P$ имеет и собственную модель мощности $m$.*

Доказательство этой теоремы извлекается из внимательного рассмотрения доказательства теоремы о непротиворечивости. Начнем с того, что исключим из языка $L$ все не входящие в $P$ символы, кроме связок и символа $=$, после чего добавим к нему бесконечное множество $M$ новых переменных, имеющее мощность $m$. Так как $n \leqslant m$, то мощность множества всех символов $L$ будет теперь равна $m$, и такую же мощность будет иметь множество формул. Теперь мы образуем множество $P'$, присоединив к $P$ множество $I$ аксиом для равенства, а также все формулы $x \neq y$, где $x$ и $y$ — различные переменные из $M$. Если бы $P'$ оказалось противоречивым, то противоречивым было бы также множество $P \cup I$, пополненное некоторым конечным множеством формул $x \neq y$. Легко видеть, однако, что моделью такого множества может служить любая бесконечная собственная модель, пополненная конечным числом произвольно выбранных интерпретаций $\varphi x$ и $\varphi y$, подчиненных единственному условию $\varphi x \neq \varphi y$. Следовательно, $P'$ непротиворечиво, так что мы заменим теперь $P$ на $P'$; иными словами, мы с самого начала исходим из того, что $P$ содержит $I$ и все формулы $x \neq y$, где $x$ и $y$ — все пары различных переменных из $M$.

Теперь мы строим языки $L_n$, множества $P_n$ и $Q_n$, как в доказательстве теоремы о непротиворечивости. В $L_1$, как мы знаем, имеется $m$ символов и $m$ формул. Пусть $L_n$ имеет мощность $m$ Тогда $L_n$ имеет не более $m$ формул вида $p = \mathsf{E} x q(x)$, так что $L_{n+1}$ получается из $L_n$ присоединением не более $m$ новых переменных. Из этого следует, что $L_{n+1}$ также имеет мощность $m$. Поскольку объединение счетной системы множеств мощности $m$ также имеет мощность $m$, то язык $L'$, как объединение всех $L_n$, имеет мощность $m$ и — поскольку он содержит множество $M$ — имеет в точности $m$ термов.

Интерпретация $\varphi$, полученная из $P'$ и $L'$, имеет, таким образом, область мощности $m$ Так как $\varphi I = 1$, то $\varphi$ определяет некоторую собственную интерпретацию $[\varphi]$, область которой имеет мощность, не превосходящую $m$. Если $x$ и $y$ суть различные элементы $M$, то формула $x \neq y$ принадлежит $P$, а так как $[\varphi]P = 1$, то $[\varphi]x \neq [\varphi]y$. Таким образом, $[\varphi]$ взаимно-однозначно отображает множество $M$ в область $[\varphi]$, которая поэтому имеет мощность, в точности равную $m$.

Следствие. *Если $P$ есть произвольное счетное или конечное множество формул языка $L$ с символом равенства, имеющее бесконечную собственную модель, то $P$ имеет собственные модели любой бесконечной мощности.*

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.





В качестве примера первого типа рассмотрим произвольное множество $A$ аксиом для натуральных чисел, которое может быть выражено на языке $L$ с символами $=$, $+$, $\times$ и, быть может, другими арифметическими символами. Допустим, что эти аксиомы истинны при обычной интерпретации — в области $N$ натуральных чисел. По теореме Лёвенгейма — Сколема отсюда следует, что $A$ имеет также несчетные модели. Как можно примирить это обстоятельство с привычным мнением о том, что аксиомы Пеано однозначным образом характеризуют натуральный ряд? Ответ на этот вопрос заключается в установлении того факта, что пеановская аксиома индукции может быть полностью выражена не в любом языке $L$. Одну из возможных формулировок этой аксиомы можно записать посредством схемы

$$[P(0) \wedge \mathsf{A} x [P(x) \supset P(x+1)] \supset \mathsf{A} x P(x),$$

где под $P$ понимается любое свойство Интуитивное содержание этой схемы состоит в том, что область, описываемая аксиомами, не содержит никаких элементов, кроме множества $N$ таких объектов, которые получаются из числа 0 путем последовательного прибавления 1. Чтобы выразить эту схему на языке $L$, мы должны заменить $P(x)$ на $p(x)$, где $p(x)$ — произвольная формула языка $L$. Но тем самым мы ограничиваем класс свойств $P$ теми свойствами, которые выразимы в языке $L$. Мы приходим, таким образом, к выводу, что, коль скоро язык $L$ фиксирован, мы не можем выразить средствами $L$ всех свойств, допускаемых нашей интуицией; в частности, мы не можем выразить свойства принадлежности множеству $N$.

В качестве примера второго типа мы хотим указать теорию, сформулированную на языке, область выражений которого имеет невысокую мощность, причем теория эта должна включать в себя утверждение о существовании некоторого обширного множества объектов. Такова, например, одна из наиболее скромных формулировок теории множеств. Допустим для определенности, что $L$ содержит счетное множество выражений, не содержит никаких функциональных символов и имеет единственный символ бинарного отношения $\in$, причем запись $x \in y$ содержательно истолковывается как утверждение о том, что $x$ есть элемент множества $y$. Допустим, что среди аксиом нашей теории $T$ имеется аксиома, утверждающая, что каждая модель содержит некоторое счетное множество, а также аксиома, утверждающая, что для любого множества $x$ существует множество $\sigma(x)$, элементами которого являются в точности все подмножества множества $x$. Создается впечатление, что любая модель такой теории $T$ должна содержать некоторое счетное множество $x$ и, кроме того, некоторое несчетное множество $\sigma(x)$. Однако по теореме Лёвенгейма — Сколема $T$ имеет счетную модель. И в этой ситуации нам снова приходится согласиться с выводом, что некоторые выражения языка расходятся в модели со своим подразумеваемым интуитивным смыслом. Обычно не представляет трудности добиться того, чтобы символ $\in$ имел свой обычный интуитивный смысл. Но утверждать, что $\sigma(x)$ содержит все подмножества множества $x$, в рассматриваемой ситуации уже нельзя: это множество теперь содержит лишь такие подмножества множества $x$, существование которых доказуемо в $T$; таким образом, $\sigma(x)$ остается счетным. Обычное доказательство того, что $\sigma(x)$ имеет бо́льшую мощность, чем $x$, здесь проходит; но теперь это доказательство утверждает лишь несуществование в модели отображения $x$ на $\sigma(x)$. Короче говоря, мы видим, что понятие мощности оказывается относительным; даже если теория и метатеория базируются на одних и тех же аксиомах, из этого еще не следует, что их модели непременно будут иметь одну и ту же мощность.

## Категоричность

Теория называется *категоричной*, если она допускает единственную (с точностью до несущественных различий) модель, иначе говоря, если она непротиворечива и если любые две ее модели изоморфны в обычном смысле. Если исходить из допущения, что понятия свойства и множества имеют некоторое





вполне определенное значение, скажем, в рамках некоторой приемлемой метатеории, и ограничиться рассмотрением интерпретаций, в которых эти понятия получают эти подразумеваемые однозначным образом значения, то обычные системы аксиом для натуральных чисел, рациональных чисел и действительных чисел оказываются категоричными. Если же мы, однако, рассматриваем аксиоматические теории в современном понимании этого слова, т. е. считаем, что такая теория — это множество $T$ всех следствий некоторого множества $A$ аксиом, то теорема Лёвенгейма — Сколема говорит нам, что никакая теория, имеющая бесконечную модель, не является категоричной.

Вместо категоричности иногда имеет смысл рассматривать более слабое понятие категоричности относительно мощности. Множество $P$ формул языка $L$ с символом равенства называют *категоричным относительно данной мощности* $m$, если с точностью до изоморфизма это множество имеет единственную модель мощности $m$. Приведем следующий критерий полноты, указанный Воотом:

Теорема. *Если теория $T$, определяемая посредством множества $A$ аксиом, имеющего мощность, не бо́льшую $m$, категорична относительно $m$ (причем $m$ бесконечно) и не имеет конечных моделей, то $T$ полна.*

Для доказательства этого утверждения допустим, что $T$ неполна и, следовательно, что имеется некоторое такое предложение $p$, что ни $p$, ни $\neg p$ не принадлежат $T$. Тогда оба множества $A \cup \{p\}$ и $A \cup \{\neg p\}$ непротиворечивы и, согласно теореме Лёвенгейма — Сколема, имеют некоторые модели мощности $m$; обозначим их $M_1$ и $M_2$. Из допущения о категоричности $A$ относительно мощности $m$ следует изоморфность $M_1$ и $M_2$, что, однако, противоречит тому, что $p$ верна в $M_1$, но не в $M_2$.

Это доказательство сохранит свою силу и для того случая, когда мы вместо категоричности относительно мощности $m$ принимаем более слабое предположение, что любые две модели теории $T$ мощности $m$

*элементарно эквивалентны* — в том смысле, что они удовлетворяют в точности одним и тем же предложениям языка $L$. Заметим, впрочем, что для большинства приложений такое усиление теоремы не требуется.

Мы уже видели, что теория плотного линейного порядка полна. Этот факт можно было бы получить из теоремы Кантора (которую нетрудно доказать с помощью аксиомы выбора) о том, что эта теория категорична относительно первой бесконечной мощности $\aleph_0$, т. е. что любые два плотных линейно упорядоченных счетных множества изоморфны.

Из описанного Тарским разрешающего метода для арифметики действительных чисел следует, что теория $T$, описывающая поле всех алгебраических чисел (теория эта формулируется на языке $L$, специальные символы которого суть $=$, $+$ и $\times$), полна. Этот результат можно также получить следующим образом из теоремы Воота. Во-первых, легко видеть, что модели теории $T$ — это в точности алгебраически замкнутые поля характеристики нуль и только они. Далее, такое поле $F$ с точностью до изоморфизма определяется своей степенью трансцендентности $d$, т. е. (однозначно определенной) мощностью максимального множества алгебраически независимых элементов поля $F$. Если $d$ конечно или счетно, то $F$ счетно; в остальных случаях $F$ имеет мощность $d$. Это означает, что теория $T$ категорична относительно любой несчетной бесконечной мощности $m$, откуда следует, что $T$ полна. Интересно отметить, что полная теория $T$ не категорична относительно счетной мощности $\aleph_0$: поле алгебраических чисел и поле всех алгебраических функций представляют собой счетные модели для $T$, но, разумеется, не изоморфны.

Интересующихся дальнейшим обсуждением этого круга вопросов отсылаем к книге А. Робинсона.

## Генценовский естественный вывод

Теперь мы рассмотрим аксиоматизацию логики предикатов, предложенную Генценом. Нам будет удобно исходить из того, что язык $L$ содержит связки





$\mathsf{N}$, $\mathsf{C}$, $\mathsf{D}$, $\mathsf{A}$ и $\mathsf{E}$, а также счетное множество переменных и счетное множество символов $\mathsf{R}$ отношений и не содержит функциональных символов. Нам будет также удобно пользоваться различными символами для обозначения свободных и связанных переменных. Мы будем считать, что множество переменных разбито на два множества: $\mathsf{V} = (v_1, v_2, \ldots)$ и $\Omega = (\omega_1, \omega_2, \ldots)$, и будем допускать в качестве правильно построенных только такие формулы, в которых каждая свободная переменная взята из множества $\mathsf{V}$, а каждая связанная переменная — из множества $\Omega$. Главное удобство такого соглашения состоит в том, что мы теперь всегда можем подставить в любую формулу переменную из множества $\mathsf{V}$.

Аксиоматизация, которую мы здесь опишем, представляет собой некоторое расширение описанного ранее понятия аксиоматизации. Вместо отдельных формул мы будем теперь иметь дело с конечными множествами формул, а точнее — даже с упорядоченными парами таких множеств. Если $S$ и $T$ — произвольные конечные множества формул, мы будем называть упорядоченную пару $C=(S, T)$ *секвенцией* и использовать для записи $C$ более выразительное обозначение $S \to T$. Мы будем также вместо $S_1, S_2 \to T_1, T_2$ писать $S_1 \cup S_2 \to T_1 \cup T_2$. Секвенция $S \to T$, где $S=(s_1, \ldots, s_m)$ и $T=(t_1, \ldots, t_n)$, *общезначима* в том и только том случае, когда общезначима формула $\bigwedge s_i \supset \bigvee t_j$. Отсюда становится ясным подразумеваемое значение секвенции как утверждения о том, что из одновременного принятия всех посылок $s_i$ выводится по крайней мере одно из заключений $t_j$.

Мы выделим некоторые секвенции определенного вида в качестве аксиом. Сформулировав затем правила вывода для секвенций, мы получим определение доказательства секвенции. Нашей ближайшей целью является теорема адекватности, согласно которой (правильно построенная) секвенция общезначима тогда и только тогда, когда она доказуема.

*Аксиомой* является любая секвенция $S \to T$, такая, что в $S$ и $T$ входит хоть одна общая формула.

*Правила вывода* — это отношения между посылкой $C$ (или парой посылок $C_1$ и $C_2$) и заключением $D$. Соответствующие схемы для правил вывода мы будем записывать в виде

$$\frac{C}{D} \quad \text{или} \quad \frac{C_1 \mid C_2}{D}.$$

Иногда нам будет удобно рассматривать однопосылочное правило вывода как двухпосылочное с двумя одинаковыми посылками. Каждое правило вывода охватывает все пары или тройки правильно построенных формул, подпадающие под некоторые определенные схемы; схемы эти имеют следующий вид:

$$N_- \ \frac{S \to T,\ p}{S,\ \neg p \to T} \qquad N_+ \ \frac{S,\ p \to T}{S \to T,\ \neg p}$$

$$C_- \ \frac{S,\ p,\ q \to T}{S,\ p \wedge q \to T} \qquad C_+ \ \frac{S \to T,\ p \mid S \to T,\ q}{S \to T,\ p \wedge q}$$

$$D_- \ \frac{S,\ p \to T \mid S,\ q \to T}{S,\ p \vee q \to T} \qquad D_+ \ \frac{S \to T,\ p,\ q}{S \to T,\ p \vee q}$$

$$A_- \ \frac{S,\ p(x) \to T}{S,\ \mathsf{A}\xi p(\xi) \to T} \qquad A_+ \ \frac{S \to T,\ p(x)}{S \to T,\ \mathsf{A}\xi p(\xi)}$$

$$E_- \ \frac{S,\ p(x) \to T}{S,\ \mathsf{E}\xi p(\xi) \to T} \qquad E_+ \ \frac{S \to T,\ p(x)}{S \to T,\ \mathsf{E}\xi p(\xi)}.$$

В схемах $A_+$ и $E_-$ предполагается, что $x$ не входит соответственно в $S$ и $T$.

*Выводом* из множества $W$ секвенций некоторой секвенции $D$ мы будем называть конечную последовательность $C_1, \ldots, C_n$ секвенций, такую, что $C_n = D$, а каждая секвенция $C_i$ есть либо аксиома, либо принадлежит $W$, либо является заключением по одному из правил из некоторых посылок, вывод которых встречается ранее в этой последовательности. *Доказательство* секвенции $D$ — это вывод $D$ из пустого множества посылок. Секвенция, для которой существует доказательство, называется *теоремой*.





Легко видеть, что каждая аксиома истинна и что если посылки любого правила истинны, то и заключение также истинно. Из этого следует, что каждая теорема истинна, так что остается доказать только обратное утверждение.

Легко также видеть, что вопросы о том, является ли данная секвенция аксиомой и следует ли данная секвенция из двух других по какому-либо из правил вывода, разрешимы. Следовательно, разрешима и проблема, является ли данная последовательность секвенций выводом данной секвенции $D$ из данного множества $W$ секвенций.

Прежде чем перейти к примеру конкретного доказательства, заметим, что в данной аксиоматизации в отличие от описанной выше основную роль играют не аксиомы, в высшей степени тривиальные, а относительно многочисленные правила вывода. Каждое конкретное правило, однако, имеет очень простой вид и служит весьма ограниченной цели, для достижения которой оно, очевидно, как раз и предназначено. Например, правило $D_-$ указывает единственный способ, которым можно ввести связку $\vee$ в левую часть секвенции по ходу вывода, причем это правило точно описывает все ситуации, в которых такое введение законно. В этом смысле два правила $D_-$ и $D_+$ вместе играют вполне определенную роль «бихевиористической» характеристики связки $\vee$. Эта специализация правил оставлят очень мало свободы выбора посылок, из которых нужно вывести данное заключение, и поэтому в значительной мере предопределяет путь доказательства каждой конкретной теоремы.

В качестве иллюстрации мы рассмотрим доказательство секвенции

$$\mathsf{A}\xi\mathsf{E}\eta r\xi\eta \to \mathsf{A}\xi\mathsf{E}\eta\mathsf{E}\zeta(r\xi\eta \wedge r\eta\zeta),$$

где $r$ — символ бинарного отношения. В столбце, помещенном справа от приводимого вывода, указывается обоснование каждой его строки.

$$\begin{array}{lll}
rxy,\ ryz \to rxy \quad \mid \quad rxy,\ ryz \to ryx & & \text{(аксиомы)} \\ \hline
rxy,\ ryz & \to rxy \wedge ryz & (C_+) \\ \hline
rxy,\ ryz & \to \mathsf{E}\zeta(rxy \wedge ry\zeta) & (E_+) \\ \hline
rxy,\ ryz & \to \mathsf{E}\eta\mathsf{E}\zeta(rx\eta \wedge r\eta\zeta) & (E_+) \\ \hline
rxy,\ \mathsf{E}\eta ry\eta & \to \mathsf{E}\eta\mathsf{E}\zeta(rx\eta \wedge r\eta\zeta) & (E_-) \\ \hline
rxy,\ \mathsf{A}\xi\mathsf{E}\eta r\xi\eta & \to \mathsf{E}\eta\mathsf{E}\zeta(rx\eta \wedge r\eta\zeta) & (A_-) \\ \hline
\mathsf{E}\eta rx\eta,\ \mathsf{A}\xi\mathsf{E}\eta r\xi\eta & \to \mathsf{E}\eta\mathsf{E}\zeta(rx\eta \wedge r\eta\zeta) & (E_-) \\ \hline
\mathsf{A}\xi\mathsf{E}\eta r\xi\eta,\ \mathsf{A}\xi\mathsf{E}\eta r\xi\eta & \to \mathsf{E}\eta\mathsf{E}\zeta(rx\eta \wedge r\eta\zeta) & (A_-) \\ \hline
\mathsf{A}\xi\mathsf{E}\eta r\xi\eta,\ \mathsf{A}\xi\mathsf{E}\eta r\xi\eta & \to \mathsf{A}\xi\mathsf{E}\eta\mathsf{E}\zeta(r\xi\eta \wedge r\eta\zeta) & (A_+)
\end{array}$$

Следует, конечно, удостовериться в том, что правила $A_+$ и $E_-$ применялись для замены переменной в формуле на связанную переменную только тогда, когда эта переменная не входила ни в какую другую формулу той же секвенции. Именно этим условием определяется в значительной степени порядок шагов в доказательстве. Следует отметить, что последняя секвенция действительно есть доказываемая секвенция $S \to T$; дело в том, что $S$ не меняется оттого, что единственный ее член записывается в ней дважды. Именно эта возможность соединения повторяющихся формул в одну обусловливает то обстоятельство, что отыскание доказательства для заданной истинной секвенции не является абсолютно механической процедурой.

### Упражнения

1. Как можно было бы изменить приведенное доказательство, не удлиняя его?

2. Докажите секвенцию $p \wedge (q \vee r) \to (p \wedge q) \vee (p \wedge r)$; секвенцию $\mathsf{F}\xi\mathsf{A}\eta p \to \mathsf{A}\eta\mathsf{E}\xi p$.

3. Видоизмените описанный выше формализм применительно к случаю, когда к $L$ добавлены связки $\mathbf{0}$ и $\mathbf{1}$; когда к $L$ добавлена связка $\mathbf{J}$; когда $L$ содержит функциональные символы.





## Другая формулировка

Применяя правило $N_+$, мы можем перенести все формулы секвенции из левой части в правую, приписывая к каждой из них символ $\to$: секвенция $C$: $s_1, \ldots, s_m \to t_1, \ldots, t_n$ заменяется при этом эквивалентной ей секвенцией $C'$: $\varnothing \to \to s_1, \ldots, \to s_m, t_1, \ldots, t_n$. Рассматривая секвенции лишь такого вида $\varnothing \to T$, мы можем упростить описание нашей системы, переформулировав всю теорию в предположении, что каждая секвенция уже приведена к такой единообразной форме. Фигурирующие в записи каждой секвенции два начальных символа $\varnothing, \to$ можно теперь опустить, после чего *секвенция* определится просто как конечное множество формул.

*Аксиомой* теперь будет называться любая секвенция $T$, содержащая некоторую формулу $p$ вместе с ее отрицанием $\to p$.

Правила вывода примут тогда следующий вид:

$$\begin{array}{llll}
N_- & \dfrac{T,\ p}{T,\ \to\to p} & N_+ & \dfrac{T,\ \to p}{T,\ \to p} \\[2ex]
C_- & \dfrac{T,\ \to p,\ \to q}{T,\ \to(p \wedge q)} & C_+ & \dfrac{T,\ p \mid T,\ q}{T,\ p \wedge q} \\[2ex]
D_- & \dfrac{T,\ \to p \mid T,\ \to q}{T,\ \to(p \vee q)} & D_+ & \dfrac{T,\ p,\ q}{T,\ p \vee q} \\[2ex]
A_- & \dfrac{T,\ \to p(x)}{T,\ \to \mathsf{A}\xi p(\xi)} & A_+ & \dfrac{T,\ p(x)}{T,\ \mathsf{A}\xi p(\xi)} \\[2ex]
E_- & \dfrac{T,\ \to p(x)}{T,\ \to \mathsf{E}\xi p(\xi)} & E_+ & \dfrac{T,\ p(x)}{T,\ \mathsf{E}\xi p(\xi)}
\end{array}$$

Здесь в $A_+$ и $E_-$ предполагается, что $x$ не входит в $T$.

Заметим прежде всего, что правило $N_+$ ввиду его бесполезности мы можем опустить. Далее мы заменим правила $A_-$ и $E_-$ следующими двумя правилами:

$$A'_- \quad \frac{T,\ \mathsf{E}\xi \to p(\xi)}{T,\ \to \mathsf{A}\xi p(\xi)}, \qquad E'_- \quad \frac{T,\ \mathsf{A}\xi \to p(\xi)}{T,\ \to \mathsf{E}\xi p(\xi)}.$$

Отметим, что применение правила $A_-$ всегда можно заменить последовательным применением правил $E_+$ и $A'_-$:

$$\frac{\dfrac{T, \rightharpoondown p(x)}{T,\ \mathsf{E}\xi \rightharpoondown p(\xi)}\ (E_+)}{T, \rightharpoondown \mathsf{A}\xi p(\xi)}\ (A'_-),$$

причем можно добиться, чтобы применения $A'_-$ в любом выводе встречались лишь в таком контексте. Из этого следует, что замена $A_-$ на $A'_-$ не изменяет множества теорем нашей теории. В точности то же самое можно сказать по поводу замены $E_-$ на $E'_-$.

Отметим, наконец, что доказательство адекватности первой формулировки позволяет немедленно сделать вывод об адекватности второй. В самом деле, если $C$ — произвольная секвенция в первой формулировке, а $C'$ — соответствующая ей секвенция, преобразованная ко второй форме, то легко усмотреть, как перевести доказательство $C$ в первом формализме в доказательство $C'$ во втором и обратно

### Упражнения

1. Приведите полностью доказательство того факта, что замена правил $A_-$ и $E_-$ на $A'_-$ и $E'_-$ не изменяет множества теорем

2. Выпишите во всех подробностях правила перевода доказательств первого формализма в доказательства второго и обратно.

3. Дайте описание третьей модификации рассматриваемой теории, получающейся в результате переноса всех преобразованных соответствующим образом формул из правой части каждой секвенции в левую ее часть.

## Теорема адекватности

Теперь мы еще несколько изменим формулировку генценовского исчисления; цель наша при этом будет заключаться в том, чтобы никакая секвенция не могла быть получена в качестве заключения посредством более чем одного правила вывода. Анализ описанных выше правил генценовской системы приводит к выводу, что для достижения этой цели нам надо было бы научиться для каждого заключения вида $C = T \cup \{p\}$ определять, какая именно формула $p$ была введена в эту секвенцию посредством применения правила вывода. Для этого же нам в свою очередь придется рассматривать секвенции как упорядоченные множества формул и договориться о том, как в каждой такой конкретной последовательности формул находить формулу, введенную последним применением правила вывода.





Переходя к более точным формулировкам, мы будем теперь называть *секвенцией* упорядоченное множество $C = (c_1, \ldots, c_n)$ формул, причем некоторые из этих формул могут и повторяться. *Аксиомой* мы попрежнему будем называть любую секвенцию $C$, содержащую какую-нибудь формулу $p$ вместе с ее отрицанием $\rightharpoondown p$. Формулу мы будем называть *простой*, если она является атомарной формулой $p$ или имеет вид отрицания $\rightharpoondown p$ атомарной формулы. *Простая* секвенция — это секвенция, состоящая исключительно из простых формул. Через $T, U, V$ или $T \cup U \cup V$ мы будем ниже обозначать секвенцию, составленную из секвенций $T, U$ и $V$, взятых в указанном здесь порядке.

Каждое из описанных нами выше правил имело вид

$$\frac{T, U_1 \mid T, U_2}{T, U_3};$$

теперь мы заменим такое правило схемой вида

$$\frac{T, U_1, V \mid T, U_2, V}{T, U_3, V},$$

предполагая при этом секвенцию $T$ непременно простой. Схему $E_+$ мы изменим, придав ей вид

$$E_+ \quad \frac{T,\ p(x),\ V,\ \mathsf{E}\xi p(\xi)}{T,\ \mathsf{E}\xi p(\xi),\ V}.$$

Легко видеть, что при такой формулировке системы секвенция $C$ может быть заключением некоторого вывода в том и только том случае, когда она не является простой. В случае когда дело обстоит именно так, мы, написав $C = T \cup U_3 \cup V$, где $U_3$ — первая по порядку формула в секвенции $C$, не являющаяся простой, можем по виду формулы $U_3$ однозначно определить, применением какого правила вывода получается секвенция $C$. Дело в том, что посылки вывода определены однозначно, если не считать правил $A_+$ и $E_+$, в посылках которых фигурирует переменная $x$, не определенная однозначным образом.

Взяв теперь произвольную секвенцию $S$, мы выпишем для нее секвенции $S_1$ и $S_2$, из которых ее можно вывести (секвенции $S_1$ и $S_2$ не только являются единственными возможными посылками для $S$, но в то же время необходимы для ее вывода). Будем продолжать эту процедуру выписывания возможных (и в то же время необходимых) посылок $T_1$ и $T_2$ для каждой появляющейся в ее ходе секвенции $T$, располагая $T_1$ и $T_2$ над $T$. Точнее говоря, если данная секвенция $T$ есть аксиома или простая секвенция, то мы не выписываем для нее никаких посылок; в противном же случае мы пишем над секвенцией $T$ одну или две посылки — в зависимости от вида $T$. Эти посылки для данной секвенции $T$ определяются по ее виду однозначным образом, если не считать случаев, когда $T$ есть секвенция, выводящаяся по правилу $A_+$ или $E_+$. В первом из этих случаев $T$ имеет вид $U \cup \mathsf{A}\xi p(\xi) \cup V$ и мы выбираем в качестве посылки $T_1$ секвенцию $U \cup p(x) \cup V$, где $x$ — первая из списка переменных $v_1, v_2, \ldots$, не входящая ни в $U$, ни в $V$. В случае же $E_+$, когда $T$ имеет вид $U \cup \mathsf{E}\xi p(\xi) \cup V$, мы пишем посылку $T_1$ — секвенцию $U \cup p(x) \cup V \cup \mathsf{E}\xi p(\xi)$, где $x$ есть первая из таких переменных $v_i$, что формула $p(x)$ не входит ни в одну из секвенций в цепочке заключений, идущих от $T$ к $S$. *Деревом* $T(S)$ мы будем называть минимальное множество секвенций, содержащее $S$ и такое, что для любой секвенции $T$, входящей в $T(S)$, в $T(S)$ входят и посылки, из которых по правилам генценовского исчисления следует $T$.

Секвенция $D$, входящая в дерево $T(S)$, называется ***вершиной***, если в $T(S)$ над ней нет ни одной секвен-





ции, являющейся ее посылкой. Из определения дерева следует, что вершина непременно должна быть аксиомой или простой секвенцией. Если дерево $T(S)$ конечно и все его вершины являются аксиомами, то, если отвлечься от порядка перечисления секвенций, $T(S)$ сразу дает нам доказательство секвенции $S$ (понимаемой как неупорядоченное множество формул) во второй из описанных выше формулировок генценовской системы. Чтобы получить теперь полное доказательство теоремы адекватности, нам остается лишь показать, что если дерево $T(S)$ бесконечно или среди его вершин не все являются аксиомами, то $S$ не общезначима.

Если какая-нибудь из вершин $D$ дерева $T(S)$ не является аксиомой, то $T(S)$, очевидно, содержит цепочку $S = S_1, S_2, \ldots, S_d = D$, каждый из членов $S_{n+1}$ которой есть одна из посылок секвенции $S_n$. Если $T(S)$ бесконечно, то, как мы сейчас покажем, $T(S)$ содержит бесконечную цепочку $S = S_1, S_2, \ldots$, каждый из членов которой есть одна из посылок секвенции $S_n$. По предположению в $T(S)$ имеется бесконечно много секвенций, расположенных над $S = S_1$; сделав индуктивное допущение, что мы уже нашли такую цепочку $S_1, \ldots, S_n$, что над $S_n$ в $T(S)$ расположено бесконечно много секвенций, мы легко придем к заключению, что то же самое справедливо и по отношению по крайней мере к одной из посылок секвенции $S_n$, так что нам остается лишь выбрать одну из этих посылок в качестве $S_{n+1}$. [Если указанным свойством обладают обе посылки секвенции $S_n$, мы можем, опираясь на аксиому выбора, всегда выбрать ту из них, которая предшествует другой в алфавитном перечне выражений языка $L$.] В любом из этих случаев множество всех формул, входящих в какую-либо из секвенций $S_n$ цепочки, мы обозначим через $P$.

Теперь мы опишем некоторую интерпретацию $\varphi$ языка $L$ с областью $\mathsf{V} = (v_1, v_2, \ldots)$. Для переменной $x$ из $\mathsf{V}$ мы положим по определению $\varphi x = x$. Как мы будем интерпретировать переменные $\xi$ из $\Omega$, несущественно; для простоты положим $\varphi\omega_i = v_i$. Для символа отношения $r$ из $\mathsf{R}_n$ определим $\varphi r$ в соответствии с соглашением, что $(\varphi r)(x_1, \ldots, x_n)=1$ тогда и только тогда, когда формула $rx_1 \ldots x_n$ *не* принадлежит $P$. Покажем индукцией по длине формулы, что $p \in P$ влечет $\varphi p=0$.

Если $p=rx_1 \ldots x_n$ — атомарная формула и $p \in P$, то $\varphi p=(\varphi r)(x_1, \ldots, x_n)=0$ в силу определения $\varphi_r$. Допустим теперь, что $p=\neg q$, где $q=rx_1 \ldots x_n$ — атомарная формула, причем $p \in P$. Если бы $q$ также принадлежала $P$, то $p$ входила бы в некоторую секвенцию $S_n$, а $q$ — в некоторую $S_m$, так что обе они входили бы в $S_h$, где $k=\operatorname{Max}(n, m)$. Тогда $S_k$ была бы аксиомой, что, разумеется, невозможно для членов нашей цепочки. Поэтому мы заключаем, что $q$ не принадлежит $P$, откуда в силу определения $\varphi r$ следует, что $\varphi q=(\varphi r)(x_1, \ldots, x_n)=1$, так что $\varphi p=0$. Этим завершается доказательство высказанного утверждения для случая простой формулы $p$.

Допустим теперь, что $p$ — не простая формула и не имеет вид $\mathsf{E}\xi q(\xi)$. В этом случае $p$ есть $U_3$ из заключения $S_n$ некоторого вывода вида

$$\frac{T,\ U_1,\ V \mid T,\ U_2,\ V}{T,\ U_3,\ V},$$

и легко убедиться посредством обращения к определению интерпретации и прямой проверки, что $\varphi U_3=1$ влечет $\varphi U_1=\varphi U_2=1$. Следовательно, одна из формул $U_1$ и $U_2$ входит в $S_{n+1}$, а, значит, и в $P$, причем эта формула $q$ короче формулы $p$. По предположению индукции, $\varphi q=0$, т. е. либо $\varphi U_1=0$, либо $\varphi U_2=0$, из чего следует, что $\varphi p=\varphi U_3=0$.

Допустим, наконец, что $p=\mathsf{E}\xi q(\xi)$ входит в $S_n= T \cup \mathsf{E}\xi q(\xi) \cup V$. Тогда из описания правил вывода ясно, что $p$ входит также в каждую $S_m$, расположенную в цепочке после $S_n$. Если некоторая $S_m= T_m \cup \{p\} \cup V_m$, где $T_m$ не является простой, то $S_{m+1}=T_{m+1} \cup \{p\} \cup V_{m+1}$, где сумма длин входящих в $T_{m+1}$ непростых формул меньше суммы длин непростых формул, входящих в $T_m$. Если $T_m$ проста, то





$S_{m+1}=T_m \cup \{q(v_i)\} \cup V_m \cup \{p\}$, где $v_i$ есть первая переменная из обладающих тем свойством, что $q(v_i)$ не входит ни в один из предшествующих членов данной цепочки. Из этого следует, что наша цепочка содержит бесконечно много секвенций $S_m$ с простыми $T_m$ и что для любой переменной $v_i$ формула $q(v_i)$ в конце концов входит в некоторый член цепочки. Следовательно, $q(x) \in P$ для любой переменной $x$ из $\mathbf{V}$. Так как $q(x)$ короче, чем $p=\mathsf{E}\xi q(\xi)$, то в силу индукционного предположения $\varphi q(x)=0$ для всех $x$ из $\mathbf{V}$, откуда в свою очередь следует, что $\varphi p=0$.

Мы показали, что $p \in P$ влечет $\varphi p=0$. Так как каждая формула $s$ из $S=S_1$ входит в $P$, то $\varphi s=0$ для любой такой $s$, а, значит, $S$ не общезначима. Иными словами, мы показали, что если $S$ не является теоремой, то $S$ не общезначима. Этим завершается доказательство теоремы адекватности.

Теорема адекватности. *Произвольная секвенция $S$ является теоремой тогда и только тогда, когда $S$ общезначима.*

Построение дерева $T(S)$ дает нам либо доказательство секвенции $S$, либо бесконечный контрпример к несуществующему доказательству. Такое построение не дает нам разрешающего алгорифма, так как для произвольной секвенции $S$ мы не можем указать такого пункта в процессе построения дерева $T(S)$, идущего вверх от $S$, начиная с которого мы, не получив доказательства, могли бы быть уверены, что его вообще никогда не удастся найти. Однако имеется метод, исходящий по существу от Эрбрана, не только естественный, но и весьма эффективный для поиска доказательства; метод этот используется для проверки истинности математических предложений с помощью вычислительных машин. Можно также выделить ограниченные, но никоим образом не тривиальные классы секвенций, для которых этот метод является разрешающим алгоритмом.

# Теорема Эрбрана — Генцена

Усовершенствование ранних идей Эрбрана достигнуто в одной теореме Генцена, которую сейчас обычно называют теоремой Эрбрана — Генцена.

Формула называется *предваренной*, если все вхождения в нее кванторов предшествуют всем вхождениям других связок. Более точно: предваренная формула имеет вид $p = Q_1\xi_1 \ldots Q_n\xi_n q$, где каждое $Q_i$ есть либо **A**, либо **E**, а $q$ есть формула, не содержащая ни **A**, ни **E**. Секвенция, каждая из формул которой является предваренной, также называется *предваренной*.

Т е о р е м а. *Каждая формула эквивалентна некоторой предваренной формуле.*

Эта теорема прямо доказывается индукцией по длине формулы с помощью следующих правил:

$$\rightarrow \mathbf{A}\xi p \vDash\dashv \mathbf{E}\xi \rightarrow p, \quad \rightarrow \mathbf{E}\xi p \vDash\dashv \mathbf{A}\xi \rightarrow p,$$

$$p \wedge \mathbf{A}\xi q(\xi) \vDash\dashv \mathbf{A}\zeta(p \wedge q(\zeta)), \quad p \wedge \mathbf{E}\xi q(\xi) \vDash\dashv \mathbf{E}\zeta(p \wedge q(\zeta)),$$

$$p \vee \mathbf{A}\xi q(\xi) \vDash\dashv \mathbf{A}\zeta(p \vee q(\zeta)), \quad p \vee \mathbf{E}\xi q(\xi) \vDash\dashv \mathbf{E}\zeta(p \vee q(\zeta),$$

где $\zeta$ — новая переменная.

Т е о р е м а Э р б р а н а — Г е н ц е н а. *Для любой общезначимой предваренной секвенции $S$ существует такая не содержащая кванторов общезначимая секвенция $P$, что $S$ выводима из $P$ посредством одних только кванторных правил $A_-$, $A_+$, $E_-$ и $E_+$.*

Утверждение теоремы сформулировано здесь в терминах первой из рассмотренных нами модификаций генценовского исчисления; легко, однако, видеть, что для доказательства этого утверждения достаточно уметь доказывать ее применительно ко второй модификации. Пусть $C$ есть $s_1, \ldots, s_m \rightarrow t_1, \ldots, t_n$ — произвольная предваренная секвенция в смысле первой модификации. Пусть $*s_i$ — предваренная формула, полученная из формулы $\rightarrow s_i$ $(i = 1, \ldots, m)$ последовательной заменой каждого вхождения вида $\rightarrow \mathbf{A}\xi$ на $\mathbf{E}\xi \rightarrow$ и $\rightarrow \mathbf{E}\xi$





на $\mathbf{A}\xi \rightarrow$. Пусть, далее, $C' = (*s_i, \ldots, *s_m, t_1, \ldots, t_n)$. Предположим теперь, что нам даны некоторая предваренная секвенция $S$ и вывод во второй модификации генценовского исчисления, использующий одни только кванторные правила, секвенции $S'$ из некоторой бескванторной секвенции $D'$. Тогда мы легко получим вывод секвенции $S$, использующий одни лишь кванторные правила, из некоторой бескванторной секвенции $D$. Для этого достаточно каждую формулу $*s_i$ заменить (посредством замен, обратных к тем, посредством которых $s_i$ преобразовывается в $*s_i$) на $s_i$, а применения правил $A_+$ и $E_+$ к формулам $*s_i$ — на применение правил $E_-$ и $A_-$ к соответствующим $s_i$.

Итак, нам остается доказать теорему Эрбрана — Генцена для второй формулировки генценовского исчисления. Для этого нам будет удобно ввести одно новое правило $X$, задаваемое схемой $\dfrac{T}{T, U}$. Очевидно, что добавление этого правила не меняет смысла утверждений теоремы адекватности и теоремы Эрбрана — Генцена. С помощью нового правила $X$ каждая аксиома может быть получена в качестве заключения некоторого вывода с единственной посылкой вида $C = (p, \rightarrow p)$. Поэтому мы, не ограничивая общности рассуждений, сможем впредь считать, что все аксиомы имеют именно такой вид: $p, \rightarrow p$.

Предположим теперь, что $S$ есть общезначимая предваренная секвенция в смысле второй формулировки. По теореме адекватности из того, что $S$ общезначима, следует, что для нее существует некоторое доказательство $D$. По предположению $S$ — предваренная секвенция. Но если заключением вывода является предваренная секвенция, то, очевидно, посылки — тоже предваренные секвенции. Отсюда видно, что в доказательство $D$ входят только предваренные формулы. Это означает, в частности, что $D$ не содержит выводов по правилам $A'_-$ и $E'_-$. Далее, если в $D$ входит некоторая аксиома $C = (p, \rightarrow p)$, то из того факта, что $\rightarrow p$ — предваренная формула, сразу следует, что $p$ не содержит кванторов, а, значит, и $C$ — бескванторная формула. Если бы нам теперь удалось показать, что все пропозициональные выводы (т. е. выводы по правилам $X$, $N_-$, $C_-$, $C_+$, $D_-$ и $D_+$) встречаются только в качестве вершин, причем в результате совместного применения этих правил из аксиом выводится некоторая бескванторная секвенция $P$, и что оставшаяся часть доказательства представляет собой вывод $S$ из $P$ по одним только правилам $A_+$ и $E_+$, то теорема была бы доказана. В самом деле, достаточно показать, что мы можем выбрать $D$ таким образом, чтобы все применения правил $A_+$ и $E_+$ входили в него подряд в самом конце доказательства, так как если $P$ содержит какую-нибудь предваренную формулу $p = Q_1\xi_1 \ldots Q_n\xi_n q(\xi_1, \ldots, \xi_n)$ (непременно в качестве результата применения правила $X$), то мы можем преобразовать $P$ в $P'$, введя вместо $p$ некоторую формулу $q(x_1, \ldots, x_n)$, и затем перейти от $P'$ к $P$ с помощью правил $A_+$ и $E_+$.

Поскольку мы можем воспользоваться очевидной индукцией по длине доказательства, достаточно будет предположить, что $D$ оканчивается применением пропозиционального правила, одна из посылок которого получена посредством кванторного правила, и показать, что эти последние два применения правил вывода могут быть заменены выводом, в котором все применения пропозициональных правил предшествуют всем применениям кванторных правил. Мы можем предположить, что $D$ заканчивается применением пропозиционального правила

$$\frac{T,\ q_1 \mid T,\ q_2}{T,\ q},$$

две посылки которого могут и совпадать друг с другом или — если имеет место применение правила $X$ — даже отсутствовать. Мы можем, кроме того, предположить, что секвенция $T,\ q_1$ есть заключение вывода по правилу $A_+$ или $E_+$. Так как $q_1$ — предваренная формула, то формула $Q\xi p(\xi)$, вводимая этим правилом, должна принадлежать $T$. Таким образом рассматриваемый вывод должен иметь вид

$$\cfrac{\cfrac{U,\ p(x),\ q_1}{U,\ Q\xi p(\xi),\ q_1} \mid U,\ Q\xi p(\xi),\ q_2}{U,\ Q\xi p(\xi),\ q}.$$





Если верхняя посылка получается по правилу $A_+$, то переменная $x$ не может входить ни в $U$, ни в $q_1$. Несущественно видоизменив часть доказательства, дающую нам секвенцию $U,\ Q\xi p(\xi),\ q_1$, мы можем добиться того, чтобы $x$ не входила в $q$.

А теперь мы заменим рассматриваемый вывод следующим:

$$\cfrac{\cfrac{\cfrac{U,\ p(x),\ q_1}{U,\ Q\xi p(\xi),\ p(x),\ q_1} \mid \cfrac{U,\ Q\xi p(\xi),\ q_2}{U,\ Q\xi p(\xi),\ p(x),\ q_2}}{U,\ Q\xi p(\xi),\ p(x),\ q}}{U,\ Q\xi p(\xi),\ q}.$$

Здесь обе посылки двухпосылочного правила получаются по правилу $X$. Следующий же шаг вывода производится посредством того же самого пропозиционального правила, которое применялось на последнем шаге в $D$. Заключительный шаг вывода — применение того самого правила $A_+$ или $E_+$, которое входило в исходный вывод. Если этот последний шаг есть применение правила $A_+$, то необходимо еще убедиться, что переменная $x$ не входит ни в $U$, ни в $Q\xi p(\xi)$, ни в $q$. Прежде всего, поскольку правило $A_+$ использовалось еще в исходном выводе, то $x$ не входит в $U$. Из определения $Q\xi p(\xi)$ через $p(x)$ ясно, что $x$ не входит в $Q\xi p(\xi)$. Наконец, предварительное преобразование, которому мы подвергли доказательство $D$, гарантирует нам, что $x$ не входит в $q$. Так как полученный нами новый вывод обладает, очевидно, требуемыми свойствами, то теорема Эрбрана — Генцена доказана.

### Упражнение

Видоизмените доказательство теоремы Эрбрана — Генцена применительно к языку $L$, содержащему дополнительные связки 0 и 1; к языку с функциональными символами.

## Теорема Крэйга

В качестве иллюстрации возможностей применения теоремы Эрбрана—Генцена мы докажем теорему Крэйга (несмотря на интуитивную ясность этой теоремы, для нее не известно никакого принципиально отличного от приводимого ниже синтаксического доказательства[1]). Для простоты мы будем сейчас предполагать, что $L$ содержит связки $\mathsf{0}$ и $\mathsf{1}$.

Теорема Крэйга. *Для любых таких формул $p$ и $q$, что $p \models q$, найдется формула $m$, содержащая лишь те символы отношений, которые входят как в $p$, так и в $q$, и такая, что $p \models m$ и $m \models q$.*

Вначале мы рассмотрим случай бескванторных $p$ и $q$. Мы можем предполагать, что $p$ записана в дизъюнктивной форме $p = \bigvee_i \bigwedge_j p_{ij}$, где $p_{ij}$ — простые формулы, и что $q$ имеет вид $q = \neg r$, где $r$ — некоторая формула, записанная в дизъюнктивной форме $r = \bigvee_h \bigwedge_k r_{hk}$ с простыми $r_{hk}$. Пусть $m = \bigvee_i \bigwedge_j{}' p_{ij}$ — формула, полученная из $p$ опусканием каждого члена $p_{ij}$, содержащего символы отношений, не входящие в $q$. Ясно, что $p \models m$, причем $m$ содержит только такие символы отношений, которые входят как в $p$, так и в $q$. Остается показать, что $m \models q$. Но так как $q = \neg r$, то из $p \models q$ следует, что $p, r \models \mathsf{0}$, из чего в свою очередь вытекает, что для любой пары номеров $i$ и $h$ $\bigwedge_j p_{ij}, \bigwedge_k r_{hk} \models \mathsf{0}$, т. е. что для некоторых $p_{ij}$ и $r_{hk}$ $p_{ij}, r_{hk} \models \mathsf{0}$. Но последнее соотношение возможно лишь в том случае, когда $p_{ij}$ содержит те же символы отношений, что и $r_{hk}$, т. е. когда $p_{ij}$ остается в части $\bigwedge_j{}' p_{ij}$ формулы $m$. Отсюда следует, что $\bigwedge_j{}' p_{ij}, \bigwedge_k r_{hk} \models \mathsf{0}$, откуда $m, r \models \mathsf{0}$ и $m \models q$.

Чтобы перейти отсюда к общему случаю, нам понадобится следующая лемма.

Лемма. *Пусть существует вывод секвенции $S' \to T'$ из секвенции $S \to T$ с помощью одних только кванторных правил, и пусть $m$ — произвольная формула. Тогда найдется такая формула $m'$, для которой существуют выводы секвенции $S' \to m'$ из секвенции $S \to m$ и секвенции $m' \to T'$ из секвенции $m \to T$ с помощью кванторных правил.*

[1] Принадлежащего автору, формулируемая ниже теорема известна также под именем интерполяционной теоремы, или теоремы Крэйга — Линдона. — *Прим. перев*





Ведя доказательство индукцией по длине данного вывода секвенции $S' \to T'$ из $S \to T$, мы можем предположить, что этот вывод состоит из единственного шага по одному из правил $A_-$, $A_+$, $E_-$ или $E_+$. Если применяемое правило есть $A_-$ или $E_+$, не предполагающее никаких условий на вхождения переменных, то мы можем положить $m' = m$. Тогда один из двух выводов

$$\frac{S \to m}{S' \to m}, \qquad \frac{m \to T}{m \to T'}$$

тривиален, а другой обосновывается тем же правилом $A_-$ или $E_+$. Если применяемое правило есть $A_+$, то исходный вывод имеет вид

$$\frac{S \to U,\ p(x)}{S \to U,\ \mathsf{A}\xi p(\xi)},$$

где $x$ не входит ни в $S$, ни в $U$. Но $x$ может входить в формулу $m$, которую мы запишем поэтому в виде $m = m(x)$; тогда мы положим $m' = \mathsf{A}\eta m(\eta)$, где $\eta$ — какая-нибудь переменная, не входящая в $m(x)$. Теперь мы обосновываем вывод

$$\frac{S \to m(x)}{S \to A\eta m(\eta)}$$

ссылкой на правило $A_+$, так как $x$ не входит в $S$, а вывод

$$\cfrac{\cfrac{m(x) \to U,\ p(x)}{\mathsf{A}\eta m(\eta) \to U,\ p(x)}}{\mathsf{A}\eta m(\eta) \to U,\ \mathsf{A}\xi p(\xi)}$$

— ссылкой на последовательное применение правил $A_-$ и $A_+$, так как $x$ не входит ни в $\mathsf{A}\eta m(\eta)$, ни в $U$. Совершенно аналогично разбирается случай, когда в исходном выводе применяется правило $E_-$.

Чтобы завершить теперь доказательство теоремы Крэйга, мы предположим, что даны такие $p$ и $q$, что $p \models q$. Без ограничения общности можно предположить, что $p$ и $q$ — предваренные формулы и что, следовательно, $p \to q$ есть общезначимая предваренная секвенция. По теореме Эрбрана — Генцена существует вывод секвенции $p \to q$ с помощью одних только кванторных правил из бескванторной общезначимой секвенции $S \to T$. Пусть $S = (s_1, \ldots, s_m)$ и $T = (t_1, \ldots, t_n)$. По теореме Крэйга для бескванторных формул, которую мы уже доказали, существует такая формула $m$, содержащая только символы отношений, входящие как в $S$, так и в $T$, что $\bigwedge s_i \models m$ и $m \models \bigvee t_j$. По доказанной выше лемме существуют формула $m'$ и выводы с помощью одних только кванторных правил секвенции $p \to m'$ из $S \to m$ и секвенции $m' \to q$ из $m \to T$. Из определения $m$ следует, что секвенции $S \to m$ и $m \to T$ общезначимы, откуда в свою очередь следует, что выводимые из них секвенции $p \to m'$ и $m' \to q$ также общезначимы. Следовательно, $p \models m'$ и $m' \models q'$. Наконец, из того, что выводы секвенции $p \to m$ из $S \to m$ и секвенции $m \to q$ из $m \to T$ производятся с помощью одних только кванторных правил, вытекает, что $p$, $m'$ и $q$ содержат соответственно в точности те же символы отношений, что $S$, $m$ и $T$. Отсюда следует, что $m'$ не содержит никаких символов отношений, не входящих одновременно в $p$ и $q$.

### Упражнения

1. Вхождение какого-либо символа в формулу будем называть *положительным* или *отрицательным* в зависимости от того, четно или нечетно число начинающихся с символа N подформул, содержащих это вхождение. Покажите, что теорему Крэйга можно усилить, потребовав, чтобы произвольный символ отношения входил положительно в $m$ в том и только в том случае, когда он входит положительно как в $p$, так и в $q$, и аналогично для отрицательных вхождений.

2. Покажите, что формула $p = p(r)$ эквивалентна формуле с одними только положительными вхождениями символа отношения $r$ ранга $n$ в том и только том случае, когда $p$ возрастает относительно $r$, т. е. когда

$$\mathsf{A}\xi_1 \ldots \mathsf{A}\xi_n (r\xi_1 \ldots \xi_n \supset r'\xi_1 \ldots \xi_n) \models p(r) \supset p(r').$$

3. Заметим, что если $\equiv$ есть конгруэнция на алгебре $A$, то имеет место $\mathsf{A}\xi\mathsf{A}\eta(\xi = \eta \supset \xi \equiv \eta)$. Докажите *теорему о гомоморфизме*, согласно которой формула $p$ языка $L$ с символом $=$ и функциональными символами, но без других символов отношений, эквивалентна формуле, содержащей только положительные вхождения символа $=$, в том и только в том случае, когда из того, что $p$ верна на алгебре $A$, следует, что она верна также на каждой факторалгебре $[A]$.





## Диагональные рассуждения и парадоксы

В основе гёделевского доказательства неполноты арифметики лежит так называемое *диагональное рассуждение*. Перед тем как изложить в общих чертах рассуждение Гёделя, поговорим о диагональных рассуждениях вообще.

Самый простой и известный пример использования диагонального рассуждения дает канторовское доказательство несчетности множества действительных чисел. В этом доказательстве показано, что никакая последовательность $r_1, r_2, \ldots$ действительных чисел (занумерованных целыми положительными числами) не содержит *всех* действительных чисел. В самом деле, если дана любая такая последовательность, то мы можем положить $a_i = 7$ для каждого целого положительного числа $i$, если $i$-я по порядку цифра после запятой в десятичном разложении числа $r_i$ отлична от 7, и $a_i = 4$, если эта цифра есть 7. В таком случае число, десятичное разложение которого есть $0, a_1 a_2 \ldots$, отлично от всех чисел нашей последовательности.

Точно такое же рассуждение в более общем контексте мы встречаем в теореме Кантора о том, что множество $T$ всех подмножеств произвольного множества $S$ имеет бóльшую мощность, чем само множество $S$. Здесь нам нужно показать, что никакое отображение $f$ множества $S$ в множество $T$ не отображает $S$ на все множество $T$. Взяв произвольное $f$, вводим в рассмотрение множество $U$, определяя его как множество всех таких элементов $s$ множества $S$, для которых $s$ не принадлежит множеству $f(s)$. В таком случае $U$ не является $f(u)$ (т. е. результатом применения отображения $f$ к элементу $u$) ни для какого $u$ из $S$, так как $u \in U$ тогда и только тогда, когда $u$ не принадлежит $f(u)$.

Если мы попытаемся применить этот результат к универсальному множеству $S$, т. е. к множеству, которому принадлежит любой объект, мы получим множество $T$, имеющее бóльшую мощность, чем $S$, что противоречит только что сформулированному определению универсального множества. Еще более простой вид это рассуждение принимает в парадоксе Рассела. Определим $U$ как множество всех таких множеств $X$, что $X$ не есть элемент $X$. В таком случае $U$ есть элемент $U$ тогда и только тогда, когда $U$ не есть элемент $U$.

Парадокс Рассела — простейший из парадоксов теории множеств. С его открытием стало ясно, что нам придется как-то ограничить использование тех способов рассуждений, посредством которых этот парадокс был получен. Открытие это показало полную обоснованность требований более тщательного изучения тех логических предпосылок, из которых исходят математики в своих выводах. И хотя большинство математиков, вообще не склонных пользоваться столь экстравагантными, по их мнению, методами рассуждений, не проявляли особой тревоги по поводу парадоксов, было предложено несколько точных формулировок лежащих в основании математики принципов, свободных, по распространенному мнению, от противоречий. К сожалению, как мы скоро увидим, на осуществление выдвинутой Гильбертом программы безотносительного к каким бы то ни было допущениям доказательства непротиворечивости любой такой теории у нас не остается ни малейшей надежды.

Самые древние из известных парадоксов носят скорее семантический, нежели математический характер. Одна из версий так называемого парадокса лжеца состоит в приписываемой Эпимениду фразе: *Я лгу*. Таким образом, Эпименид лжет в том и только том случае, когда он не лжет. Трудность здесь связана не с математикой, а с использованием языка. Совершенно справедливо указывалось, что затруднение возникает из-за так называемой самоотносимости предложения: предложение Эпименида относится к самому себе. Но сама по себе констатация самоотносимости недостаточна — как и в случае теории множеств, нам нужна точная теория языка, в котором не могли бы больше появляться противоречия.

Парадокс лжеца удобнее рассматривать в несколько видоизмененной форме: *Это предложение ложно*. Может создаться впечатление, что самоотносимость, связанная с указательным местоимением *это*, не позволяет приписать рассматриваемому предложению точного смысла. Однако в данном случае дело обстоит не так. С помощью остроумного диагонального рассуждения Гёдель показал, что если допустить в языке $L$ формулы $p$, выражающие свойства предложений этого языка, то можно построить предложение $s$, выражающее, что само это предложение $s$ обладает некоторым свойством $P$. Основная трудность, связанная с парадоксами типа парадокса лжеца, заключается, как показал Тарский, в употреблении слова *ложно*. У нас нет достаточно убедительных оснований считать, что любая формула языка $L$, выражающая свойство предложений этого языка, непременно должна быть истинной или ложной.

Главное в рассуждении Гёделя — замена слова *ложное* на слово *недоказуемое*, в результате которой мы получаем предложение: *Это предложение недоказуемо*. В разумно устроенном языке выразимо понятие доказуемости формул этого языка и можно сформулировать некоторое предложение $s$, утверждающее свою собственную недоказуемость. Это предложение истинно в том и только том случае, когда оно недоказуемо. Если считать, что всякое доказуемое предложение истинно, то мы придем к выводу, что предложение $s$ истинно, но недоказуемо.





## Гёделевы номера

Для того чтобы описать рассуждение Гёделя, нам понадобится язык $L$, в котором мы смогли бы говорить о самом этом языке или хотя бы о чем-то, достаточно похожем на этот язык. Гёдель решает эту задачу, переводя $L$ в некоторый числовой код, причем перевод этот происходит таким образом, что все существенные синтаксические свойства выражений переходят в элементарно арифметические (в некотором разумном смысле) свойства их числовых кодов. Язык $L$ должен в таком случае обладать достаточно богатыми выразительными средствами для формулировки этих свойств и аксиомами, гарантирующими, что эти выражения в любой модели имеют нужное значение.

Если мы сопоставляем символам языка $L$ различные натуральные числа, то множество этих символов непременно должно быть счетным. Если мы хотим на языке $L$ формулировать и решать арифметические задачи, нам будет удобно ввести в $L$, кроме обычных связок и бесконечного множества переменных, еще символы $=$, $+$, $\times$, $\bar{0}$ и $\bar{1}$, обозначающие соответственно равенство, сложение, умножение, нуль и единицу. Нам будет также удобно считать, что $L$ содержит конечное множество $\mathsf{F}=(f_1, \ldots, f_f)$ функциональных символов и конечное множество $\mathsf{R}=(r_1, \ldots, r_r)$ символов отношений. Припишем символам языка $L$ некоторый фиксированный порядок:

$$\mathsf{0},\ \mathsf{1},\ \mathsf{N},\ \mathsf{C},\ \mathsf{D},\ \mathsf{A},\ \mathsf{E},\ =,\ +,\ \times,\ \bar{0},\ \bar{1},$$
$$f_1, \ldots, f_f,\ r_1, \ldots, r_r,\ v_1,\ v_2, \ldots .$$

Пусть $\alpha$ — функция, отображающая это множество (при данном расположении его элементов) в множество целых положительных чисел (расположенных в порядке возрастания). Определим теперь функцию $\beta$, сопоставляющую каждому выражению $e=s_1 \ldots s_n$ (где $s_i$ суть символы) число

$$\beta[e]=2^{\alpha[s_1]}3^{\alpha[s_2]} \ldots p_n^{\alpha[s_n]},$$

где $2, 3, \ldots, p_n$ — первые $n$ простых чисел. Самым существенным свойством этой функции является то, что она сопоставляет различные номера различным выражениям, причем числа $n$ и $\alpha[s_i]$ легко вычисляются по данному $\beta[e]$. Поскольку мы захотим говорить о конечных последовательностях $E=(e_1, \ldots, e_n)$ выражений — скажем, о доказательствах, — мы повторно применим тот же прием, определяя на множестве выражений функцию $\gamma$, полагая

$$\gamma[E]=2^{\beta[e_1]}3^{\beta[e_2]} \ldots p_n^{\beta[e_n]}.$$

Для последовательности $E$, состоящей из единственного члена $e$, мы полагаем по определению $\gamma[e]=\gamma[E]$,





а для выражения $e$, состоящего из единственного символа $s$, полагаем $\gamma[s]=\gamma[e]$. Числа $\gamma[s]$, $\gamma[e]$ и $\gamma[s]$ мы будем называть *гёделевыми номерами* символа $s$, выражения $e$ и последовательности $E$.

## Выразимость и теорема Тарского

Мы будем рассматривать здесь теории $T$, формулируемые на языке $L$ и задаваемые посредством разрешимого множества $A$ аксиом — разрешимого в том смысле, что для любой формулы $p$ разрешима задача: принадлежит ли $p$ множеству $A$. Мы будем предполагать, что $A$ обязательно включает в себя множество $A_0$ аксиом логики предикатов с равенством, а также множество $A_1$, состоящее из следующих шести аксиом:

$$v_1+\bar{0}=v_1, \quad v_1+(v_2+\bar{1})=(v_1+v_2)+\bar{1},$$
$$v_1\times\bar{0}=\bar{0}, \quad v_1\times(v_2+\bar{1})=(v_1\times v_2)+v_1,$$
$$v_1+\bar{1}\neq\bar{0}, \quad v_1+\bar{1}=v_2+\bar{1}\supset v_1=v_2.$$

При этом $A$ может содержать и другие аксиомы. Например, $A$ может содержать определения, фиксирующие интерпретацию остальных функциональных символов и символов отношений в терминах символов $=$, $\bar{0}$, $\bar{1}$, $+$ и $\times$. Скажем, пара аксиом $f(x, \bar{0})=\bar{1}$, $f(x, y+\bar{1})=f(x, y)\times x$ может служить *рекурсивным определением*, придающим функциональному символу $f$ значение $f(x, y)=x^y$.

Начиная с этого момента мы будем употреблять термин *истинное*, понимая истинность как общезначимость в *стандартной модели*, областью которой является множество $N$ натуральных чисел и в которой символы $=$, $\bar{0}$, $\bar{1}$, $+$ и $\times$ понимаются в их обычном смысле.

Для каждого $n\in N$, $n>1$, мы вводим сокращение $\bar{n}=(\ldots(\bar{1}+\bar{1})+\ldots+\bar{1})$ ($n$ символов $\bar{1}$). Пусть $\bar{N}$ есть множество термов $\bar{0}$, $\bar{1}$, $\bar{2}, \ldots$ языка $L$. Если $\varphi$ — произвольная модель теории $T$, то из $A_1$ по индукции можно вывести, во-первых, что отображение $n$ в $\varphi\bar{n}$ индуцирует взаимно-однозначное отображение $N$ на

$\varphi\overline{N}$ и, во-вторых, что это отображение переводит операции $+$ и $\times$, определенные на множестве $N$, в операции $\varphi(+)$ и $\varphi(\times)$, определенные на множестве $\varphi\overline{N}$. Наличие этого изоморфизма позволяет нам отождествить, не опасаясь путаницы, $\varphi\overline{N}$ с $N$ и писать $n$ вместо $\varphi\overline{n}$, $+$ вместо $\varphi(+)$ и $\times$ вместо $\varphi(\times)$.

Свойство $P(x_1, \ldots, x_n)$, относящееся к натуральным числам, мы будем называть *выразимым* в теории $T$, если в языке $L$ существует такая формула $p = p(v_1, \ldots, v_n)$, что $P(m_1, \ldots, m_n)$ для всех $m_1, \ldots, m_n$ из $N$ истинно тогда и только тогда, когда истинна $p(\overline{m}_1, \ldots, \overline{m}_n)$. Свойство $P$, относящееся к символам, выражениям или к последовательностям выражений, называется выразимым, если выразимо соответствующее свойство, относящееся к гёделевым номерам этих символов, выражений или последовательностей выражений.

То обстоятельство, что все введенные нами синтаксические понятия — такие, как переменная, терм, формула и предложение, — выразимы, должно быть ясно из соображений общего характера. В самом деле, мы ведь можем выразить соответствующее каждому из этих понятий условие, налагаемое в соответствии с его определением на гёделевы номера, в обычных арифметических обозначениях, и, чтобы перевести это условие на язык $L$, нам надо лишь потребовать, чтобы множество $A$ включало рекурсивные определения всех арифметических функций (например, $x^y$), используемых при этом выражении понятий. Мы предположим также, что множество $A$ аксиом разрешимо; после того как мы дадим точное определение разрешимости, мы увидим, что из сказанного вытекает выразимость свойства быть аксиомой. Теперь уже ясно, что свойство быть доказательством (точнее, свойство последовательности $E$ формул быть доказательством формулы $p$) также выразимо.

Мы можем, следовательно, считать, что язык $L$ содержит некоторую конкретную формулу $b(v_1, v_2)$, такую, что для любых двух натуральных чисел $m$ и $n$ формула $b(\overline{m}, \overline{n})$ истинна тогда и только тогда, когда $m$ есть номер доказательства формулы, имеющей номер $n$. Заметим тут же, что формула $\mathsf{E}v_2 b(v_2, v_1)$ выражает свойство (формулы с номером $v_1$) быть теоремой. Мы вправе также предположить, что $L$ содержит некоторую конкретную формулу $s(v_1, v_2) = v_3$, такую, что формула $s(\overline{m}, \overline{n}) = \overline{q}$, где $m = \gamma[l]$, а $n = \gamma[p(v_1)]$, истинна тогда и только тогда, когда $q = \gamma[p(\overline{m})]$.





Имея теперь в распоряжении весь этот аппарат, обратимся вновь к парадоксу лжеца. Допустим, что $L$ содержит, кроме упомянутой выше формулы $s(v_1, v_2) = v_3$, формулу $w(v_1)$, выражающую свойство быть истинной формулой. Пусть $p(v_1) = \rightharpoondown w(s(v_1, v_1))$, и пусть $m = \gamma[p(v_1)]$. Заметим, что $s(\overline{m}, \overline{m})$ есть номер формулы, полученной подстановкой терма $\overline{m}$ вместо переменной $v_1$ в формулу, имеющую номер $m$, т. е. в формулу $p(v_1)$, так что $s(\overline{m}, \overline{m}) = \gamma[p(\overline{m})]$. Итак, формула $p(\overline{m}) = \rightharpoondown w(s(\overline{m}, \overline{m}))$ истинна тогда и только тогда, когда формула, имеющая номер $s(\overline{m}, \overline{m})$, не является истинной, т. е. когда не истинна формула $p(\overline{m})$. Это противоречие показывает, что $L$ не может содержать одновременно формул $s(v_1, v_2) = v_3$ и $w(v_1)$. Нами доказана, таким образом, следующая теорема:

Теорема Тарского. *Если теория $T$ такова, что в ней имеется формула $s(v_1, v_2) = v_3$, выражающая подстановку, то свойство быть истинной формулой теории $T$ не выразимо в $T$.*

В формулировке этой теоремы на теорию $T$ наложено весьма слабое условие. Мы могли бы без особого труда построить в явном виде формулу $s(v_1, v_2) = v_3$ и добавить к $A_0$ и $A_1$ конечное множество $A_2$ рекурсивных определений всех вспомогательных арифметических функций, фигурирующих в описании $s(v_1, v_2)$. Тогда мы придем к выводу, что если $A_0 \cup A_1 \cup A_2 \subseteq T$, то понятие истинности формулы не выразимо в $T$.

Вывод, к которому приводит теорема Тарского, не является неожиданным с интуитивной точки зрения; трудно представить себе, каким образом могло бы удаться синтаксически выразить в рамках некоторой теории семантическое понятие быть истинной формулой этой теории. Предпринятый здесь анализ этого вопроса решает, таким образом, недоуменные вопросы, которые могли бы возникнуть в связи с парадоксом лжеца.

## Теорема Гёделя о неполноте

Мы получим вначале слабую форму теоремы о неполноте, а затем уже и сильную форму. Предположим снова, что в числе аксиом, входящих в множество $A$, имеются арифметические аксиомы, дающие в терминах $\overline{0}$ и $\overline{1}$ рекурсивные определения операций сложения и умножения; пусть $s(v_1, v_2)=v_3$ и $b(v_1, v_2)$ выражают в $T$ те же свойства, что и в предыдущем разделе.

Теорема о неполноте. *Если все формулы теории T обозначимы, то она неполна.*

Доказательство снова проводится посредством диагонального рассуждения; однако теперь вместо формулы $w(v_1)$ мы возьмем формулу $t(v_1) = \mathsf{E} v_2 b(v_2, v_1)$, выражающую, как мы знаем, свойство доказуемости. Если положить по определению $p(v_1) \rightleftharpoons \rightarrow t(s(v_1, v_1))$ и $m=\gamma[p(v_1)]$, то, как и ранее, $s(\overline{m}, \overline{m}) = \gamma[p(\overline{m})]$. Значит формула $p(\overline{m})$ истинна и только тогда, когда $s(\overline{m}, \overline{m})$ не является номером доказуемой формулы, т. е. в том и только том случае, когда $p(\overline{m})$ недоказуема. Таким образом, если бы $p(\overline{m})$ была доказуема, она не была бы истинной, вопреки предположению о теории $T$; поэтому мы приходим к заключению, что формула $p(\overline{m})$ недоказуема, но истинна. Наконец, так как $p(\overline{m})$ истинна, то $\rightarrow p(\overline{m})$ — не истинная формула и, в силу предположения о теории $T$, $\rightarrow p(\overline{m})$ — также недоказуемая формула.

Следствие. *Теория $T'$, включающая все истинные формулы арифметики, неразрешима.*

Если бы $T'$ была разрешимой, мы могли бы аксиоматизировать ее, взяв в качестве множества $A$ аксиом само множество $T'$. Но по теореме о неполноте $T'$ неполна, а между тем как теория, определенная посредством единственной стандартной модели, непременно должна быть полной.

В двух теоремах настоящего раздела заключается основное интуитивное содержание утверждения, что обычная арифметика не является ни разрешимой, ни аксиоматизируемой. Следует, однако, заметить, что фигурирующее в обеих теоремах понятие истинности (общезначимости) придает им семантическую окраску. Ниже мы получим уточненные формулировки обеих теорем, носящие уже чисто синтаксический характер.





## Разрешимость и теорема Чёрча

Рассмотрим снова формулу $p(v_1, \ldots, v_n)$ языка $L$, выражающую некоторое свойство $P(m_1, \ldots, m_n)$ натуральных чисел. Мы будем предполагать, что $p$ — *определенная* формула, т. е. для произвольных натуральных чисел $m_1, \ldots, m_n$ формула $p(\overline{m}_1, \ldots, \overline{m}_n)$ доказуема в том и только том случае, когда она истинна, и то же условие выполняется для отрицания этой формулы. Для произвольных данных чисел $m_1, \ldots, m_n$ либо сама $p(\overline{m}_1, \ldots, \overline{m}_n)$, либо ее отрицание истинно, так что одна из этих формул доказуема. Перебирая в алфавитном порядке все доказательства, мы наверняка дойдем до доказательства либо самой этой формулы, либо ее отрицания и решим, таким образом, верно или неверно свойство $P(m_1, \ldots, m_n)$. Пусть, обратно, свойство $P$ разрешимо в интуитивном смысле. Тогда существует алгорифм (схема вычисления), применимый к множеству аргументов $m_1, \ldots, m_n$ и дающий ответ на вопрос, истинно $P(m_1, \ldots, m_n)$ или ложно. Этот алгорифм должен тогда быть выразимым в $T$ посредством некоторой формулы $p(v_1, \ldots, v_n)$, такой, что $p(\overline{m}_1, \ldots, \overline{m}_n)$ выражает, что $P(m_1, \ldots, m_n)$ истинно, и давать при этом доказательство либо для формулы $p(\overline{m}_1, \ldots, \overline{m}_n)$, либо для ее отрицания.

На основе этих содержательных рассмотрений мы теперь назовем свойство $P$ натуральных чисел *разрешимым*, если оно выразимо в некоторой конечно аксиоматизируемой теории $T$ посредством определенной формулы $p$.

Большая часть рассматривавшихся нами синтаксических понятий в интуитивном смысле разрешима, так что у нас есть основания ожидать, что соответствующие им (т. е. выражающие их) формулы являются определенными. Это относится, в частности, к формулам $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$. Полное доказательство этого факта потребовало бы явного задания этих формул; мы наметим здесь лишь наиболее принципиальные шаги такого доказательства.

Вхождение какого-либо квантора в формулу называют *ограниченным*, если этим вхождением начинается подформула вида $\mathsf{A}x[x \leqslant t \supset p]$ или $\mathsf{E}x[x \leqslant t \wedge p]$ ($x \leqslant y$ есть сокращение для $\mathsf{E}z(x+z=y)$), где $t$ — терм, в который не входит свободно $x$. Представляется интуитивно правдоподобным, что разрешимое свойство, выразимое формулой $p(v_1, \ldots, v_n)$ вида $\mathsf{A}xq(x, v_1, \ldots, v_n)$ или вида $\mathsf{E}xq(x, v_1, \ldots, v_n)$, где $q$ — определенная формула, должно быть выразимым с помощью ограниченных кваторов. (Для нашего случая это можно показать, если в явной форме выписать соответствующие выражения.) В частности, $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$ могут быть заменены эквивалентными им формулами, содержащими лишь ограниченные кванторы. Рассмотрим теперь формулу

$$p(v_1, \ldots, v_n) = \mathsf{A}x[x \leqslant t(v_1, \ldots, v_n) \supset q(x, v_1, \ldots, v_n)],$$

где $x$ не входит свободно в $t$ и формулы $t(v_1, \ldots, v_n) = v_{n+1}$ и $q(v_1, \ldots, v_n)$ — определенные. Если $m_1, \ldots, m_n$ заданы, то решение $m$ уравнения $t(\overline{m}_1, \ldots, \overline{m}_n) = \overline{m}$ может быть найдено посредством конечного перебора возможностей, а формула $p(\overline{m}_1, \ldots, \overline{m}_n)$ эквивалентна, очевидно, конъюнкции

$$q(\overline{0}, \overline{m}_1, \ldots, \overline{m}_n) \wedge \ldots \wedge q(\overline{m}, \overline{m}_1, \ldots, \overline{m}_n).$$

Так как формула $q$ определенна, то определенна и формула $p$. В случае квантора существования рассуждение проводится в точности так же. Из сказанного видно, что формула, все кванторы в которой ограниче-





ны, определенна, и, следовательно, определенными являются формулы $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$.

Нет никаких оснований рассчитывать найти такую арифметическую функцию $f(v_1)$, которая по заданному гёделевому номеру $m$ теоремы давала бы длину наикратчайшего доказательства этой теоремы. Иными словами, не видно, каким образом можно было бы заменить первый квантор в формуле $t(v_1) = \mathsf{E}v_2 b(v_2, v_1)$ ограниченным квантором, так что возникает подозрение, что $t(v_1)$ не является определенной, а следовательно, множество $T$ теорем неразрешимо. И дело обстоит именно так:

Теорема. *Если $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$ — определенные формулы некоторой теории $T$, то $T$ неразрешима.*

Доказательство и здесь проходит по образцу парадокса лжеца. Определяя, как выше, $p(v_1) = \neg t(s(v_1, v_1))$ и $m = \gamma[p(v_1)]$, мы снова получаем, что $p(\overline{m})$ истинна в том и только том случае, когда она недоказуема. С другой стороны, если $t(v_1)$ была бы определенной формулой, мы получили бы, что $p(\overline{m}) = \neg t(s(\overline{m}, \overline{m}))$ истинна в том и только том случае, когда она доказуема, т. е. пришли бы к противоречию.

Теорема Чёрча. *Множество всех общезначимых формул логики предикатов неразрешимо.*

Чтобы доказать это утверждение, мы выберем теорию $T$ как можно более экономным образом. Желая быть уверенным в том, что $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$ — определенные формулы, мы можем потребовать, чтобы язык $L$ содержал различные функциональные символы для вспомогательных функций, используемых при определении этих формул, т. е. попросту потребовать, чтобы в множество $A$ аксиом, кроме аксиом, составляющих множество $A_0 \cup A_1$, входили аксиомы, имеющие вид рекурсивных определений этих функциональных символов, обеспечивающие правильную их интерпретацию. При этом, однако, мы можем считать, что $L$ содержит лишь конечное число функциональных символов и символов отношений и что $A_= = A_0 \cup A_1 \cup A_2$, где $A_2$ конечно. Но если $L$ содержит лишь конечное число функциональных символов и символов отношений, то множество $A_=$ аксиом равенства также можно выбрать конечным. Пусть $a$ — конъюнкция всех формул, входящих в конечное множество $A_= \cup A_1 \cup A_2$. Тогда $A \models p$ равносильно $\models a \supset p$; иными словами, формула $p$ принадлежит $T$ в том и только том случае, когда $a \supset p$ есть общезначимая формула логики предикатов. Следовательно, разрешимость логики предикатов означала бы разрешимость теории $T$, откуда и следует утверждение теоремы Чёрча.

## Недоказуемость непротиворечивости

Прежде всего мы усилим теорему о неполноте, придав ей чисто синтаксическую формулировку.

Положим снова $p(v_1) = \neg \mathsf{E} v_2 b(v_2, s(v_1, v_1))$ и $m = \gamma[p(v_1)]$. Докажем две леммы.

Лемма. *Если $T$ непротиворечива, то $p(\overline{m})$ недоказуема.*

Допустим, что $p(\overline{m})$ доказуема. В таком случае для нее существует доказательство, имеющее некоторый гёделев номер $n$ и, так как $\gamma[p(\overline{m})] = s(\overline{m}, \overline{m})$, то формула $b(\overline{n}, s(\overline{m}, \overline{m}))$, выражающая, что $n$ есть номер доказательства формулы $p(\overline{m})$, истинна. Но так как $b(v_1, v_2)$ — определенная формула, то из этого следует, что формула $b(\overline{n}, s(\overline{m}, \overline{m}))$ доказуема, а значит, и $\mathsf{E} v_2 b(v_2, s(\overline{m}, \overline{m}))$ — доказуемая формула. А так как формула $p(\overline{m})$, являющаяся отрицанием последней формулы, также доказуема, то мы заключаем, что $T$ противоречива.

Теория $T$ называется *ω-непротиворечивой*, если нет такой формулы $q(v_1)$, что $T$ одновременно содержала бы и формулу $\mathsf{E} x q(x)$, и все формулы $\neg q(\overline{n})$, где $n$ пробегает множество $N$. Очевидно, что любая теория, интерпретируемая на области $N$, является ω-непротиворечивой; однако, вообще говоря, ω-непротиворечивость сильнее, чем просто непротиворечивость.





Лемма. *Если $T$ ω-непротиворечива, то $\neg p(\overline{m})$ недоказуема.*

Допустим, что $\neg p(\overline{m})$ доказуема. Так как $T$ непротиворечива, то $p(\overline{m})$ недоказуема и никакое натуральное число $n$ не является гёделевым номером доказательства этой формулы $p(\overline{m})$; иначе говоря, формула $\neg b(\overline{n}, s(\overline{m}, \overline{m}))$ истинна. Но так как $b(v_1, v_2)$ — определенная формула, то из этого следует, что при любом $n$ формула $\neg b(\overline{n}, s(\overline{m}, \overline{m}))$ доказуема. Из ω-непротиворечивости $T$ мы делаем вывод о недоказуемости формулы $\mathsf{E} x b(x, s(\overline{m}, \overline{m}))$, а потому и формула $\neg p(\overline{m}) = \neg\neg \mathsf{E} x b(x, s(\overline{m}, \overline{m}))$ недоказуема, что противоречит принятому допущению.

Таким образом, если $T$ ω-непротиворечива, то не доказуемы ни $p(\overline{m})$, ни $\neg p(\overline{m})$, а следовательно, $T$ неполна. Следует для полноты картины отметить, что Россеру удалось, усовершенствовав приведенное рассуждение, усилить этот результат, получив то же заключение, исходя из более слабого предположения о простой непротиворечивости (а не ω-непротиворечивости) теории $T$.

Теорема о неполноте (синтаксическая форма). *Если $T$ есть теория, в которой $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$ — определенные формулы, то $T$ неполна.*

Этот результат можно уточнить, определив $T$ (как выше) посредством некоторого конкретного множества аксиом.

В заключение мы приведем еще одну теорему Гёделя, представляющую собой, быть может, самый значительный его вклад в основания математики.

Теорема. *Пусть $T$ — теория, в которой $b(v_1, v_2)$ и $s(v_1, v_2) = v_3$ — определенные формулы. Тогда $T$ содержит предложения, выражающие непротиворечивость $T$, но ни одно такое предложение недоказуемо в $T$.*

Поскольку $\gamma[\mathsf{O}] = 4$, то предложение $c = \neg \mathsf{E} x b(x, \overline{4})$ выражает то обстоятельство, что предложение $\mathsf{O}$

недоказуемо, т. е. что $T$ непротиворечива. С помощью первой из доказанных выше лемм мы покажем, что непротиворечивость теории $T$ влечет недоказуемость формулы $p(\overline{m})$, а следовательно, и истинность $p(\overline{m})$, утверждающей недоказуемость $p(\overline{m})$. Если $d$ есть гёделев номер формулы $c \supset p(\overline{m})$, то, так как эта формула имеет доказательство, имеющее некоторый гёделев номер $h$, формула $b(\overline{h}, \overline{d})$ истинна при некотором натуральном $h$. Если бы $c$ была доказуема, то $b(k, \overline{\gamma[c]})$ была бы истинна при некотором $k$, из чего легко следовало бы, что некоторое число $j$ является гёделевым номером доказательства формулы $p(\overline{m})$. Но $T$ непротиворечива, так что из предположения об определенности в $T$ формулы $b(v_1, v_2)$ следует недоказуемость формулы $p(\overline{m})$, т. е. мы пришли к противоречию.

# Литература


Church A., Introduction to Mathematical Logic, I, Princeton, 1956. (Русский перевод: Чёрч А., Введение в математическую логику, т. I, М., ИЛ, 1960.)

Davis M., Computability and Unsolvability, New York, 1958. (Русский перевод: Дэвис М., Вычислимость и неразрешимость, М., изд-во «Наука», в печати.)

Halmos P. R., Algebraic Logic, New York, 1962.

Henkin L., The Completeness of the First-order Functional Calculus, *J. Symbolic Logic*, **14** (1949), 159—166.

Henkin L., Tarski A., Cylindric Algebras, Proc. Symposia Pure Math., v. 2, Providence, 1961, 83—113.

Heyting A., Intuitionism, Amsterdam, 1956. (Русский перевод: Гейтинг А., Интуиционизм, М., «Мир», 1965.)

Kleene S. C., Introduction to Metamathematics, New York, 1952. (Русский перевод: Клини С. К., Введение в метаматематику, М., ИЛ, 1957.)

Kripke S. A., Semantical Analysis of Modal Logic, I: Normal Modal Propositional Calculi, *Zeitschrift Math. Logik Grundlagen Math.*, **9** (1963), 67—96.

Lorenzen P., Metamathematik, Mannheim, 1962.

Nagel E., Newman J. R., Gödel's Proof, London, 1959.

Rasiowa H., Sikorski R., On the Gentzen Theorem, *Fundamenta Math.*, **58** (1960), 59—69.

Robinson A., Introduction to Model Theory and the Metamathematics of Algebra, Amsterdam, 1963. (Русский перевод: Робинсон А., Введение в теорию моделей и метаматематику алгебры, М., «Наука», 1967.)

Tarski A., The Semantic Conception of Truth, *Philos. Phenomenological Research*, **4** (1944), 13—47.

Tarski A., A Decision Method for Elementary Algebra and Geometry, Berkeley and Los Angeles, 1951.

Tarski A., Mostowski A., Robinson R. M., Undecidable Theories, Amsterdam, 1953.

Гильберт Д. и Аккерман В., Основы теоретической логики, М., ИЛ, 1947.

Гудстейн Р., Математическая логика, М., ИЛ, 1961.

Мальцев А. И., Алгоритмы и рекурсивные функции, М., «Наука», 1966.

Новиков П. С., Элементы математической логики, М., Физматгиз, 1959.

Тарский А., Введение в логику и методологию дедуктивных наук, М., ИЛ, 1948.

# Именной указатель



# Указатель терминов

# Содержание




Р. ЛИНДОН

**ЗАМЕТКИ ПО ЛОГИКЕ**

Редактор *Н. Н. Щербиновская* Художник *А. В. Шипов*
Художественный редактор *П. Ф. Некундэ*
Технический редактор *Т. В. Чечик*

Сдано в производство 12/IV 1968 г. Подписано к печати 4/XI 1968 г.
Бумага № 3 $84\times108^{1}/_{32}$=2 бум. л., 6,72 усл. печ. л. Уч.-изд. л. 5,94
Изд. № 1/4617. Цена 41 коп. Зак. 1253
Темплан 1968 г. изд-ва «Мир», пор. № 33

ИЗДАТЕЛЬСТВО „МИР", Москва, 1-й Рижский пер., 2

Ленинградская типография № 2 имени Евгении Соколовой
Главполиграфпрома Комитета по печати при Совете Министров СССР.
Измайловский проспект, 29