Санкт-Петербургский Государственный Институт
Точной Механики и Оптики (Технический Университет)
Факультет Информационных Технологий и Программирования
Кафедра Компьютерных технологий

М. А. Коротков Е. О. Степанов

Основы формальных логических языков

Санкт-Петербург
2003

УДК 510.62, 510.63, 510.65, 510.675, 510.676.

Коротков М. А., Степанов Е. О. Основы формальных логических языков. СПб: СПб ГИТМО (ТУ), 2003. 84с.

Данное учебное пособие посвящено основам формальных логических языков. В нем дается краткое изложение языков логики первого и второго порядков, элементов теории доказательств, теории моделей и формальной теории множеств. Пособие основано на курсе лекций, читаемом на кафедре Компьютерных технологий Санкт-Петербургского Государственного Института Точной Механики и Оптики.

Пособие предназначено для студентов компьютерных и математических специальностей.

Утверждено к печати Ученым Советом факультета Информационных Технологий и Программирования, протокол №5 от 09.01.03.

ISBN 5-7577-0122-6

© Санкт-Петербургский Государственный Институт Точной Механики и Оптики (Технический Университет), 2003.

© М. А. Коротков, Е. О. Степанов, 2003.

Оглавление

1 Введение

Формальная логика. Дать краткое, но исчерпывающее определение той или иной науки – задача, как правило, не простая. В особенности это относится к таким наукам, которые, как, например, математика или физика, содержат в себе большое число различных специальных дисциплин. В значительной мере относится это и к логике, которая фактически пронизывает всю современную математику и информатику, а также является фундаментом многочисленных естественнонаучных и гуманитарных дисциплин, от "абстрактных", таких как философия, до "прикладных", таких как юриспруденция. Поэтому мы попробуем подойти к понятию о предмете современной логики, не претендуя ни на полноту, ни на точность.

Общепринятым является понимание логики как науки о правильном умозаключении ("логическом рассуждении"). Чтобы понять смысл этого определения, стоит конкретизировать, что такое умозаключение, а главное, что следует понимать под правильностью. Существует только два способа, которыми человек приобретает новые знания – в результате опыта и путем умозаключения. При этом первым способом получена только малая часть всех используемых людьми знаний. Заметим, что всякое рассуждение основывается на опытных фактах ("посылках"), которые сами по себе могут соответствовать или не соответствовать действительности. Однако истинность или ложность посылок никак не влияют на правильность рассуждения.

Вот очень простой, но показательный пример. Умозаключение "страус – птица, все птицы имеют крылья, следовательно страус имеет крылья" несомненно правильное, а все использованные посылки соответствуют действительности, поэтому истинным является и заключение. А вот в умозаключении "кит – морская рыба, все рыбы в море селедки, следовательно кит – селедка" обе посылки ложны, заключение также ложно, но само рассуждение следует признать правильным, ибо оно ничем, кроме входящих в него опытных фактов, не отличается от предыдущего. По сути дела, оба рассуждения – это всего лишь две разные модификации одной и той же логической конструкции "y обладает свойством P, все x, имеющие свойство P, имеют и свойство Q, следовательно y имеет свойство Q". Здесь уже нет никаких опытных фактов, на их месте осталась только абстрактная конструкция, которая является общепризнанно правильной, и мы очень часто используем ее в самых разных логических рассуждениях.

Это был, конечно, только простой пример, а на практике проверить правильность сложных умозаключений можно только сведением их к последовательности таких вот элементарных общепризнанно правильных рассуждений (в этом и состоит процесс доказывания заключения из заданных посылок). Таким образом, правильность умозаключений вводится и проверяется совершенно фор-

мально, без какой-либо связи с истинностью входящих в него посылок, т.е. исключительно с точки зрения структуры рассуждения. Поэтому логику, изучающую правильные умозаключения, часто называют формальной логикой (иногда приходится встречать название логистика). С практической точки зрения самое важное свойство такой формальной правильности рассуждений заключается в следующем: если нам удалось доказать, пользуясь методами формальной логики, правильность рассуждения, и нам известно из опыта, что все используемые посылки истинны, то мы можем быть уверены в истинности заключения.

Строго говоря, логика несколько шире формальной логики – например, последняя не отвечает на вопросы, какие рассуждения считать "элементарными" и почему. Для ответа на них приходится углубляться в философию и психологию. Однако, как правило, предмет логики ограничивают все-таки именно вопросами формальной логики, так что логика и формальная логика оказываются просто синонимами. Некоторые базовые вопросы относят к философским основаниям логики, хотя граница между логикой и философией весьма размыта. В дальнейшем мы будем заниматься именно формальной логикой, хотя нам придется часто обращаться к ее внелогическим, в т.ч. общефилософским основаниям и выводам.

Символьная и математическая логика. В конце XIX – начале XX века логика, являющаяся одной из наиболее древних наук (по современным представлениям, рождение логики связано с деятельностью софистов в Древней Греции в 4-5 веке до н.э. – именно они создали логику как науку и активно использовали ее, в частности, для обучения ведению судебных споров; к этой же эпохе относится и деятельность первого ученого, систематизировавшего разрозненные логические знания – "отца логики" Аристотеля) пережила невиданную по своим масштабам и значению революцию. Вначале преобразования казались несущественными и заключались в активном использовании в логических исследованиях символьной записи. Разработанная в 40-70х гг. прошлого века Дж. Булем, а затем развитая другими учеными (в основном математиками, в т.ч. Г. Кантором) символьная запись логических рассуждений оказалась очень удобной и быстро завоевала популярность, превратив формальную логику в символьную логику. Например, рассмотренное выше логическое рассуждение "y обладает свойством P, все x, имеющие свойство P, имеют и свойство Q, следовательно y имеет свойство Q", в современной записи выглядит очень компактно

$$P(y), \forall x(P(x) \to Q(x)) \vdash Q(y).$$

При этом $P(y)$ обозначает "y обладает свойством P", $P(x) \to Q(x)$ обозначает "если x имеет свойство P, то x имеет свойство Q", $\forall x(...)$ обозначает "для всех x верно $(...)$", а $\vdash$ обозначает "доказывает". "Символьная" революция в логике совпала по времени со столь же революционными преобразованиями в математике. Основными вехами этих преобразований было появление созданной

Г. Кантором теории множеств, качественным повышением требований к строгости доказательств, прежде всего в математическом анализе в результате работ К. Вейерштрасса, активным поиском общих теоретикомножественных оснований математического анализа и математики в целом. Возникшие на этом пути трудности оказались принципиальными и потребовали значительной формализации оснований математики с использованием методов символьной логики. В свою очередь, произошедшее таким образом соприкосновение логики и математики привело к их взаимопроникновению настолько, что считавшаяся ранее частью философии логика оказалась пропитанной математическими методами, которые оказались эффективными и в применении к чисто логическим задачам. В результате современная логика полностью базируется на математических методах и часто находит приложение в задачах математики и прикладных математических дисциплин, включающих теоретическую информатику, и является, таким образом, математической логикой. Однако нет никакого смысла в противопоставлении "логики" и "математической логики", так как математическая логика представляет собой современное развитие классической логики, основы которой заложены еще Аристотелем.

Формальные языки. Современная логика изучает *формальные языки*, служащие для выражения логических рассуждений. Используемые для этой цели математические методы пригодны для изучения и значительно более широкого класса формальных языков.

Любой язык, как *естественный* (русский, английский, латинский), так и *формальный* (языки программирования, язык шахматной записи, языки логики предикатов), служит для передачи информации. С этой точки зрения язык представляет собой совокупность знаковой системы (включающей в себя набор символов для передачи текстов и правила написания текстов, называемые *синтаксисом языка*) и набора смыслов, которые можно сопоставить текстам языка, а также правил сопоставления смысла текстам языка, называемых *семантикой языка*. Вопросы синтаксиса, как правило, существенно проще семантических вопросов и гораздо легче поддаются формальному анализу.

Чтобы задать язык, необходимо прежде всего задать его алфавит – множество объектов ("символов"), из которых составляются тексты языка. Алфавитом языка может, вообще говоря, служить произвольное множество. Например, алфавит английского языка состоит из букв латинского алфавита, арабских цифр и знаков пунктуации, письменный язык индейцев майя – из узелков. Также из букв латинского алфавита, арабских цифр и некоторых специальных символов (например, #) состоит алфавит большинства распространенных языков программирования.

Далее мы будем говорить только о *формальных языках*. Пусть задано множество V – алфавит языка. Элементы этого множества мы будем называть *симво-*

лами алфавита. *Цепочками* (*string*) будем называть конечные позиционные наборы символов *алфавита* с учетом порядка следования символов. В дальнейшем мы, как правило, будем иметь дело с довольно распространенной ситуацией, когда символы алфавита представляют собой знаки, которые могут быть записаны на бумаге. В этом случае цепочки символов будем записывать так, как это принято в европейских языках – слева направо в порядке следования символов. Пустая цепочка символов это пустое множество символов. Множество всех цепочек, включая пустую, будем обозначать V^*. *Формальный язык* с алфавитом V это просто заданное подмножество $L \subset V^*$. Элементы этого множества могут называться по-разному для разных языков. Например, элементы языков логики предикатов принято называть формулами, элементы языков программирования – программами, элементы языка шахматной записи – ходами (или записями ходов), а элементы языков, в той или иной мере моделирующих естественные – предложениями или фразами.

Задать формальный язык (т.е. правило, по которому формируется множество $L \subset V^*$) можно по-разному. Чаще всего для этой цели используют *формальные грамматики*. Нас будет интересовать только один весьма распространенный тип формальной грамматики – *контекстно-свободная грамматика*, записываемая в форме Бэкуса-Наура.

Язык и метаязык. Для описания синтаксиса и семантики формального языка мы, как правило, будем пользоваться естественным (в данном случае русским) языком. Например, фраза “Ход e2–e4 состоит в передвижении пешки с поля e2 на поле e4”, является предложением русского языка, объясняющим смысл записи e2–e4 на формальном языке шахматной записи. Использовать для этой же цели можно было бы и другой язык, как естественный, так и формальный, специально предназначенный для описания синтаксиса и семантики данного формального языка. В таком случае будем называть тот язык, который используется для описания данного формального языка, *метаязыком* для последнего, а “описываемый” язык предметным языком. Приставка греческого происхождения “мета”, в прямом переводе означающая “следующий за”, имеет здесь значение “над”.

Стоит отметить, что предметный формальный язык и метаязык, как правило, отличаются друг от друга. Метаязык обычно в некотором смысле богаче, например, его алфавит часто строго содержит алфавит предметного языка. Дело в том, что многие формальные языки, в том числе и те, которые мы будем рассматривать в дальнейшем, недостаточно богаты, чтобы использовать их в качестве метаязыков для себя самих (это или просто невозможно, или по меньшей мере весьма неудобно). При этом все естественные языки достаточно богаты, чтобы с их помощью можно было бы описать их собственную грамматику (“синтаксис”), а также проводить рассуждения о смысле тех или иных фраз этого же языка (т.е. о семантике языка). Например, мы обучаемся русскому языку на

русском (который в процессе обучения служит, таким образом, метаязыком для самого себя. В то же время книжки по обучению формальным языкам, таким как, например, языки программирования, написаны также на естественном (русском, английском и т.п.) языке, а не на самом изучаемом формальном языке (представьте себе, можно ли было бы научиться программировать на C++, если бы соответствующие учебники не были написаны на привычном русском языке). Это, однако, не значит, что никакой формальный язык не может использоваться в качестве метаязыка для себя самого: существуют и такие формальные языки, которые, вовсе не будучи столь же богатыми, как и естественные, в принципе могут быть использованы для "описания себя самих".

2 Языки логики предикатов первого порядка

Языки логики предикатов представляют собой основной класс языков, с которыми приходится иметь дело в формальной логике. Разные языки этого класса используются для описания различных предметных областей. Наибольшее применение в силу ряда причин, которые мы рассмотрим позднее, получили языки логики предикатов первого порядка. Главная их особенность состоит в том, что они достаточно выразительны (например, на языке логики первого порядка можно описать всю математику) и в то же время легко поддаются формальному анализу.

2.1 Алфавит и сигнатура

Алфавит $\mathcal{A}$ любого языка логики предикатов первого порядка состоит из шести подмножеств

$$\mathcal{A} = \mathbf{Const} \cup \mathbf{Func} \cup \mathbf{Pred} \cup \mathbf{Var} \cup \mathbf{Log} \cup \mathbf{Aux},$$

где

- **Const** – множество символов предметных констант,
- **Func** – множество функциональных символов,
- **Pred** – множество предикатных символов,
- **Var** – множество символов предметных переменных,
- **Log** $:= \{\neg, \wedge, \vee, \rightarrow, \exists, \forall\}$ – множество логических символов,
- **Aux** $:= \{,, (,)\}$ –множество вспомогательных символов (запятая и круглые скобки).

Объединение $\sigma = \mathbf{Const} \cup \mathbf{Func} \cup \mathbf{Pred}$ множеств символов предметных констант, функциональных и предикатных символов называется *сигнатурой* языка и определяется той конкретной предметной областью, для описания которой предназначен язык. Язык логики первого порядка, таким образом, определяется своей сигнатурой, поэтому говорят об алфавите и языке сигнатуры σ (если необходимо подчеркнуть зависимость от сигнатуры, ее указывают в верхнем индексе, например, алфавит $\mathcal{A}^\sigma$, язык L^σ).

Как правило, для обозначения символов предметных констант, переменных и функциональных символов принято использовать малые латинские буквы, а для предикатных символов – большие латинские буквы. Кроме того, все функциональные и предикатные символы делятся на *унарные, бинарные, тернарные, n-арные* и т.п. (если символ n-арный, то это значит, что он используется в записи с n аргументами). Множества n-арных функциональных и предикатных символов будем обозначать, соответственно, $\mathbf{Func}^n$ и $\mathbf{Pred}^n$.

Множество логических символов состоит из следующие элементов:

- $\neg$ – символ отрицания (логическое “не”),
- $\wedge$ – символ конъюнкции (логическое “и”),
- $\vee$ – символ дизъюнкции (логическое “или”),
- $\rightarrow$ – символ импликации (логическое “следствие”),
- $\exists$ – квантор существования,
- $\forall$ – квантор всеобщности.

Первые четыре из перечисленных символов (символ отрицания, символ конъюнкции, символ дизъюнкции и символ импликации) называются также логическими связками, оставшиеся — квантор существования и квантор всеобщности — просто кванторами. Иногда определяют языки логики предикатов первого порядка с другими логическими связками, либо с меньшим числом связок – сделать так можно без ущерба для выразительной силы языка, как мы покажем в дальнейшем.

2.2 Синтаксис языка первого порядка

Язык L^σ логики предикатов первого порядка с сигнатурой σ определяется как формальный язык с алфавитом $\mathcal{A}^\sigma$, порождаемый следующей грамматикой (в

форме Бэкуса-Наура):

$$
\begin{array}{lll}
< \text{формула} > & ::= & < \text{атомная формула} > \\
 & & | \ (\neg < \text{формула} >) \\
 & & |(< \text{формула} > \wedge < \text{формула} >) \\
 & & |(< \text{формула} > \vee < \text{формула} >) \\
 & & |(< \text{формула} > \rightarrow < \text{формула} >) \\
 & & |(\exists < \text{переменная} > < \text{формула} >) \\
 & & |(\forall < \text{переменная} > < \text{формула} >), \\
< \text{атомная формула} > & ::= & < n - \text{арный пред. символ} > (< \text{терм} >, ...), \\
< \text{терм} > & ::= & < \text{константа} > \\
 & & | < \text{переменная} > \\
 & & | < n - \text{арный функ. символ} > (< \text{терм} >, ...),
\end{array}
$$

где $< \textit{константа} >$, $< \textit{переменная} >$, $< n - \textit{арный функциональный символ} >$ и $< n - \textit{арный предикатный символ} >$ – произвольные символы из **Const**, **Var**, $\mathbf{Func}^n$ и $\mathbf{Pred}^n$, соответственно.

Элементы L^σ называются *формулами*. Согласно приведенному выше определению, формулы бывают *атомными* и *составными*. Последние, в свою очередь, составляются из атомных формул с помощью логических символов. *Атомная формула* представляет собой предикатный символ с соответствующим количеством аргументов-термов (для n-арного предикатного символа – n термов). Наконец, *терм* языка L^σ это или предметная константа, или выражение, в которое входит функциональный символ и соответствующее число (n для n-арного символа) термов. Это можно выразить и с помощью следующего эквивалентного определения.

Определение 2.1 *(i) Множество термов* $\mathbf{TER}(L^\sigma)$ *языка* L^σ *определяется по следующим правилам:*

- *любой символ предметной переменной или константы является термом;*
- *если* $f \in \mathbf{Func}^n$, *а* $t_1, \ldots, t_n \in \mathbf{TER}(L^\sigma)$, *то* $f(t_1, \ldots, t_n) \in \mathbf{TER}(L^\sigma)$*;*
- *других термов, кроме построенных по приведенным выше правилам, нет.*

(ii) Множество формул L^σ *определяется по следующим правилам:*

- *если* $A \in \mathbf{Pred}^n$, *а* $t_1, \ldots, t_n \in \mathbf{TER}(L^\sigma)$, *то* $A(t_1, \ldots, t_n)$ *– формула, называемая в этом случае атомной формулой;*
- *если* $\mathcal{P}$, $\mathcal{Q}$ *– формулы, то* $(\neg\mathcal{P})$, $(\mathcal{P} \vee \mathcal{Q})$, $(\mathcal{P} \wedge \mathcal{Q})$, $(\mathcal{P} \rightarrow \mathcal{Q})$ *– формулы;*

- *если $\mathcal{P}$ – формула, а x – символ предметной переменной, то $((\forall x)\mathcal{P})$, $((\exists x)\mathcal{P})$ – формулы;*
- *других формул, кроме построенных по приведенным выше правилам, нет.*

Пример 2.1 *Пусть A^1 и B^2 – унарный и бинарный предикатные символы, соответственно, f – бинарный функциональный символ, а c – символ предметной константы, а все остальные малые латинские буквы – символы предметных переменных. Тогда цепочки символов c, x, $f(c,x)$, $f(x,f(c,f(x,x)))$ являются термами, а цепочки символов*

$$A^1(f(c,x)), \qquad B^2(c,f(c,x)), \text{ и}$$

$$(((\forall x)(A^1(x) \wedge A^2(y))) \to ((\forall y)(B^2(c,f(c,c)) \vee A^1(x)))$$

являются формулами.

Упражнения.

1. Докажите, что в условиях предыдущего примера цепочки символов $c(f(A^1(x) \to))$, $(())(c\forall$ не являются ни формулами, ни термами.

2. Докажите следующие теоремы об индукции по структуре термов и формул:

Теорема 2.1 (об индукции по структуре термов) *Пусть* Π *такое подмножество* $\mathbf{TER}(L^\sigma)$, *что*

(i) Π *содержит все предметные константы и переменные;*

(ii) Если Π *содержит* $t_1,\ldots,t_n \in \mathbf{TER}(L^\sigma)$, *то* Π *содержит и* $f(t_1,t_2,\ldots,t_n)$, *где* f *– произвольный* n*-арный функциональный символ.*

Тогда Π *содержит все термы.*

Теорема 2.2 (об индукции по структуре формул) *Пусть* Π *такое подмножество* L^σ, *что*

(i) Π *содержит все атомные формулы;*

(ii) Если $\mathcal{P},\mathcal{Q} \in \Pi$, *то* $(\neg\mathcal{P}),(\mathcal{P}\vee\mathcal{Q}),(\mathcal{P}\wedge\mathcal{Q}),(\mathcal{P}\to\mathcal{Q}) \in \Pi$;

(iii) Если $\mathcal{P} \in \Pi$, *то* $((\forall x)\mathcal{P}),((\exists x)\mathcal{P}) \in \Pi$ *для произвольного символа предметной переменной* x.

Тогда Π *содержит все формулы.*

3. Докажите, что любая формула языка логики предикатов первого порядка содержит одинаковое количество открывающих и закрывающих скобок.

Указание. Воспользуйтесь доказанными теоремами об индукции по структуре термов и формул.

Приоритеты операций. Запись формул можно сократить путем некоторого уменьшения количества ненужных скобок. Для этого введем следующие приоритеты логических символов:

$$Pr(\exists) = Pr(\forall) = Pr(\neg) > Pr(\wedge) > Pr(\vee) > Pr(\rightarrow),$$

где символ $Pr(\mathcal{A})$ обозначает приоритет операции $\mathcal{A}$.

Таким образом, самый высокий приоритет имеют кванторы, далее в порядке убывания приоритета следуют символы отрицания, конъюнкции, дизъюнкции, и, наконец, импликации. С учетом этого правила, например, цепочки символов $\forall x(A^1(x) \rightarrow B^1(x))$ и $\exists x \neg A^2(x,y)$ являются сокращенным обозначением формул $((\forall x)(A^1(x) \rightarrow B^1(x)))$ и $((\exists x)(\neg A^2(x,y)))$, соответственно. Впредь мы будем записывать все формулы в сокращенном виде с использованием введенных приоритетов.

2.3 Свободные и связанные переменные

Определим множество свободных переменных $\mathbf{Free}(\mathcal{P})$ и множество связанных переменных $\mathbf{Bound}(\mathcal{P})$ формулы $\mathcal{P} \in L^\sigma$. Здесь и далее $\mathrm{var}(t)$, $\mathrm{var}(\mathcal{P})$ обозначает множество символов предметных переменных, входящих, соответственно, в терм t и формулу $\mathcal{P}$.

Определение 2.2 *Множество свободных переменных* $\mathbf{Free}(\mathcal{P})$ *и множество связанных переменных* $\mathbf{Bound}(\mathcal{P})$ *формулы* $\mathcal{P} \in L^\sigma$ *определяются по следующим правилам:*

- *если* $\mathcal{P}$ *– атомная формула, то* $\mathbf{Free}(\mathcal{P}) := \bigcup\limits_t var(t)$*, где объединение берется по всем термам, входящим в формулу* $\mathcal{P}$*, и* $\mathbf{Bound}(\mathcal{P}) := \emptyset$*;*
- *если* $\mathcal{P} = (\neg\mathcal{Q})$*, то* $\mathbf{Free}(\mathcal{P}) := \mathbf{Free}(\mathcal{Q})$ *и* $\mathbf{Bound}(\mathcal{P}) := \mathbf{Bound}(\mathcal{Q})$*;*
- *если* $\mathcal{P} = (\mathcal{Q} \vee \mathcal{S})$ *или* $\mathcal{P} = (\mathcal{Q} \wedge \mathcal{S})$*, или* $\mathcal{P} = (\mathcal{Q} \rightarrow \mathcal{S})$*, то* $\mathbf{Free}(\mathcal{P}) := \mathbf{Free}(\mathcal{Q}) \cup \mathbf{Free}(\mathcal{S})$ *и* $\mathbf{Bound}(\mathcal{P}) := \mathbf{Bound}(\mathcal{Q}) \cup \mathbf{Bound}(\mathcal{S})$*;*
- *если* $\mathcal{P} = ((\forall x)\mathcal{Q})$ *или* $\mathcal{P} = ((\exists x)\mathcal{Q})$*, то* $\mathbf{Free}(\mathcal{P}) = \mathbf{Free}(\mathcal{Q}) \setminus \{x\}$ *и* $\mathbf{Bound}(\mathcal{P}) = \mathbf{Bound}(\mathcal{Q}) \cup \{x\}$.

Иначе говоря, переменные "связываются" кванторами $\forall$, $\exists$. Заметим, что вовсе не обязательно $\mathbf{Free}(\mathcal{P}) \cap \mathbf{Bound}(\mathcal{P}) = \emptyset$. Например, если

$$\mathcal{P} := \forall x(Q(x,y) \to R(x)) \vee \forall y(\neg Q(x,y) \to \forall z R(z)),$$

то для данной формулы $\mathbf{Free}(\mathcal{P}) = \{x, y\}$, $\mathbf{Bound}(\mathcal{P}) = \{x, y, z\}$, а значит, $\mathbf{Free}(\mathcal{P}) \cap \mathbf{Bound}(\mathcal{P}) = \{x, y\} \neq \emptyset$. Тем не менее, каждое конкретное *вхождение* переменной в формулу может быть либо свободным, либо связанным.

Определение 2.3 *Формула $\mathcal{P}$ называется замкнутой (или предложением), если у нее нет свободных переменных.*

2.4 Семантика языков логики первого порядка

До сих пор мы занимались исключительно вопросами синтаксиса языков логики предикатов первого порядка, рассматривая эти языки совершенно формально как наборы цепочек символов, построенных по определенным правилам. Теперь нашей задачей будет придать смысл введенным синтаксическим конструкциям.

Формулы языков первого порядка будем интерпретировать как утверждения о некоторой предметной области, заранее не фиксированной при рассмотрении каждого конкретного языка. Так, например, любая формула может восприниматься как утверждение о натуральных числах, о геометрических фигурах, о крокодилах в Южной Америке и т. п. При этом одна и та же формула может представлять истинное утверждение в одной предметной области и ложное в другой. Например, формула $\forall x A(x)$ может представлять истинное утверждение о крокодилах (например, "все крокодилы являются рептилиями", если $A(x)$ интерпретируется как "x – рептилия") и ложное утверждение о натуральных числах ("все натуральные числа являются четными", если $A(x)$ интерпретируется как "x – четное число"). И даже в одной и той же предметной области формула может оказаться как истинной, так и ложной, в зависимости от того, какой смысл приписывается символам констант, функциональным и предикатным символам, а также символам свободных переменных. Например, приведенная выше формула может представлять и истинное утверждение о натуральных числах, если $A(x)$ интерпретируется как "x – натуральное число".

Прежде чем вводить формальные определения, сделаем еще одно важное замечание. Мы будем рассматривать только классическую *двузначную семантику* (как правило, принято говорить о двузначной логике), в которой каждая формула языка первого порядка интерпретируется как истинное либо ложное утверждение. При этом говорят, что формула имеет истинностное значение: 1 (отождествляемом с истиной) или 0 (отождествляемом с ложью). Существует и многозначная семантика, в которой истинностное значение формулы может принимать

более двух значений. Наиболее широко известной является трехзначная логика Лукасевича, в которой допускается наряду с 0 и 1 истинностное значение 1/2 (интерпретируемое, например, как "вероятно"). Можно рассматривать и континуальную многозначную семантику, в которой истинностное значение формулы может быть любым числом от 0 до 1 и интерпретироваться, например, как степень правдоподобности. Особенно интересны приложения таких многозначных логик. Например, в языке логики предикатов, предназначенном для описания действий с абстрактными множествами, можно записать формулу, выражающую утверждение "данный элемент принадлежит заданному множеству". В классической однозначной семантике такая формула может считаться либо истинной (истинностное значение 1), либо ложной (истинностное значение 0). Однако в только что упомянутой континуальной семантике эта формула может иметь любое истинностное значение в промежутке $[0, 1]$, которое логично интерпретировать как степень принадлежности элемента множеству. Таким образом, в теории множеств, базирующейся на такой семантике, элемент может принадлежать множеству в большей или меньшей степени. Эта теория получила название *теории нечетких множеств (fuzzy set theory)* и нашла широкое применение в методе экспертных оценок.

Теперь мы можем строго определить истинностное значение формулы языка логики предикатов первого порядка L^σ для двузначной семантики. Для этого нам понадобятся понятия *универсума*, *алгебраической системы* и *интерпретации* для языка L^σ.

Определение 2.4 *Алгебраической системой для сигнатуры σ называется набор $\mathcal{M}$ следующих объектов:*

- *непустого множества M, называемого универсумом,*
- *для каждого символа предметной константы $c \in \mathbf{Const}$ выделенного элемента универсума $c^{\mathcal{M}} \in M$,*
- *для каждого n-арного функционального символа $f \in \mathbf{Func}^n$ выделенной функции $f^{\mathcal{M}}\colon M^n \to M$, где $M^n := \underbrace{M \times M \times ... \times M}_{n \text{ раз}}$,*
- *для каждого n-арного предикатного символа $A \in \mathbf{Pred}^n$ характеристической функции выделенного n-местного отношения $A^{\mathcal{M}}\colon M^n \to \{0, 1\}$.*

Определение 2.5 *Интерпретацией в алгебраической системе $\mathcal{M}$ называется пара $(\mathcal{M}, \xi)$, где ξ — функция $\xi\colon \mathbf{Var} \to M$.*

Таким образом, *алгебраическая система* для языка L^σ определяет тот "мир", о котором "говорят" формулы L^σ. Символы предметных констант представлены в ней элементами универсума, функциональные символы – функциями на универсуме, а предикатным символам соответствуют отношения на универсуме. *Интерпретация нужна*, чтобы поставить в соответствие символам предметных переменных элементы универсума.

Пользуясь введенными определениями, мы можем связать элементы универсума и термы языка L^σ. Для этого, фиксировав интерпретацию $(\mathcal{M}, \xi)$, введем в рассмотрение функцию $[\,]$: $\mathbf{TER}(L^\sigma) \to M$ "значения" терма в соответствии со следующими правилами:

- если $t = c \in \mathbf{Const}$, то $[t] := c^{\mathcal{M}}$,
- если $t = x \in \mathbf{Var}$, то $[t] := \xi(x)$,
- если $t = f(t_1, t_2, ..., t_n)$, где $t_1, \ldots, t_n \in \mathbf{TER}(L^\sigma)$, то где $f \in \mathbf{Func}^n$, то $[t] := f^{\mathcal{M}}([t_1], ..., [t_k])$.

Заметим, что приведенные правила корректно определяют функцию $[\,]$ на всем множестве $\mathbf{TER}(L^\sigma)$.

Теперь мы можем наконец определить понятие истинностного значения формулы $\mathcal{P} \in L^\sigma$ в интерпретации $(\mathcal{M}, \xi)$.

Определение 2.6 *Истинностным значением формулы $\mathcal{P} \in L^\sigma$ в интерпретации*
$(\mathcal{M}, \xi)$ называется число $v(\mathcal{P}) \in \{0, 1\}$, определяемое по следующим правилам:

1. *если $\mathcal{P}$ – атомная формула, т. е. $\mathcal{P} = A(t_1, ..., t_n)$, $A \in \mathbf{Pred}^n$, $t_1, \ldots t_n \in \mathbf{TER}(L^\sigma)$, то $v(\mathcal{P}) := A^{\mathcal{M}}([t_1], ..., [t_k])$,*
2. *если $\mathcal{P} = \neg\mathcal{Q}$, то $v(\mathcal{P}) := 1 - v(\mathcal{Q})$,*
3. *если $\mathcal{P} = \mathcal{Q} \wedge \mathcal{S}$, то $v(\mathcal{P}) := \min\{v(\mathcal{Q}), v(\mathcal{S})\}$,*
4. *если $\mathcal{P} = \mathcal{Q} \vee \mathcal{S}$, то $v(\mathcal{P}) := \max\{v(\mathcal{Q}), v(\mathcal{S})\}$,*
5. *если $\mathcal{P} = \mathcal{Q} \to \mathcal{S}$, то $v(\mathcal{P}) := \max\{1 - v(\mathcal{Q}), v(\mathcal{S})\}$,*
6. *если $\mathcal{P} = \forall x\mathcal{Q}$, то $v(\mathcal{P}) := \min\{v_{[a/x]}(\mathcal{Q}) : a \in M\}$, где $v_a(\mathcal{Q})$ – истинностное значение формулы $\mathcal{Q}$ в интерпретации $(\mathcal{M}, \xi_{[a/x]})$, а функция $\xi_{[a/x]}$: $\mathbf{Var} \to M$ определена соотношениями $\xi_{[a/x]}(y) := \xi(y)$ при $y \neq x$, и $\xi_{[a/x]}(x) := a$,*

7. *если* $\mathcal{P} = \exists x \mathcal{Q}(x)$, *то* $v(\mathcal{P}) := \max\{v_{[a/x]}(\mathcal{Q}) : a \in M\}$, *где* $v_{[a/x]}(\mathcal{Q})$ – *истинностное значение формулы* $\mathcal{Q}$ *в интерпретации* $(\mathcal{M}, \xi_{[a/x]})$, *определенной выше.*

Определение 2.7 *Будем говорить, что формула* $\mathcal{P}$ *истинна в интерпретации* $(\mathcal{M}, \xi)$, *если* $v(\mathcal{P}) = 1$, *и ложна, если* $v(\mathcal{P}) = 0$.

Будем писать $(\mathcal{M}, \xi) \models \mathcal{P}$, если $v(\mathcal{P}) = 1$ в интерпретации $(\mathcal{M}, \xi)$.

Определение 2.8 *Будем говорить, что формула* $\mathcal{P}$*:*

- *выполнима в алгебраической системе* $\mathcal{M}$, *если* $(\mathcal{M}, \xi) \models \mathcal{P}$ *для какой-либо интерпретации* $(\mathcal{M}, \xi)$*;*
- *выполнима, если она выполнима в какой-либо алгебраической системе;*
- *тавтология, если она выполнима в любой алгебраической системе;*
- *противоречива, если она невыполнима.*

Определение 2.9 *Алгебраическая система* $\mathcal{M}$ *называется моделью формулы* $\mathcal{P}$, *если* $(\mathcal{M}, \xi) \models \mathcal{P}$ *для любой интерпретации* $(\mathcal{M}, \xi)$. *При этом пишут* $\mathcal{M} \models \mathcal{P}$. *Формула* $\mathcal{P}$ *называется истинной, если у нее есть модель.*

Определение 2.10 *Формула* $\mathcal{P}$ *называется семантическим следствием множества формул* Γ, *если из того, что* $(\mathcal{M}, \xi) \models \mathcal{Q}$ *для всех одновременно* $\mathcal{Q} \in \Gamma$, *следует* $(\mathcal{M}, \xi) \models \mathcal{P}$. *В этом случае принято писать* $\Gamma \models \mathcal{P}$.

Определение 2.11 *Формулы* $\mathcal{P}$, $\mathcal{Q}$ *называются семантически эквивалентными, если* $v(\mathcal{P}) = v(\mathcal{Q})$ *в любой интерпретации. В этом случае пишут* $\mathcal{P} \equiv \mathcal{Q}$.

Пример 2.2 Пусть $\sigma = \{c, f^1, g^2, A^2, B^1\}$, где c – символ предметной константы, f, g – одноместный и двуместный функциональные символы, соответственно, A – двуместный предикатный символ, B – одноместный предикатный символ. В качестве универсума выберем множество $\mathrm{Z}_0^+ = \mathrm{N} \cup \{0\}$ неотрицательных целых чисел. Зададим алгебраическую систему для L^σ, положив:

$$
\begin{aligned}
&c^{\mathcal{M}} := 0,\\
&f^{\mathcal{M}}(n) := n + 1,\\
&g^{\mathcal{M}}(m, n) := m + n,\\
&A^{\mathcal{M}}(m, n) := \begin{cases} 1, & m > n \\ 0, & m \le n, \end{cases}\\
&B^{\mathcal{M}}(n) := \begin{cases} 1, & n \text{ — простое число} \\ 0, & n \text{ — составное число} \end{cases}
\end{aligned}
$$

Пусть $\xi(y) := 2$. Тогда формула $\mathcal{P} := \forall x A(x, f(x)) \vee B(g(c, y))$ истинна, т. е. $v(\mathcal{P}) = 1$. В данной алгебраической системе формула $\mathcal{P}$ выражает следующее утверждение о натуральных числах: "Либо $n + 1 < n$ для любого числа n, либо $y+0$ – простое число". Если в той же алгебраической системе положить $\xi(y) := 4$, то в такой интерпретации формула $\mathcal{P}$ окажется ложной, т. е. $v(\mathcal{P}) = 0$.

Заметим, что истинностное значение формулы $\mathcal{P}$ не зависит от интерпретации связанной переменной.

Рассмотрим еще один любопытный пример.

Пример 2.3 (Парадокс брадобрея) В одном городе жил брадобрей, который брил всех тех, и только тех, кто не брил самого себя. Кто брил брадобрея? Парадокс заключается в том, что попытка дать ответ на этот вопрос приводит к замкнутому кругу рассуждений. А именно, если брадобрей брил себя сам, то он не мог брить себя сам, так как он брил **только** тех, кто не брил самого себя, и наоборот. Объяснение состоит в противоречивости основного утверждения.

Запишем на формальном языке логики первого порядка формулу, выражающую "парадокс брадобрея". Для этого в сигнатуре нам понадобится бинарный предикатный символ, выражающий отношение "бреет": $R(x, y)$ значит x бреет y. Рассмотрим сигнатуру $\sigma = \{b, R\}$, где символ константы b – это брадобрей. Утверждение "брадобрей бреет тех и только тех, кто не бреет самого себя" записывается тогда в виде формулы:

$$\mathcal{P} := \forall x(\neg R(x, x) \to R(b, x)) \wedge \forall x(R(b, x) \to \neg R(x, x))$$

Достаточно простого подсчета в соответствии с определением истинностного значения, чтобы убедиться в том, что эта формула не выполняется ни в какой алгебраической сестеме.

Упражнение 2.1 *Покажите справедливость следующих утверждений:*

$$\neg\forall x P(x) \equiv \exists x \neg P(x),$$
$$\neg\exists x P(x) \equiv \forall x \neg P(x)$$

Определение 2.12 *Будем называть замыканием формулы $\mathcal{P}$ со свободными переменными* $\mathbf{Free}(\mathcal{P}) = \{x_1, x_2, \ldots, x_k\}$ *формулу*

$$Cl(\mathcal{P}) := \forall x_1, \forall x_2, \ldots, \forall x_k \mathcal{P}$$

Теорема 2.3 *Алгебраическая система $\mathcal{M}$ является моделью формулы $\mathcal{P}$, если и только если $\mathcal{M}$ является моделью замыкания $\mathcal{P}$, т. е. $\mathcal{M} \models \mathcal{P}$ если и только если $\mathcal{M} \models Cl(\mathcal{P})$.*

Упражнение 2.2 *Доказать теорему о замыкании.*

Определение 2.13 *Язык логики первого порядка, сигнатура которого содержит счетный набор символов констант, счетный набор функциональных символов и счетный набор предикатных символов любой арности будем обозначать $L^{\sigma\infty}$. Очевидно, что при этом любой другой язык логики первого порядка с не более чем счетным алфавитом можно, не ограничивая общности, считать содержащимся в $L^{\sigma\infty}$.*

3 Языки логики второго порядка

Языки логики *второго порядка* отличаются от языков логики первого порядка наличием в алфавите дополнительно символов *предикатных переменных* (для которых мы резервируем большие латинские буквы X, Y, Z, возможно, с цифровыми индексами), а также наличием дополнительных формул вида $\forall X\, Q$, $\exists X\, Q$ с использованием символов предикатных переменных.

Множество *предикатных переменных* алфавита $\mathcal{A}$ языка логики второго порядка будем обозначать **VarPred**. Если надо подчеркнуть, что речь идет о множестве k-арных предикатных переменных, то будем писать $\mathbf{VarPred}^k$. Таким образом,

$$\mathcal{A} = \mathbf{Const} \cup \mathbf{Func} \cup \mathbf{Pred} \cup \mathbf{VarPred} \cup \mathbf{Var} \cup \mathbf{Log} \cup \mathbf{Aux}.$$

Термы языка логики второго порядка определяются так же, как и термы языка логики первого порядка, а формулы отличаются возможностью использовать предикатные переменные после кванторов:

$$\begin{aligned}
< \text{атомная формула} > \quad ::= \quad & < n - \text{арный пред. символ} > (< \text{терм} >, ...) \\
& | < n - \text{арная пред. переменная} > (< \text{терм} >, \ldots), \\
< \text{формула} > \quad ::= \quad & < \text{атомная формула} > | \ (\neg < \text{формула} >) \\
& |(< \text{формула} > \wedge < \text{формула} >) \\
& |(< \text{формула} > \vee < \text{формула} >) \\
& |(< \text{формула} > \rightarrow < \text{формула} >) \\
& |(\exists < \text{переменная} >< \text{формула} >) \\
& |(\forall < \text{переменная} >< \text{формула} >) \\
& |((\forall < \text{пред. переменная} >< X >) < \text{формула} >) \\
& |((\exists < \text{пред. переменная} >< X >) < \text{формула} >), \\
< \text{терм} > \quad ::= \quad & < \text{константа} > \\
& | < \text{переменная} > \\
& | < n - \text{арный функ. символ} > (< \text{терм} >, ...).
\end{aligned}$$

Чтобы не писать лишних скобок, мы применяем ранее введенное правило приоритетов операций:

$$Pr(\exists) = Pr(\forall) = Pr(\neg) > Pr(\wedge) > Pr(\vee) > Pr(\rightarrow).$$

Очевидно, чтобы интерпретировать формулы языка логики второго порядка, достаточно лишь слегка скорректировать сформулированные правила для семантики языков первого порядка, добавив возможность интерпретировать "новые" формулы с предикатными переменными. Приведем поэтому только те определения, которые существенно меняются по сравнению с семантикой языков первого порядка.

Определение 3.1 *Интерпретацией для языка логики второго порядка называется тройка* $(\mathcal{M}, \xi, \eta)$*, где* $\mathcal{M}$ *– алгебраическая система,* ξ*:* $\mathbf{Var} \to M$*,* $\eta : \mathbf{VarPred}^k \to \mathbf{B}^k$*,* $\mathbf{B}^k := \left\{\chi : L \to \{0,1\} \;\middle|\; L \subset M^k\right\}$*.*

Таким образом, если символ предметной переменной интерпретируется элементом выбранного универсума, то символ k-арной предикатной переменной интерпретируется характеристической функцией k-арного отношения на универсуме.

Для вычисления истинностного значения формул языка логики второго порядка необходимо в дополнение к соответствующим правилам, сформулированным для логики первого порядка, использовать следующие правила:

(i) $v(X^k(t_1, \ldots, t_k)) := \eta(X^k)([t_1], ..., [t_k])$, где $X^k \in \mathbf{VarPred}^k$, а все $t_i \in \mathbf{TER}$;

(ii) $v(\forall Y\,(\mathcal{P})) := \min\left\{v_{\eta_Y}(\mathcal{P}) \,:\, \chi \in \mathbf{B}^k\right\}$,

(iii) $v(\exists Y\,(\mathcal{P})) := \max\left\{v_{\eta_Y}(\mathcal{P}) \,:\, \chi \in \mathbf{B}^k\right\}$,

где символом $v_{\eta_Y}(\mathcal{P})$ обозначено истинностное значение формулы $\mathcal{P}$ в интерпретации $(\mathcal{M}, \xi, \eta_Y)$,

$$\eta_Y(X) := \begin{cases} \chi \in \mathbf{B}^k, & X = Y \\ \eta(X), & X \neq Y. \end{cases}$$

4 Логические языки с равенством

Очень часто в алфавит языков логики первого или второго порядка, предназначенных для формализации математических или естественнонаучных утверждений, включается двуместный предикатный *символ равенства*, обозначаемый, как правило, символом $=$. Такие языки будем называть *языками с равенством*. Заметим, что вместо $=(x, y)$ принято писать $x = y$.

Пусть задана алгебраическая система $\mathcal{M}$ для интерпретации формул языка с равенством. Вообще говоря, если ничего дополнительно не требовать, то предикатному символу равенства может соответствовать в ней двуместное отношение, никак не соотносящееся с привычным для нас понятием равенства. Чтобы избежать такой ситуации, принято требовать, чтобы в $\mathcal{M}$ был выполним набор предложений, называемых *аксиомами равенства*, характеризующих особые свойства отношения равенства.

Для языка первого порядка аксиомы равенства следующие:

(R) $\forall x\,(x = x)$,

(S) $\forall x \forall y (x = y \to y = x)$,

(T) $\forall x \forall y \forall z (x = y \wedge y = z \to x = z)$,

(F) $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n ((x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n) \to (\varphi^n(x_1, \ldots, x_n) = \varphi^n(y_1, \ldots, y_n))$,

(P) $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n ((x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n) \to (\mathcal{P}^n(x_1, \ldots, x_n) = \mathcal{P}^n(y_1, \ldots, y_n))$.

Здесь (R), (S), (T) – аксиомы, выражающие, соответственно, рефлексивность, симметричность и транзитивность отношения равенства. (F) и (P) – это *схемы аксиом*, т.е. "шаблоны" бесконечного, вообще говоря, множества аксиом. Отдельные аксиомы получаются из схем (F) и (P) подстановкой вместо φ^n любой выразимой в рассматриваемом языке n-местной функции (т.е. терма с n различными символами переменных), а вместо $\mathcal{P}^n$ – любого выразимого в этом языке n-местного предиката (т.е. атомной формулы с n свободными переменными). Получаемые таким образом аксиомы называются *вариантами* соответствующих схем аксиом. Схемы аксиом (F) и (P) выражают, соответственно, неразличимость "равных" объектов (элементов универсума) при помощи выразимых в данном языке функций и предикатов.

Для языка логики второго порядка набор аксиом равенства состоит из аксиом (R), (S), (T) и аксиом (F') и (P'), заменяющих схемы аксиом (F) и (P) соответственно:

(F') $\forall f^n \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n ((x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n) \to (f^n(x_1, \ldots, x_n) = f^n(y_1, \ldots, y_n))$,

(P') $\forall X^n \forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n ((x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n) \to (X^n(x_1, \ldots, x_n) = X^n(y_1, \ldots, y_n))$.

Заметим, что в (P') используется символ n-арной предикатной переменной X^n, а в (F') используется символ n-арной *функциональной* переменной f^n. Строго говоря, согласно данному нами определению, в алфавите языков логики второго порядка нет специально зарезервированных символов для функциональных переменных. Однако это никак не ограничивает выразительной силы языка второго порядка: на самом деле функциональные переменные можно заменить предикатными переменными.

Действительно, функцию можно отождествить с ее графиком, а графики функций это частный случай отношений. Например, "формулу" $\forall f\,(P(f(x)))$ (где f – символ унарной функциональной переменной) можно считать просто сокращенным написанием формулы $\forall X\,(\underline{func}(X) \wedge (\forall y(X(x,y) \to P(y))))$, где формула

$$\underline{func}(X) := \forall x \exists! y\, X(x,y)$$

выражает то факт, что X – график функции. Здесь использовано весьма распространенное сокращение $\exists!$ ("существует и единственно"):

$$\exists! x \mathcal{P}(x) := \exists x \mathcal{P}(x) \wedge \forall x \forall y (\mathcal{P}(x) \wedge \mathcal{P}(y) \to x = y).$$

Таким образом, не ограничивая общности, можно считать, что в языках логики второго порядка с равенством присутствуют и символы функциональных переменных, либо, что то же самое, считать формулы, в которых появляются такие символы, просто сокращением формул, использующих только символы предикатных переменных.

Тем не менее, хотя истинность аксиом равенства в выбранной алгебраической системе и означает, что предикатный символ равенства будет интерпретироваться "разумно", но она все-таки не гарантирует того, что он будет интерпретироваться именно равенством, т.е. совпадением элементов универсума. Поэтому в дальнейшем, имея дело с языками с равенством, будем дополнительно требовать, чтобы в выбранной алгебраической системе предикатному символу равенства соответствовало бы отношение равенства (совпадения) элементов универсума. Естественно, аксиомы равенства при этом автоматически оказываются истинными.

5 Арифметика Пеано

Рассмотрим в качестве первого содержательного примера языков логики предикатов языки для описания арифметических действий с натуральными числами. Для этой цели зададим сигнатуру

$$\sigma_{ar} := (0, s, +, \cdot, =),$$

где 0 – символ константы "нуль", s – символ унарной функции выделения следующего по порядку числа, $+$ и $\cdot$ – символы бинарных функций суммы и произведения, и, наконец, $=$ – предикатный символ равенства. Как и в случае с символом равенства, для символов $+$ и $\cdot$ будем в дальнейшем писать $(x+y)$ и $(x\cdot y)$ вместо $+(x,y)$ и $\cdot(x,y)$, соответственно, а так же не писать "лишние" скобки, приписывая символу $\cdot$ более высокий приоритет по сравнению с $+$, как это и принято в математике. Эта сигнатура задает два языка логики предикатов с равенством – первого $L_I^{\sigma_{ar}}$ и второго порядка $L_{II}^{\sigma_{ar}}$ соответственно, которые мы будем называть языками арифметики Пеано (по имени итальянского математика Giuseppe Peano, впервые рассмотревшего формальные языки для описания арифметики). Эти языки описывают только самые простые действия с натуральными числами "в пределах начальной школы", в число которых, например, даже не входит возведение в степень. И все же даже такие простые на первый взгляд языки обладают, как мы в дальнейшем покажем, весьма неожиданными свойствами.

Возникает вопрос: какие формулы языка арифметики Пеано имеют смысл? Очевидно, лишь те из них, которые верны для натуральных чисел (ведь именно для действий с ними предназначен этот язык). Выражаясь точнее, осмысленными разумно считать только формулы, выполнимые в алгебраической системе $\mathcal{N}$, универсум которой есть множество натуральных чисел (с нулем), символ 0 соответствует нулю (т.е. $0^{\mathcal{N}} := 0$), символ s соответствует функции прибавления единицы (т.е. $s^{\mathcal{N}}(n) := n+1$), а символы $+$ и $\cdot$ соответствуют функциям сложения и умножения двух чисел (т.е. $+^{\mathcal{N}}(m,n) := m+n$, $\cdot^{\mathcal{N}}(m,n) := mn$). Алгебраическую систему $\mathcal{N}$ будем в дальнейшем называть *стандартной моделью арифметики*.

Например, формулы $x = s(0)$ или $\forall x \forall y(\neg y = 0 \to \neg x = x + y)$ языка арифметики Пеано (заметим, что это формулы первого порядка, поэтому они принадлежат как $L_I^{\sigma_{ar}}$, так и $L_{II}^{\sigma_{ar}}$), являются осмысленными утверждениями о натуральных числах, иначе говоря, выполнимы в $\mathcal{N}$, а формула $\forall x(x = 0)$, невыполнима в $\mathcal{N}$, т.к. будучи "прочитанной" как утверждение о натуральных числах, она очевидно неверна.

Назовем множество формул языка арифметики Пеано первого или второго порядка, соответственно, истинных в $\mathcal{N}$, теорией элементарной арифметики $Th_i(\mathcal{N})$ (соответствующего порядка, указываемого индексом $i = I$ или $i = II$). В дальнейшем, если из контекста ясно, о каком языке арифметики – первого или второго порядка – идет речь, либо это не имеет значения, мы будем говорить просто о языке арифметики Пеано и о теории элементарной арифметики, не указывая порядок. Таким образом, теория элементарной арифметики

$$Th_i(\mathcal{N}) := \{\mathcal{P} \in L_i^{\sigma_{ar}} : \mathcal{N} \models \mathcal{P}\}, \qquad i = I, II$$

является набором формул соответствующего порядка, выражающего истинные

факты для натуральных чисел. Легко заметить, что введенные понятия весьма неконструктивны. А именно, они не заключают в себе никакого способа проверки, принадлежит ли данная формула языка арифметики Пеано теории элементарной арифметики (т.е. действительно ли она описывает некоторое свойство натуральных чисел). Конечно, такой алгоритм, пусть и очень сложный, найти было бы весьма заманчиво. Ведь тогда творческую работу математиков, доказывающих все новые теоремы теории чисел, можно было бы заменить на программу, работающую по такому алгоритму. Кстати, то же самое можно сказать и о любой другой математической (или даже шире – любой вообще научной) теории.

Попытаемся найти такой алгоритм. Для этого проанализируем, как на самом деле математики проверяют истинность утверждений, например, из теории чисел. Конечно, не путем "прямого перебора" всех возможных наборов чисел, поскольку такая проверка в силу бесконечности множества натуральных чисел никогда бы не завершилась! Для проверки истинности данного утверждения математик ищет его доказательство, исходя из некоторого набора аксиом. Иначе говоря, математик имеет в виду некоторый набор утверждений (называемых аксиомами) Γ, не просто истинных в данной модели $\mathcal{M}$, но и в каком-то смысле вполне ее характеризующих, иначе говоря, таких, что можно надеяться, что *любое истинное утверждение о данной модели является логическим следствием этих аксиом*. Часто говорят при этом, что Γ – система аксиом для модели $\mathcal{M}$. Далее он пытается проверить, является ли данная формула $\mathcal{P}$ логическим следствием аксиом Γ (в этом и состоит процесс доказывания). Если $\Gamma \models \mathcal{P}$, то $\mathcal{P}$ истинно в данной модели, поскольку любая модель всех одновременно формул Γ, в частности и $\mathcal{M}$, является и моделью $\mathcal{P}$.

О том, как устроен процесс доказывания, речь еще впереди. Сейчас же отметим, что успешность подобного рода действий во всяком случае должна зависеть от того, насколько удачно подобрана система аксиом Γ. Действительно, обозначим $\Gamma^{\models}$ множество всех логических следствий Γ, а $Th(\mathcal{M})$ – множество всех утверждений, истинных в модели $\mathcal{M}$. Если Γ выбрано корректно, то есть так, что все формулы из Γ истинны в $\mathcal{M}$, то $\Gamma^{\models} \subset Th(\mathcal{M})$. Но нам бы, естественно, хотелось, чтобы все формулы, истинные в $\mathcal{M}$, были бы логическими следствиями Γ. Но как это обеспечить? Иначе говоря, как выбрать множество Γ, чтобы $\Gamma^{\models} = Th(\mathcal{M})$? Вопрос об удачном подборе такой системы аксиом Γ для алгебраической системы $\mathcal{M}$ часто называют вопросом аксиоматизации $\mathcal{M}$).

На поставленный вопрос есть, конечно, и тривиальный ответ: $\Gamma := Th(\mathcal{M})$, очевидно, удовлетворяет этому требованию. Но этот ответ совершенно не интересен: ведь вся затея с аксиомами нужна была как раз для того чтобы, "конструктивно" (т.е. алгоритмически) описывать множество $Th(\mathcal{M})$, например, найти алгоритм проверки того, является ли данная формула истинной в модели $\mathcal{M}$. Для этого множество Γ должно быть в определенном смысле "обозримым" (же-

лательно вообще конечным или уж во всяком случае таким, которое может быть построено при помощи некоторого алгоритма), и конечно, не может совпадать с $Th(\mathcal{M})$.

Вернемся к рассмотрению элементарной арифметики. Попытка предложить для нее разумную систему аксиом была осуществлена Пеано. Он показал, что практически все основные теоремы теории чисел (т.е. истинные утверждения о натуральных числах), записываемые в языке арифметики первого порядка, являются логическими следствиями аксиом

(PA_1) $\forall x \neg(s(x) = 0)$,

(PA_2) $\forall x \forall y \, (s(x) = s(y) \to x = y)$,

(PA_3) $\forall x \, (x + 0 = x)$,

(PA_4) $\forall x \, (x \cdot 0 = 0)$,

(PA_5) $\forall x \forall y \, (x + s(y) = s(x + y))$,

(PA_6) $\forall x \forall y \, (x \cdot s(y) = x + x \cdot y)$,

(PA_7) $\mathcal{P}(0) \wedge \forall x \, (\mathcal{P}(x) \to \mathcal{P}(s(x))) \to \forall y \, \mathcal{P}(y)$, где
$\mathcal{P}$ – любая формула языка $L_I^{\sigma_{ar}}$ с одной свободной переменной.

Мы будем называть формальной арифметикой Пеано первого порядка $PA_I^{\models}$ множество всех логических следствий аксиом (PA_5)–(PA_7). Формальной арифметикой Пеано второго порядка $PA_{II}^{\models}$ будем называть множество всех логических следствий аксиом (PA_1)–(PA_6) и аксиомы

$$\forall X \, (X(0) \wedge \forall x \, (X(x) \to X(s(x))) \to \forall x \, X(x)) \qquad (IND).$$

Сами эти аксиомы мы также будем называть аксиомами Пеано. Аксиома (PA_1) утверждает, что нуль – первый по порядку элемент натурального ряда. Аксиома (PA_2) утверждает, что функция выбора следующего по порядку элемента инъективна, иначе говоря, что за каждым числом непосредственно следует только одно число. (PA_3) и (PA_4) задают правила прибавления нуля и умножения на нуль, а (PA_5) и (PA_6) связывают между собой функции сложения и умножения с функцией выбора следующего по порядку элемента. Наконец, (PA_7) представляет собой схему аксиом (т.е. "шаблон" бесконечного числа аксиом) и выражает принцип математической индукции. Тот же самый принцип выражает и аксиома второго порядка (IND). Стоит еще раз подчеркнуть, что отличие формальной арифметики Пеано первого и второго порядка состоит только в написании принципа математической индукции. В первом случае он записывается при помощи

бесконечного числа аксиом, объединенных в одну схему аксиом, а во втором – в одну аксиому второго порядка.

Очевидно, что стандартная модель $\mathcal{N}$ является моделью для арифметики Пеано (как первого, так и второго порядка). А есть ли у арифметики Пеано другие модели? Стоит отметить, что заданный вопрос весьма глубокий, и по сути дела является вопросом о том, что вообще следует понимать под натуральными числами. В самом деле, действия с натуральными числами являются для нас настолько привычными, что мы и не задумываемся об их смысле, а именно, о том, что такое число, что следует понимать под суммой и произведением чисел и т.п. В окружающем нас мире натуральные числа отсутствуют – это лишь абстракция, "идея", присутствующая только в нашем сознании (хотя, конечно, при построении этой, как и всякой другой, абстрактной конструкции, человечество использует идеализацию свойств реальных объектов окружающего мира). Значит, ответить на вопрос о том, что такое число, просто указав на какой-то объект или явление природы, невозможно. Поэтому математики, в особенности те из них, которые с особым трепетом относятся к строгости рассуждений, как правило, дают другой, весьма естественный и вместе с тем достаточно строгий (хотя и не вполне очевидный) ответ на этот вопрос. А именно, натуральные числа и действия с ними можно определить просто как элементы алгебраической системы, являющейся моделью всех "осмысленных утверждений о числах". Слова "осмысленные утверждения о числах" взяты в кавычки, так как под этим на самом деле понимается некоторый набор утверждений языка арифметики Пеано первого или второго порядка, которые мы условимся считать таковыми. Раньше мы говорили об осмысленности формул языка арифметики, если они были выполнимы в стандартной модели $\mathcal{N}$. Но если мы хотим строго определить сами понятия натуральных чисел и действий с ними, то на такое понимание "осмысленности" опираться уже нельзя, так как, строго говоря, пока не определено даже само множество натуральных чисел $\mathbf{N}$, являющееся универсумом алгебраической системы $\mathcal{N}$. Поэтому осмысленными в данном случае естественно считать лишь все логические следствия выбранной "разумной" системы аксиом, например, в нашем случае формальную арифметику Пеано первого или второго порядка. Тогда определение натуральных чисел и действий с ними как элементов соответствующей модели формальной арифметики становится уже достаточно строгим, поскольку оно не ссылается на интуитивное понятие числа как количества объектов любого сорта. Кстати, именно таким способом обычно строго определяют все другие базовые математические понятия, которые мы привыкли считать интуитивно ясными и неопределимыми. Например, в геометрии такими базовыми и неопределимыми понятиями принято считать точки, прямые и плоскости. "В природе" геометрических точек, прямых и плоскостей не существует. Эти понятия получены в результате систематизации многотысячелетнего опыта

обращения людей с реальными предметами очень маленьких размеров (в случае точек), очень тонкими и длинными предметами (в случае прямых) и очень плоскими предметами больших размеров (в случае плоскостей), а именно, в результате абстрактизации (идеализации) свойств такого рода предметов. Полученная в результате умственная конструкция – мир геометрических точек, прямых и плоскостей – далее описывается при помощи подходящего набора аксиом, т.е. такого, который бы адекватно нашему интуитивному представлению описывал свойства объектов этого мира и, по возможности, был бы достаточно полным в том смысле, что все (или, по крайней мере, значительная часть) истинные (опять-таки в соответствии с нашим интуитивным представлением) утверждения о таких объектах были бы логическими следствиями этих аксиом. Выбор системы аксиом, естественно, при этом соответствует только нашим интуитивным представлениям об "адекватности" и "полноте" и поэтому никак не может быть формализован. Единственное формальное и к тому же естественное требование к набору аксиом – непротиворечивость. Так, большинство людей, ограничивающих свое представление о физическом мире современной физикой, могут вполне удовлетвориться аксиомами Эвклида (с аксиомой или без аксиомы параллельных). Когда система аксиом выбрана, можно дать и строгое определение точкам, прямым и плоскостям как элементам алгебраической системы, являющейся моделью выбранных аксиом (а значит, и всех их логических следствий). Таким образом, эти понятия, строго говоря, становятся зависимыми от выбранной системы аксиом.

Итак, натуральные числа и действия с ними будут пониматься как элементы алгебраической системы, являющейся моделью формальной арифметики Пеано первого или второго порядка, в зависимости от того, какую систему аксиом – первого или второго порядка – мы будем выбирать. В связи с этим возникают два связанных между собой вопроса. Во-первых, насколько выбор набора аксиом влияет на получаемое понятие натуральных чисел (a priori это понятие зависит от выбранных аксиом)? Во-вторых, сколько вообще различных "версий" натуральных чисел определяются выбранной системой аксиом (т.е. сколько разных моделей у выбранных аксиом). Простой ответ на второй вопрос очевиден: ни аксиомы Пеано первого, ни второго порядка не определяют натуральные числа и действия с ними однозначно. Действительно, предположим, что формальная арифметика Пеано (безразлично какого порядка) имеет модель. Элементы универсума этой модели мы считаем "настоящими" натуральными числами, т.е. таким образом эта модель становится стандартной моделью арифметики. Но тогда очевидно, что моделью формальной арифметики Пеано будет являться и любая алгебраическая система $\mathcal{M}$, универсум которой – произвольно выбранная последовательность $\{x_i\}_{i=0}^{\infty}$, $0^{\mathcal{M}} := x_0$, $s^{\mathcal{M}}(x_n) := x_{n+1}$, $+^{\mathcal{M}}(x_m, x_n) := x_{m+n}$, $\cdot^{\mathcal{M}}(x_m, x_n) := x_{mn}$). Однако более пристальное рассмотрение всех таких моделей убеждает, что все они между собой весьма схожи, а именно, они изоморфны в

смысле следующего определения.

Определение 5.1 *Пусть $\mathcal{A}$ и $\mathcal{B}$ алгебраические системы для языка L^σ. $\mathcal{A}$ называется изоморфной $\mathcal{B}$ (пишут $\mathcal{A} \simeq \mathcal{B}$), если существует биекция π: $\mathcal{A} \to B$, удовлетворяющая условиям*

(i) $\pi(c^{\mathcal{A}}) = c^{\mathcal{B}}$ *для всех* $c \in \mathbf{Const}$,

(ii) $\pi(f^{\mathcal{A}}(t_1, t_2, \ldots, t_n)) = f^{\mathcal{B}}(\pi(t_1), \pi(t_2), \ldots, \pi(t_n))$ *для всех* $f \in \mathbf{Func}^n$,

(iii) $P^{\mathcal{A}}(t_1, t_2, \ldots, t_n) = P^{\mathcal{B}}(\pi(t_1), \pi(t_2), \ldots, \pi(t_n))$ *для всех* $P \in \mathbf{Pred}^n$.

Очевидно, что отношение изоморфности моделей является отношением эквивалентности, т.е. оно симметрично, рефлексивно и транзитивно (проверьте это!). Не менее тривиально проверяется и следующее свойство.

Упражнение 5.1 *Пусть $\mathcal{A}$ и $\mathcal{B}$ алгебраические системы для языка L^σ, и пусть $\mathcal{A} \simeq \mathcal{B}$. Докажите, что для любого $\mathcal{P} \in \Gamma$ верно $\mathcal{A} \models \mathcal{P}$, если и только если $\mathcal{B} \models \mathcal{P}$.*

Данное упражнение показывает, что изоморфные алгебраические системы неразличимы при помощи языков логики первого и второго порядка. Поэтому уточним поставленный выше вопрос о существовании моделей формальной арифметики Пеано, отличных от стандартной, следующим образом: существуют ли модели формальной арифметики Пеано, неизоморфные стандартной? Оказывается, ответ на этот вопрос различен для формальной арифметики первого и второго порядка. Для формальной арифметики второго порядка ответ дает следующая теорема.

Теорема 5.1 (Дедекинд) *Любые две модели формальной арифметики Пеано второго порядка изоморфны между собой.*

Доказательство: Пусть $\mathcal{A} \models PA_{II}^{\models}$. Докажем, что $\mathcal{A} \simeq \mathcal{N}$. Определим функцию π: $\mathbf{N} \to A$ следующим образом:

(i) $\pi(0) := 0^{\mathcal{A}}$,

(ii) $\pi(n+1) := s^{\mathcal{A}}(\pi(n))$.

В силу принципа математической индукции функция π, таким образом, корректно задана на всем множестве $\mathcal{N}$. Заметим, что в силу аксиомы (IND) принцип математической индукции действует во всех моделях $PA_{II}^{\models}$.

Выполнение условий (i)–(iii) определения изоморфизма алгебраических систем при таком определении очевидно (проверьте это!). Осталось только проверить, что таким образом определенная функция действительно является биекцией.

Шаг 1. Докажем, что π – инъекция, то есть из $m \neq n$ следует $\pi(m) \neq \pi(n)$. Поведем доказательство по методу математической индукции в $\mathcal{N}$.

- База индукции. Пусть $n = 0$, $m \neq 0$. Тогда $m = k + 1$ для некоторого k. Этот факт верен, вообще говоря, только для стандартной модели. Тогда $\pi(m) = \pi(k + 1) = s^A(\pi(k)) \neq 0^{\mathcal{A}} = \pi(0^N)$ в силу (PA_1). База индукции доказана.

- Шаг индукции. Пусть $m \neq n + 1$. Докажем, что при этом $\pi(m) \neq \pi(n + 1)$. Рассмотрим два случая.

  Случай 1. $m = 0$. Тогда $\pi(n + 1) = s^{\mathcal{A}}(\pi(n)) \neq 0^{\mathcal{A}} = \pi(0^{\mathcal{N}}) = \pi(m)$.

  Случай 2. $m = k+1$. Из предположения $m \neq n+1$ следует $k \neq n$. Но тогда $\pi(k) \neq \pi(n)$ в силу предположения индукции, а значит, $s^{\mathcal{A}}(\pi(k)) \neq s^{\mathcal{A}}(\pi(n))$ в силу (PA_2). Поэтому $\pi(m) = \pi(k + 1) = s^{\mathcal{A}}(\pi(k)) \neq \pi(n + 1) = s^{\mathcal{A}}(\pi(n))$.

В силу принципа математической индукции, таким образом, доказана инъективность функции π.

Шаг 2. Докажем, что π сюръективна, то есть, что для всех $a \in A$ выполнено $a \in Im(\pi)$. Для этого воспользуемся принципом математической индукции, но на этот раз в $\mathcal{A}$. Напомним, что этот принцип действует во всех моделях $PA_{II}^{\models}$ в силу (IND). База индукции в этом случае тривиальна: $0^{\mathcal{A}} \in Im(\pi)$ по определению π. Пусть теперь $b \in Im(\pi)$, то есть $b = \pi(n)$ для некоторого $n \in \mathbf{N}$. Тогда и $s^{\mathcal{A}}(b) = \pi(n+1) \in Im(\pi)$ в силу определения π, т.е. доказан и шаг индукции. В силу произвольности b по принципу математической индукции все $a \in A$ принадлежат образу π, иначе говоря, функция π сюрьективна.

В дальнейшем мы покажем, что утверждение, аналогичное теореме Дедекинда, неверно для формальной арифметики Пеано первого порядка, а именно, последняя имеет бесконечно много разных с точностью до изоморфизма моделей. Более того, среди этих моделей можно найти и такие, которые обладают универсумом сколь угодно большой наперед заданной мощности. Иначе говоря, формальная арифметика Пеано первого порядка допускает бесконечно много принципиально разных "версий" натуральных чисел и действий над ними, в том числе и таких, в которых "множество натуральных чисел" несчетно (т.е. неизоморфно "стандартному" множеству натуральных чисел $\mathbf{N}$)! Почему же доказательство теоремы Дедекинда не работает для формальной арифметики Пеано первого порядка? Анализируя доказательство, мы видим, что в первом шаге нет никаких

рассуждений, которых нельзя было бы провести для арифметики первого порядка (на этом шаге мы пользовались лишь аксиомами (PA_1), (PA_2) и принципом математической индукции в $\mathcal{N}$). Проблема, таким образом, во втором шаге, где мы воспользовались уже принципом математической индукции в $\mathcal{A}$, а именно, тем, что для любого свойства X элементов универсума A верно следующее: если $0^{\mathcal{A}}$ обладает свойством X (база индукции), а также для любого $b \in A$ из обладания b свойством X следует обладание $s^{\mathcal{A}}(b)$ тем же свойством, то свойством X обладают все элементы A. Для арифметики второго порядка выполнимость этого принципа в любой модели гарантирована аксиомой (IND). Однако в арифметике первого порядка вместо этой аксиомы имеется гораздо более слабый набор (схема) аксиом (PA_7). Он гарантирует выполнение вышеприведенного принципа не для всех свойств X, а лишь для тех из них, которые можно записать при помощи формул $\mathcal{P}$ языка арифметики Пеано первого порядка с одной свободной переменной. Заметим, что множество таких свойств очевидно счетно, так как алфавит языка конечен. В то же время всех вообще свойств элементов множества A гораздо больше. Действительно, такие свойства можно тривиально отождествить с подмножествами универсума A (каждому свойству X соответствует подмножество элементов A, обладающих этим свойством, а каждому подмножеству A соответствует свойство принадлежности этому подмножеству). Так как A не может быть конечным множеством (в силу (PA_1) и (PA_2)), то множество всех свойств элементов A более чем счетно! Таким образом, обязательно найдутся свойства, невыразимые формулами первого порядка с одной свободной переменной, и таким вполне может оказаться свойство принадлежности множеству $Im(\pi)$, а значит, второй шаг доказательства становится необоснованным.

Еще одно важное замечание: в доказательстве теоремы Дедекинда мы воспользовались тем, что в стандартной модели арифметики из $m \neq 0$ следует $m = k+1$ для некоторого натурального k. Никакая аксиома Пеано не гарантирует выполнение этого свойства во всех моделях формальной арифметики Пеано. Тот же факт, что это свойство верно для стандартной модели арифметики, следует из наших знаний именно об этой модели, а не из аксиом арифметики. Кстати, и само существование такой стандартной модели арифметики тоже не обеспечивается аксиомами Пеано. Строго обосновать существование стандартной модели арифметики, обладающей привычными для нас свойствами, можно только при помощи введения специальных "более сильных" аксиом, например, аксиом теории множеств, речь о которой впереди.

6 Элементы теории доказательств

6.1 Формальные системы

В предыдущей главе мы отложили вопрос о том, как проверять, является ли данная формула $\mathcal{P} \in L^\sigma$ логическим следствием заданного множества формул $\Gamma \in L^\sigma$. Очевидно, что осуществить такую проверку в соответствии с определением не представляется возможным. Действительно, нельзя просто перебрать всевозможные модели всех одновременно формул множества Γ, чтобы проверить, являются ли они моделями формулы $\mathcal{P}$, т.к. число таких моделей может быть бесконечно, за исключением разве что некоторых тривиальных случаев. Математики заменяют такую проверку поиском доказательства формулы $\mathcal{P}$ из набора формул Γ, т.е. поиском способа "свести" формулы Γ и, возможно, ещё некоторые дополнительные формулы, к формуле $\mathcal{P}$, при помощи конечного числа логических заключений (иногда говорят *логических переходов*) являющихся общепризнанно элементарными. В этой главе мы формализуем процесс доказывания таким образом, чтобы полученная формализация была применима к языкам логики предикатов первого порядка.

Будем различать *семантические* и *формальные* истины, определяемые для формул Γ. Семантические истины это те формулы, которые семантически следуют из Γ, формальные – те, которые выводятся из данного набора при помощи принятых правил доказывания. Важно отметить, что истина, полученная при помощи формального вывода (доказательства) существенно зависит от того, какие правила доказывания мы считаем допустимыми. В любом случае хотелось бы, чтобы формулы выводимые (доказуемые) были истинны семантически. Иначе правила вывода получаются некорректны (они существуют для вывода семантических истин, а не всякой ерунды). Но, конечно, желательно, чтобы наши правила были в определенном смысле полны, то есть формально выводились бы *все* семантические истины.

Рассмотрим формальный язык $L \subset V^*$ над алфавитом V. Будем называть *секвенцией* выражение вида

$$V_1, V_2, \ldots, V_n \vdash V,$$

где $V_i \in L$, $i = 1, \ldots, n$ и $V \in L$, либо выражение вида

$$\vdash V,$$

где $V \in L$. В первом случае будем читать секвенцию $V_1, V_2, \ldots, V_n \vdash V$ как "$V_1, V_2, \ldots, V_n$ выводит (или доказывает, если L – какой-либо логическийязык) V", или "из $V_1, V_2, \ldots, V_n$ следует V". Во втором случае секвенцию $\vdash V$ будем читать как "V выводима", или выводима из пустого множества посылок (доказуема, если L – какой-либо язык логики). Теперь введем следующее определение.

Определение 6.1 *Будем говорить, что задана формальная система* Φ*, если заданы*

(i) набор секвенций вида $\vdash V$*, где* $V \in L$*, называемых аксиомами формальной системы;*

(ii) набор секвенций вида $V_1, V_2, \ldots, V_n \vdash V$ *где* $V \in L$ *и* $V_i \in L, i = 1, \ldots, n$*, называемых простыми правилами вывода;*

(iii) набор условных правил вывода вида "из $\Gamma^0 \vdash V^0$ *и* $\Gamma^1 \vdash V^1$ *следует* $\Gamma \vdash V$*", где* $\Gamma^0, \Gamma^1, \Gamma$ *конечные подмножества* L*, и* $\{V^0, V^1, V\} \subset L$*.*

Определение 6.2 *Слово (формула)* $V \in L$ *называется непосредственным следствием слов (формул)* $\{V_1, V_2, \ldots, V_n\} \subset L$*, если либо* $V_1, V_2, \ldots, V_n \vdash V$*, где* $V_1, V_2, \ldots, V_n \vdash V$ *– одно из простых правил вывода в формальной системе* Φ*, либо если найдутся такие конечные множества* $\Gamma^0 \subset L$*,* $\Gamma^1 \subset L$ *и такие слова (формулы)* $V^0 \in L$ *и* $V^1 \in L$*, что правило "из* $\Gamma^0 \vdash V^0$ *и* $\Gamma^1 \vdash V^1$ *следует* $V_1, V_2, \ldots V_n \vdash V$*" является одним из условных правил вывода формальной системы* Φ*.*

Определение 6.3 *Слово (формула)* $V \in L$ *выводимо (доказуемо) из* $\{V_1, V_2, \ldots, V_n\} \subset L$*, если найдется такая последовательность формул* $\{W_i\}_{i=1}^k$*, где* $k \in \mathbf{N}$*, где* $W_k = V$ *и каждое из слов* $W_i \in L$*, где* $i = 1, \ldots, k$ *является*

(i) либо аксиомой формальной системы Φ*;*

(ii) либо одной из формул $V_1, V_2, \ldots, V_n$*;*

(iii) либо непосредственным следствием некоторого подмножества слов (формул) $\Gamma \subset \{W_1, W_2, \ldots, W_{i-1}\}$*.*

В этом случае будем писать

$$V_1, V_2, \ldots, V_n \vdash_\Phi V,$$

причем индекс Φ*, указывающий на используемую формальную систему, будем опускать, если это не ведет к неясности.*

Определение 6.4 *Формальная система* Φ *называется корректной, если для любого множества* $\Gamma \subset L$ *и для любого* $\mathcal{P} \in L$ *из* $\Gamma \vdash_\Phi \mathcal{P}$ *следует* $\Gamma \models \mathcal{P}$*, то есть все формальные истины, получаемые при помощи данной формальной системы, являются семантическими истинами.*

Определение 6.5 *Формальная система* Φ *называется полной, если для любого множества* $\Gamma \subset L$ *и для любого* $\mathcal{P} \in L$ *из* $\Gamma \models \mathcal{P}$ *следует* $\Gamma \vdash_\Phi \mathcal{P}$*, то есть все семантические истины можно получить формально.*

Таким образом определенное понятие формальной системы применимо вовсе не только к языкам логики. Это просто инструмент для операций с цепочками символов заданного формального языка.

Приведем простейший пример формальной системы.

Пример 6.1 *Рассмотрим язык* L*, совпадающий со множеством всех слов над алфавитом* $\{a, b\}$*, и формальную систему, содержащую*
две аксиомы
- $\vdash \ a$,
- $\vdash \ b$,

и бесконечное количество правил вывода, объединенных в две группы
- $\mathcal{A} \ \vdash \ a\mathcal{A}a$,
- $\mathcal{A} \ \vdash \ b\mathcal{A}b$,

где $\mathcal{A}$ *– любое непустое слово языка. Для этой формальной системы, например, можно получить* $\vdash aaa$, $\vdash bab$, $\vdash babab$. *В частности, из пустого множества выводимы любые палиндромы нечетной длины (цепочки символов, которые читаются одинаково слева направо и справа налево). Этот же пример показывает и различие семантической и формальной истин. К примеру, условимся считать "осмысленными" (семантически истинными) все палиндромы, а формальными истинами – всё, что выводимо из пустого множества. Тогда не все семантические истины оказываются формальными (то есть формальная система неполна), но формальные истины всегда являются семантическими, иначе говоря, формальная система корректна.*

Другой пример формальной системы, не имеющей отношения к логике: формальная система для языка записи шахматных позиций. У неё одна аксиома – это начальная позиция, а правила вывода – правила ходов. Стоит отметить, что в понятие позиции входит не только положение фигур на доске, но также и признаки того, делал ли игрок ход королем и кто из игроков сделал последний ход.

В следующем разделе мы будем изучать формальную систему, применимую к языку логики предикатов первого порядка, правила вывода которой моделируют те элементарные логические заключения, которые используют математики при доказательстве формул.

6.2 Естественная дедукция

Логические заключения, которые используют люди в своих рассуждениях, определяется рядом элементарных правил, которые сформулированы ещё Аристотелем. Формализация этих правил приводит к различным формальным системам

для логических языков. Впредь мы будем рассматривать одну из таких формальных систем для языка логики предикатов первого порядка, называемую *естественной дедукцией* (Natural deduction). Аксиом в ней нет, а правила вывода можно разделить на две группы: правила введения (обозначаются буквой i – "introduce", слева соответствующий значок отсутствует, справа присутствует), и правила исключения (обозначаются буквой e – "eliminate", справа соответствующий значок отсутствует, слева присутствует) для каждого логического значка и квантора ($\vee, \wedge, \to, \neg, \forall, \exists$). При формулировке этих правил мы покажем их запись в строчной форме и в форме столбца (дерева), а именно, строчную запись $\mathcal{A} \vdash \mathcal{B}$ можно заменить записью в столбец (в виде дерева) $\dfrac{\mathcal{A}}{\mathcal{B}}$.

$(\wedge e_1)$	правило исключения “и”	$\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{A}$	$\dfrac{\mathcal{A} \wedge \mathcal{B}}{\mathcal{A}}$
$(\wedge e_2)$	правило исключения “и”	$\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{B}$	$\dfrac{\mathcal{A} \wedge \mathcal{B}}{\mathcal{B}}$
$(\wedge i)$	правило введения “и”	$\mathcal{A}, \mathcal{B} \vdash \mathcal{A} \wedge \mathcal{B}$	$\dfrac{\mathcal{A} \quad \mathcal{B}}{\mathcal{A} \wedge \mathcal{B}}$
$(\vee i_1)$	правило введения “или” слева	$\mathcal{A} \vdash \mathcal{A} \vee \mathcal{B}$	$\dfrac{\mathcal{A}}{\mathcal{A} \vee \mathcal{B}}$
$(\vee i_2)$	правило введения “или” справа	$\mathcal{A} \vdash \mathcal{B} \vee \mathcal{A}$	$\dfrac{\mathcal{A}}{\mathcal{B} \vee \mathcal{A}}$
$(\vee e)$	правило исключения “или”	Если $\mathcal{A} \vdash \mathcal{C}$ и $\mathcal{B} \vdash \mathcal{C}$, то $\mathcal{A} \vee \mathcal{B} \vdash \mathcal{C}$	$\dfrac{\dfrac{[\mathcal{A}]_1}{\mathcal{C}} \quad \dfrac{[\mathcal{B}]_1}{\mathcal{C}} \quad \mathcal{A} \vee \mathcal{B}}{\mathcal{C}}{}_1$

Иначе говоря, последнее правило можно “прочесть” так: если $\mathcal{C}$ доказано с использование допущения $\mathcal{A}$, и $\mathcal{C}$ доказано с использованием допущения $\mathcal{B}$, и при этом мы знаем, что верно $\mathcal{A} \vee \mathcal{B}$, то можно считать доказанным $\mathcal{C}$ (уже без предположений о верности $\mathcal{A}$ и $\mathcal{B}$). В последнем правиле использовалось следующее обозначение: посылка в квадратных скобках означает, что её можно исключить из рассмотрения. Можно представить себе это как “обрывание” листьев дерева доказательства, соответствующих тем посылкам, которые можно исключить. Индексом около квадратных скобок показывается то место в дереве, где “оборванный лист” был использован (то есть посылки, заключенные в квадратные скобки, стали ненужными). Дерево доказательства можно читать так: необорванные листья доказывают корень. Читателю предоставляется возможность самому

разобраться, какой формой записи пользоваться удобно, а именно, запись в виде дерева весьма компактна, но не всегда легко читаема. Зато запись в строчку (с подробными комментариями), как правило, легко читается, но редко получается компактной.

$(\to e)$	правило исключения импликации или modus ponens (m.p.)	$\mathcal{A}, \mathcal{A} \to \mathcal{B} \vdash \mathcal{B}$	$\dfrac{\mathcal{A} \quad \mathcal{A} \to \mathcal{B}}{\mathcal{B}}$
$(\to i)$	правило введения импликации	Если $\mathcal{A} \vdash \mathcal{B}$ то $\vdash \mathcal{A} \to \mathcal{B}$	$\dfrac{\dfrac{[\mathcal{A}]_1}{\mathcal{B}}}{\mathcal{A} \to \mathcal{B}}{}^{1}$

Обратимся к правилам, имеющим дело с логическим значком отрицания. Введем псевдоформулу $\bot$ “ложь”, истинностное значение которой во всех интерпретациях будем считать нулем. С помощью такой псевдоформулы можно, например, весьма легко записать противоречивость множества формул Γ следующим образом:

$$\Gamma \models \bot.$$

Теперь можно сформулировать правила для значка отрицания и константы "ложь":

$(\bot e)$	правило исключения константы ложь.	$\bot \vdash \mathcal{A}$	$\dfrac{\bot}{\mathcal{A}}$

Данное правило допускает простую интерпретацию: из лжи следует все что угодно (ex falsum sequitor quodlibet). Даже несведущим в формальной логике людям это правило хорошо известно; например, оно применяется в житейском споре в виде восклицания “если это (очевидно ложное для собеседника утверждение) верно, то я Папа Римский”.

$(\bot i)$	правило введения константы “ложь”	$\neg\mathcal{A}, \mathcal{A} \vdash \bot$	$\dfrac{\neg\mathcal{A} \qquad \mathcal{A}}{\bot}$
$(\neg i)$	правило введения отрицания	Если $\mathcal{A} \vdash \bot$ то $\vdash \neg\mathcal{A}$	$\dfrac{\dfrac{[\mathcal{A}]_1}{\bot}}{\neg\mathcal{A}}{}^{1}$
(RAA)	правило сведения к противоречию (reductio ad absurdum)	Если $\neg\mathcal{A} \vdash \bot$ то $\vdash \mathcal{A}$	$\dfrac{\dfrac{[\neg\mathcal{A}]_1}{\bot}}{\mathcal{A}}{}^{1}$

Наиболее "нетривиальное" правило – последнее. При использовании этого правила непонятно, как конструктивно выписать $\vdash \mathcal{A}$, что породило два крупных направления в логике – классическая и интуиционистская (не принимает последнего правила). Чтобы доказать какое-либо утверждение, в интуиционистской логике необходимо предъявить цепочку доказательства.

Теорема 6.1 *Правило сведения к противоречию (RAA) эквивалентно закону исключенного третьего (tertium non datur)*

$$\vdash (\mathcal{A} \vee \neg\mathcal{A}) \qquad (TND)$$

Доказательство:

1. Докажем, что из правила сведения к противоречию (RAA) следует закон исключенного третьего (TND). Доказательство удобно записать в виде следующего дерева.

$$\dfrac{\dfrac{\dfrac{[\mathcal{A}]_1}{\neg\mathcal{A} \vee \neg\mathcal{A}} \quad [\mathcal{A} \vee \neg\mathcal{A}]_2}{\dfrac{\dfrac{\bot}{\neg\mathcal{A}}_1}{\mathcal{A} \vee \neg\mathcal{A}}} \qquad [\neg(\mathcal{A} \vee \neg\mathcal{A})]_2}{\dfrac{\bot}{\mathcal{A} \vee \neg\mathcal{A}}_2}$$

2. Докажем, что из закона исключенного третьего (TND) следует правило сведения к противоречию (RAA).

Пусть $\neg\mathcal{A} \vdash \bot$, тогда

$$\dfrac{\dfrac{}{\mathcal{A} \vee \neg\mathcal{A}} \qquad \dfrac{\dfrac{[\neg\mathcal{A}]_1}{\bot}}{\mathcal{A}} \qquad \dfrac{[\mathcal{A}]_1}{\mathcal{A}}}{\mathcal{A}}_1$$

Таким образом нами была доказана эквивалентность закона исключенного третьего и правила сведения к противоречию. □

Подход интуиционистов нельзя отметать сразу, поскольку уверенными можно быть в истинности только проверяемых утверждений. Рассмотрим в качестве примера утверждение о бесконечной последовательности бит, например

(i) данная последовательность состоит только из единиц;

(ii) в данной последовательности есть хотя бы один нуль.

Очевидно, что ни одно из этих утверждений не может быть проверено (для проверки их понадобилось бы бесконечное время). Классическая логика тем не менее утверждает, что ровно одно из утверждений (i) и (ii) является истинным (в силу закона исключенного третьего (TND)). Интуиционистский же подход в данном случае является более осторожным: поскольку ни одно из рассматриваемых утверждений практически проверено быть не может, то нельзя утверждать истинность того, что "верно либо (i), либо (ii)".

6.3 Подстановки в термах и формулах

Для того, чтобы сформулировать правила введения кванторов всеобщности и существования, будем считать неразличимыми формулы, которые отличаются только именами связанных переменных. Например, $\forall y P(x,y)$ и $\forall z P(x,z)$ будем считать одной и той же формулой.

Нам также понадобится ввести операцию замены переменных в формуле. В дальнейшем будем понимать под обозначением $\mathcal{P}[t/x]$, где $\mathcal{P} \in L_I^\sigma$, $x \in \mathbf{Var}$, и $t \in \mathbf{TER}(L_I^\sigma)$ замену всех вхождений переменной x на терм t. Мы определим замену переменных для языка логики первого порядка следующим образом.

Определение 6.6 *(***Замена переменных для термов***). Пусть $s, t \in \mathbf{TER}$, $x \in \mathbf{Var}$. Определим замену $s[t/x]$ следующим образом.*

(i) *Если $s = c \in \mathbf{Const}$, то $s[t/x] := c$.*

(ii) *Если $s = y \in \mathbf{Var}$, причем y отлично от x, то $s[t/x] := y$.*

(iii) *Если $s = x \in \mathbf{Var}$, то $s[t/x] := t$.*

(iv) *Если $s = f^k(t_1, \ldots, t_k)$, где f^k—k-арный функциональный символ, и $t_1, \ldots, t_k \in \mathbf{TER}(L_I^\sigma)$, то $s[t/x] := f^k(t_1[t/x], ..., t_k[t/x]$.*

Пример 6.2 *Пусть c—символ константы, x, y—символы предметных переменных, а f—тернарный функциональный символ. Тогда*

$$f(s(x,c),c,y)\left[f(x,s(x,y),y)/_x\right] = f(s(f(x,s(x,y),y),c),c,y)$$

Определение 6.7 *(***замена переменных для правильных формул***). Пусть $t \in \mathbf{TER}(L_I^\sigma)$, $x \in \mathbf{Var}$, $\mathcal{P}, \mathcal{Q} \in \mathbf{\Gamma}$, A^k—k-арный предикатный символ. Определим замену так:*

(i) *Если $\mathcal{P}$—атомная формула, т. е. $\mathcal{P} = A^k(t_1, ..., t_k)$, то*

$$\mathcal{P}[t/x] = A^k(t_1, ..., t_k)[t/x] := A^k(t_1[t/x], ..., t_k[t/x]).$$

(ii) *Если* $\mathcal{P} = (\neg\mathcal{Q})$, *то*

$$\mathcal{P}[t/x] := (\neg\mathcal{Q}[t/x]).$$

(iii) *Если* $\mathcal{P} = (\mathcal{R} * \mathcal{Q})$, *то*

$$(\mathcal{P})[t/x] = (\mathcal{R}[t/x] * \mathcal{Q}[t/x]),$$

где $*$*—это один из символов* $\wedge, \vee$ *или* $\rightarrow$.

(iv) *Если* $\mathcal{P} = (\zeta y\mathcal{Q})$, *где* ζ*—один из кванторов* $\forall$ *или* $\exists$, *то*

1. *Если* $y \neq x$ *и* $y \notin VAR(t)$, *то* $(\zeta y\mathcal{Q})[t/x] = (\zeta y\mathcal{Q}[t/x])$., *где* $VAR(t)$ *– множество всех символов предметных переменных в терме* t.
2. *Если* $y \neq x$, *но* $y \in VAR(t)$, *то* $(\zeta y\mathcal{Q})[t/x] = (\zeta r\mathcal{Q}[r/y][t/x])$, *где* $r \notin VAR(t)$ *(см. пример).*
3. *Если* $y = x$, *то замена не делается, т. е.* $(\zeta x\mathcal{Q})[t/x] = (\zeta x\mathcal{Q})$.

Пример 6.3 *Пусть* $<$ *– бинарный предикатный символ (вместо* $<(x, y)$ *будем писать* $x < y$*),* f *– унарный функциональный символ,* x *и* y *– символы предметных переменных. Тогда*

$$\exists y\,(x < y)\left[f\,(y)/_{x}\right] = \exists z\,(f\,(y) < z)$$

(а не $\exists y\,(f\,(y) < y)$*).*

Теперь мы можем сформулировать правила введения и исключения для кванторов всеобщности и существования:

$(\forall e)$	правило исключения квантора всеобщности	$\forall x\mathcal{A} \vdash \mathcal{A}\,[y/x]$ где $y \in TER(L_I^\sigma)$	$\dfrac{\forall x\mathcal{A}}{\mathcal{A}\,[y/x]}$
$(\forall i)$	правило введения квантора всеобщности	Если $\Gamma \vdash \mathcal{A}\,[y/x]$ то $\Gamma \vdash \forall x\mathcal{A}$ если $y \notin \bigcup\limits_{\mathcal{Q}\in\Gamma} \mathrm{free}(\mathcal{Q})$	$\dfrac{\mathcal{A}\,[y/x]}{\forall x\mathcal{A}}$

Заметим, что в последнем правиле весьма важно предположение о том, что y не входит свободно ни в одну из формул множества Γ (иначе говоря, y – "произвольная" переменная). Это правило иногда формулируют так: если $\Gamma \vdash \mathcal{A}\,[y/x]$ для произвольного y, то $\Gamma \vdash \mathcal{A}$ для любого x. Опустить "предположение" о произвольности y здесь нельзя. Например, введем в арифметике Пеано две формулы с одной свободной переменной: $\underline{Odd}(x)$ и $\underline{Even}(x)$, означающие по смыслу, что x соответственно "нечетное" или "четное" число. Запишем их следующим образом

$$\underline{Even}(x) := \exists y(\underline{2} \cdot y = x),$$

где $\underline{2} := s(s(0))$,

$$\underline{Odd}(x) := \underline{Even}(s(x))$$

Тогда в силу доказанного правила (id) имеем $\underline{Odd}(y) \vdash \underline{Even}(S(y))$

Однако неверно, что $\underline{Odd}(y) \vdash \forall x \underline{Even}(s(x))$. То есть из нечетности некоторого y не следует четность всех чисел! Правило введения квантора всеобщности было применено неправильно, поскольку символ предикатной переменной y, входящий в формулу, не являлся произвольным (он входил свободно в формулу-посылку).

Правила введения и исключения для квантора существования следующие:

$(\exists i)$	правило введения квантора существования	$\mathcal{A}[t/x] \vdash \exists x \mathcal{A}$ где $t \in TER(L_I^\sigma)$	$\dfrac{\mathcal{A}[t/x]}{\exists x \mathcal{A}}$
$(\exists e)$	правило исключения квантора существования	Если $\Gamma, \mathcal{A}[y/x] \vdash \mathcal{C}$ то $\Gamma, \exists x \mathcal{A} \vdash \mathcal{C}$ где $y \notin \bigcup\limits_{\mathcal{Q} \in \Gamma \cup \mathcal{C}} free(\mathcal{Q})$	$\dfrac{\exists x \mathcal{A} \quad \dfrac{[\mathcal{A}[y/x]]_1}{\mathcal{C}}}{\mathcal{C}}1$

В качестве примера докажем следующую метатеорему:

Теорема 6.2 $\vdash \exists x \left(\mathcal{A}\left(x\right) \to \forall y \mathcal{A}(y)\right)$ *для любой формулы* $\mathcal{A} \in L^\sigma$ *с одной свободной переменной.*

В вольной формулировке утверждение данной теоремы можно проинтерпретировать следующим образом: можно доказать, что найдется такой человек, что если он носит шляпу, то и все люди носят шляпу (или что существует такая лошадь, что если она синяя, то остальные лошади также синие).

Доказательство: Сначала докажем, что $\neg \mathcal{A}(x) \vdash \exists x(\mathcal{A}(x) \to \forall y(\mathcal{A}(y)))$. Доказательство представим в виде дерева

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg \mathcal{A}(x)]_2 \qquad [\mathcal{A}(x)]_1}{\bot}(\bot i)}{\forall y(\mathcal{A}(y))}\bot e}{\mathcal{A}(x) \to \forall y \mathcal{A}(y)}(1, \to i)}{\exists x(\mathcal{A}(x) \to \forall y \mathcal{A}(y))}(\exists i)$$

Теперь предположим дополнительно, что $\neg \exists x(\mathcal{A}(x) \to \forall y \mathcal{A}(y))$. Получим

$$\dfrac{\dfrac{\dfrac{\dfrac{\exists x(\mathcal{A}(x)\to\forall y\mathcal{A}(y)) \quad \underline{[\neg\exists x(\mathcal{A}(x)\to\forall y\mathcal{A}(y))]_2}_{(\bot i)}}{\bot}_{(\bot e)}}{\mathcal{A}(x)}_{(\forall i)}}{\forall y\mathcal{A}(y)}_{(\to i)}}{\mathcal{A}(x)\to\forall y\mathcal{A}(y)}_{(\exists i)}}{\exists x(\mathcal{A}(x)\to\forall y\mathcal{A}(y))}$$

При доказательстве было использовано новое правило вывода $\mathcal{B}\vdash\mathcal{A}\to\mathcal{B}$. Справедливость такого правила вывода доказывается так:

$$\dfrac{\dfrac{[\mathcal{A}]_2 \quad \mathcal{B}}{\mathcal{B}}_{(2\to i)}}{\mathcal{A}\to\mathcal{B}}$$

Таким образом доказано, что $\vdash\exists x\left(\mathcal{A}\left(x\right)\to\forall y\mathcal{A}(y)\right)$ $\square$.
В интуиционистской теории данная метатеорема неверна (использован закон исключенного третьего (TND)). Объясняется же она просто: либо все люди носят шляпы, либо есть человек, который шляпу не носит, тогда он и есть искомый.

В качестве второго примера докажем, что в арифметике Пеано никакой элемент не следует сам за собой.

Теорема 6.3

$$(PA)\vdash\forall x\left(\neg s\left(x\right)=x\right).$$

Доказательство: Будем пользоваться принципом математической индукции. Доказательство построим в несколько этапов.

1. База индукции:
   $(PA)\vdash\neg s\left(0\right)=0$. Доказательство использует аксиому(PA_1).

$$\dfrac{\forall x\neg s\left(x\right)=0}{\neg s\left(0\right)=0}$$

2. Докажем $(PA)\vdash\forall x\left(\neg s\left(x\right)=x\to\neg s\left(s\left(x\right)\right)=s\left(x\right)\right)$. Доказательство удобно представить в виде дерева

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x\forall y(s(x)=s(y)\to x=y)}{\forall y(s(x)=s(y)\to x=y)}}{s(x)=s(s(x))\to x=s(x)} \quad [s(x)=s(s(x))]_1}{x=s(x)} \quad [\neg x=s(x)]_2}{\dfrac{\dfrac{\dfrac{\bot}{\neg s(x)=s(s(x))}_1}{\neg x=s(x)\to\neg s(x)=s(s(x))}_2}{\forall x(\neg x=s(x)\to\neg s(x)=s(s(x)))}}$$

3. Используя результаты шагов 1 и 2 и правило $(\wedge i)$ получаем

$$(PA)\vdash s\left(0\right)=0\wedge\forall x\left(\neg s\left(x\right)=x\to\neg s\left(s\left(x\right)\right)=s\left(x\right)\right).$$

4. Произведем подстановку в схему аксиом индукции (PA_7) на место $\mathcal{P}$ формулы с одной свободной переменной

$$\mathcal{P}\left(x\right):=\neg s\left(x\right)=x.$$

   В результате получим

$$(PA)\vdash s\left(0\right)=0\wedge\forall x\left(\neg s\left(x\right)=x\to\neg s\left(s\left(x\right)\right)=s\left(x\right)\right)\to\forall x(\neg s\left(x\right)=x).$$

5. Из результатов шагов 3 и 4, с помощью правила modus ponens получим

$$(PA)\vdash\forall x\neg s\left(x\right)=x,$$

   что и требовалось доказать. □

6.4 Корректность и полнота естественной дедукции

Напомним определения корректности и полноты формальной системы.

Определение 6.8 *Формальная система для языка L^σ называется*

- *корректной, если для любых $\Gamma\subset L^\sigma$, $\mathcal{P}\in L^\sigma$ из $\Gamma\vdash\mathcal{P}$ следует $\Gamma\models\mathcal{P}$;*
- *полной, если для любых $\Gamma\subset L^\sigma$, $\mathcal{P}\in L^\sigma$ из $\Gamma\models\mathcal{P}$ следует $\Gamma\vdash\mathcal{P}$.*

Иначе говоря, формальная система корректна, если для произвольного набора формул Γ все выводимые (доказуемые в данной формальной системе) из него формулы являются семантическими следствиями Γ, и полна, если, наоборот, все семантические следствия Γ выводимы из Γ при помощи этой формальной системы. Иногда пользуются и следующими более слабыми понятиями, которые требуют выполнения соответствующих условий только для $\Gamma = \emptyset$.

Определение 6.9 *Формальная система для языка L^σ называется*

- *корректной в слабом смысле, если для любой формулы $\mathcal{P} \in L^\sigma$ из $\vdash \mathcal{P}$ следует $\models \mathcal{P}$;*
- *полной в слабом смысле, если для любой формулы $\mathcal{P} \in L^\sigma$ из $\models \mathcal{P}$ следует $\vdash \mathcal{P}$.*

Требование корректности формальной системы является совершенно естественным. Действительно, если формальная система корректной не является, то найдется такая система аксиом Γ и такая теорема $\mathcal{P}$, что $\mathcal{P}$ можно доказать с использованием этой формальной системы и множества посылок Γ, но в то же время $\mathcal{P}$ семантически не следует из Γ. Так что такая формальная система не удовлетворяет своему предназначению – формальными синтаксическими манипуляциями выводить именно только логические следствия. Другое дело – свойство полноты. Оно является в некотором смысле более сильным, так как означает возможность при помощи данной формальной системы вывести любое логическое следствие произвольного множества формул Γ.

Теорема 6.4 (о корректности) *Естественная дедукция корректна.*

Доказательство: Пусть $\Gamma \subset L^\sigma$, $\mathcal{P} \in L^\sigma$ и $\Gamma \vdash \mathcal{P}$. Докажем $\Gamma \models \mathcal{P}$ индукцией по глубине n дерева вывода формулы $\mathcal{P}$ (т. е. количеству шагов вывода). Иначе говоря, сначала докажем $\Gamma \models \mathcal{P}$ для случая деревьев, в которых не использовано ни одно правило вывода ($n = 0$), затем, предполагая, что $\Gamma \models \mathcal{P}$ доказано для всех деревьев вывода глубиной $n \leq k$, докажем справедливость этого утверждения для случая $n = k + 1$. При этом в силу принципа математической индукции утверждение будет доказано для всех возможных деревьев вывода $\Gamma \vdash \mathcal{P}$ независимо от глубины.

База индукции. Пусть $n = 0$. Тогда $\mathcal{P} \in \Gamma$, а значит, $\Gamma \models \mathcal{P}$.

Шаг индукции. Пусть утверждение доказано для всех $n \leq k$. Предположим, что $\Gamma \vdash \mathcal{P}$ за $n = k + 1$ шаг. Рассмотрим все возможные правила вывода, которые могли быть использованы на последнем шаге для получения формулы $\mathcal{P}$, и докажем для каждого случая $\Gamma \models \mathcal{P}$.

($\wedge e$) Это значит $\mathcal{P} = \mathcal{P}_1$, причем $\Gamma \vdash \mathcal{P}_1 \wedge \mathcal{P}_2$ и за k шагов, а значит, в силу предположения индукции $\Gamma \models \mathcal{P}_1 \wedge \mathcal{P}_2$. Следовательно, в любой модели всех одновременно формул Γ $v(\mathcal{P}_1 \wedge \mathcal{P}_2) = 1$, а значит, $v(\mathcal{P}) = v(\mathcal{P}_1) = 1$, то есть $\Gamma \models \mathcal{P}$.

($\wedge i$) В этом случае $\mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2$, причем $\Gamma \vdash \mathcal{P}_1$ и $\Gamma \vdash \mathcal{P}_2$ не более чем за k шагов, а значит, в силу предположения индукции $\Gamma \models \mathcal{P}_1$ и $\Gamma \models \mathcal{P}_2$. Рассмотрим любую модель всех одновременно формул Γ. Мы только что доказали, что $v(\mathcal{P}_1) = 1$ и $v(\mathcal{P}_2) = 1$, но тогда и $v(\mathcal{P}) = v(\mathcal{P}_1 \wedge \mathcal{P}_2) = 1$, иначе говоря, $\Gamma \models \mathcal{P}$.

($\to i$) Тогда $\mathcal{P} = \mathcal{P}_1 \to \mathcal{P}_2$, причем $\Gamma, \mathcal{P}_1 \vdash \mathcal{P}_2$ за k шагов, а значит, в силу предположения индукции $\Gamma, \mathcal{P}_1 \models \mathcal{P}_2$. Рассмотрим любую модель всех одновременно формул Γ. Если в этой модели $v(\mathcal{P}_1) = 1$, то в силу только что доказанного $v(\mathcal{P}_2) = 1$, а значит и $v(\mathcal{P}) = v(\mathcal{P}_1 \to \mathcal{P}_2) = 1$. Но если $v(\mathcal{P}_1) = 0$, то $v(\mathcal{P}) = v(\mathcal{P}_1 \to \mathcal{P}_2) = 1$. Таким образом, в любом случае $\Gamma \models \mathcal{P}$.

1. ($\forall i$) Тогда $\mathcal{P} = \forall x \mathcal{Q}$, причем $\Gamma \vdash \mathcal{Q}[y/x]$ за k шагов. Значит, $\Gamma \models \mathcal{Q}[y/x]$ в силу предположения индукции. Рассмотрим любую интерпретацию $(\mathcal{M}, \xi)$, являющуюся моделью всех одновременно формул Γ. Тогда для любого $b \in M$ при $\xi(y) = b$ имеем $v(\mathcal{Q}[y/x]) = 1$, а значит, $v(\mathcal{P}) = v(\forall x \mathcal{Q}) = 1$. Следовательно, $\Gamma \models P$.

Все остальные случаи, соответствующие правилам вывода, которые могли быть применены на последнем шаге вывода для получения формулы $\mathcal{P}$, предлагается разобрать в качестве упражнения.

Упражнение 6.1 *Докажите, что из выполнимости множества формул* Γ *следует его непротиворечивость в естественной дедукции.*

Полнота естественной дедукции. Исторически первая теорема о полноте формальной системы была доказана К. Геделем, поэтому традиционно всякую теорему о полноте некоторой формальной системы принято называть теоремой Геделя о полноте этой системы. Соответственно, в данном случае мы имеем дело с теоремой Геделя о полноте классической естественной дедукции. Доказательство ее будет основано на следующей теореме:

Теорема 6.5 (о модели) *Пусть множество формул* Γ *совместно в смысле классической естественной дедукции. Тогда* Γ *выполнимо (т. е. имеет модель).*

Теорема 6.6 (о полноте) *Классическая естественная дедукция полна.*

Доказательство: Пусть $\Gamma \subset L^\sigma$, $\mathcal{P} \subset L^\sigma$ такие, что $\Gamma \models \mathcal{P}$. Тогда множество $\Gamma \cup \{\neg\mathcal{P}\}$ невыполнимо, а значит, в силу теоремы о модели, и несовместно в классической естественной дедукции. Иначе говоря, $\Gamma, \neg\mathcal{P} \vdash \bot$. Применяя правило сведения к противоречию (RAA), или ($\neg e$), получаем $\Gamma \vdash \mathcal{P}$.

Для доказательства теоремы о модели нам понадобится ряд вспомогательных конструкций.

Определение 6.10 *Будем говорить, что множество $\Gamma \subset L^\sigma$ содержит свидетелей, если для любой формулы вида $\exists x\mathcal{P} \in L^\sigma$ найдется такой терм $t \in TER(L^\sigma)$ (называемый свидетелем), что $\exists x\mathcal{P} \to \mathcal{P}[t/x] \in \Gamma$.*

Важно отметить следующее: для того, чтобы множество $\Gamma \subset L^\sigma$ содержало свидетелей, мало наличия соответствующих термов-свидетелей только для существовательных формул из Γ. Они должны найтись для любой существовательной формулы всего языка L^σ.

Определение 6.11 *Γ называется максимально совместным множеством, если оно строго не содержится ни в одном другом совместном множестве.*

Лемма 6.1 *Если множество Γ является максимально совместным, то $\Gamma \vdash \mathcal{P}$ если и только если $\mathcal{P} \in \Gamma$.*

Доказательство: Нетривиальным является только доказательство того, что $\Gamma \vdash \mathcal{P}$ влечет $\mathcal{P} \in \Gamma$. Предположим противное, т. е. $\Gamma \vdash \mathcal{P}$, но $\mathcal{P} \notin \Gamma$. Тогда множество $\Gamma \cup \{\mathcal{P}\}$ совместно, что противоречит исходному предположению о максимальной совместности множества Γ. Действительно, иначе бы $\Gamma, \mathcal{P} \vdash \bot$, а значит, в силу правила ($\neg i$), $\Gamma \vdash \neg\mathcal{P}$, что вместе с предположением $\Gamma \vdash \mathcal{P}$ приводит к противоречию $\Gamma \vdash \bot$.

Теперь мы можем перейти непосредственно к основной конструкции доказательства теоремы о модели. Зададимся целью построить модель $(\mathcal{M}_\Gamma, \xi_\Gamma)$ совместного множества формул Γ. Для этого выберем в качестве универсума $\mathcal{M}_\Gamma$ множество термов языка L^σ, т. е. $\mathcal{M}_\Gamma := TER(L^\sigma)$. Положим $c^{\mathcal{M}_\Gamma} := c$ для любого символа предметной константы $c \in \mathbf{Const}$, $f^{\mathcal{M}_\Gamma}(t_1, t_2, \ldots, t_n) := f(t_1, t_2, \ldots, t_n)$ для любого n-арного функционального символа $f \in \mathbf{Func}^n$ и

$$A^{M_\Gamma}(t_1, t_2, \ldots t_n) := \begin{cases} 1, & A(t_1, t_2, \ldots t_n) \in \Gamma, \\ 0, & \text{иначе} \end{cases}$$

для каждого n-арного предикатного символа $A \in \mathbf{Pred}^n$, и, наконец, $\xi_\Gamma(x) := x$ для любого символа предметной переменной $x \in \mathbf{Var}$.

Лемма 6.2 *Если* Γ *содержит свидетелей и является максимально совместным, то* $(\mathcal{M}_\Gamma, \xi_\Gamma) \models \mathcal{P}$*, если и только если* $\Gamma \vdash \mathcal{P}$*. В частности, построенная интерпретация* $(\mathcal{M}_\Gamma, \xi_\Gamma)$ *является моделью всех одновременно формул множества* Γ*.*

Доказательство: Для доказательства воспользуемся теоремой об индукции по структуре формул языка L^σ.

База индукции. Пусть $\mathcal{P}$ – атомная формула, т. е. $\mathcal{P} = A(t_1, t_2, \ldots, t_n)$. Тогда непосредственно из нашей конструкции следует, что условие $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}$ выполняется в том и только в том случае, когда $\mathcal{P} = A(t_1, t_2, \ldots, t_n) \in \Gamma$, а это, в свою очередь, эквивалентно тому, что $\Gamma \vdash \mathcal{P}$.

Шаг индукции.

1. Пусть $\mathcal{P} = \neg\mathcal{Q}$. Тогда условие $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}$ эквивалентно условию $(M_\Gamma, \xi_\Gamma) \not\models \mathcal{Q}$. В силу предположения индукции последнее эквивалентно $\Gamma \nvdash \mathcal{Q}$, что в силу максимальной совместности Γ выполняется, если и только если $\mathcal{Q} \notin \Gamma$. Докажем теперь, что в силу максимальной совместности Γ условие $\mathcal{Q} \notin \Gamma$ эквивалентно условию $\neg\mathcal{Q} \in \Gamma$. Действительно, если $\neg\mathcal{Q} \in \Gamma$, то $\mathcal{Q} \notin \Gamma$, иначе множество Γ не было бы совместным. Если же $\mathcal{Q} \notin \Gamma$, то так как множество $\Gamma \cup \{\mathcal{Q}\}$ несовместно в силу предположения о максимальной совместности множества Γ, можно заключить по правилу $(\neg i)$, что $\Gamma \vdash \neg\mathcal{Q}$, или $\neg\mathcal{Q} \in \Gamma$ в силу леммы 6.1.

   Таким образом, доказано, что $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}$, если и только если $\mathcal{P} = \neg\mathcal{Q} \in \Gamma$. Но последнее ввиду леммы 6.1 эквивалентно $\Gamma \vdash \mathcal{P}$.

2. Пусть $\mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2$. Тогда условие $(M_\Gamma, \xi_\Gamma) \models P$ выполнено, если и только если одновременно $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}_1$ и $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}_2$. В силу предположения индукции $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}_i$, $i = 1, 2$, эквивалентно условию $\Gamma \vdash \mathcal{P}_i$. Таким образом, доказано, что $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}$, если и только если одновременно $\Gamma \vdash \mathcal{P}_1$ и $\Gamma \vdash \mathcal{P}_2$. Но последнее эквивалентно $\Gamma \vdash \mathcal{P} = \mathcal{P}_1 \wedge \mathcal{P}_2$. Действительно, если $\Gamma \vdash \mathcal{P}_i$, $i = 1, 2$, то $\Gamma \vdash \mathcal{P}_1 \wedge \mathcal{P}_2$ в силу правила $(\wedge i)$. Наоборот, пусть $\Gamma \vdash \mathcal{P}_1 \wedge \mathcal{P}_2$. Тогда $\Gamma \vdash P_i$ в силу правил $(\wedge e.1)$ и $(\wedge e.2)$.

3. Пусть $\mathcal{P} = \exists x\mathcal{Q}$. Тогда условие $(M_\Gamma, \xi_\Gamma) \models \mathcal{P}$ выполнено, если и только если существует такой терм $t \in TER(L^\sigma) = M_\Gamma$, что $(M_\Gamma, \xi_\Gamma[t/x]) \models \mathcal{Q}$. Но последнее условие эквивалентно $(M_\Gamma, \xi_\Gamma) \models \mathcal{Q}[t/x]$ (докажите это в качестве упражнения!), что в свою очередь в силу предположения индукции эквивалентно условию $\Gamma \vdash \mathcal{Q}[t/x]$. Докажем, что $\Gamma \vdash Q[t/x]$ выполняется тогда и только тогда, когда $\Gamma \vdash \exists x\mathcal{Q}$, т. е. $\Gamma \vdash \mathcal{P}$. Действительно, из $\Gamma \vdash P[t/x]$ следует $\Gamma \vdash \exists x\mathcal{Q}$ в силу правила $(\exists i)$. Наоборот, если $\Gamma \vdash \exists x\mathcal{Q}$, то так как Γ содержит свидетелей, то найдется такой терм-свидетель $t \in TER(L^\sigma)$, что $\exists x\mathcal{Q} \to P[t/x] \in \Gamma$. Тогда в силу modus ponens $\Gamma \vdash \mathcal{Q}[t/x]$.

Все остальные случаи, соответствующие возможной структуре формулы $\mathcal{P}$ (т. е. случаи $\mathcal{P} = \mathcal{P}_1 \vee \mathcal{P}_2$, $\mathcal{P} = \mathcal{P}_1 \to \mathcal{P}_2$ и $\mathcal{P} = \forall x \mathcal{Q}$), предлагается разобрать в качестве упражнения.

Доказанная лемма указывает на возможный путь построения модели для произвольного совместного множества формул Γ. Действительно, достаточно дополнить множество Γ до максимально совместного множества, содержащего свидетелей. Последнее будет выполнимым, а значит, тем более будет выполнимым и множество Γ. Вся сложность в дополнении множества Γ до максимально совместного множества, содержащего свидетелей. К сожалению, в общем случае выполнить его конструктивно (т.е. непосредственно «предъявив» конструкцию расширенного множества) не удастся.

Построим новую сигнатуру σ^*, содержащую σ, а также дополнительно для каждой формулы вида $\exists x \mathcal{P} \in L^\sigma$ новый (т. е. не содержащийся в σ) символ предметной константы $c_\mathcal{P}$, разный для разных формул. В новом языке логики предикатов первого порядка $L^* := L^{\sigma^*}$ содержится, таким образом, весь язык L^σ. В этом новом языке дополним множество Γ всеми формулами вида $\exists x \mathcal{P} \to \mathcal{P}[c_\mathcal{P}/x]$, где $c_\mathcal{P}$ – «новый» символ предметной константы, соответствующий формуле $\exists x \mathcal{P}$. Полученное расширенное множество обозначим Γ^*.

Лемма 6.3 *Множество* Γ *совместно, если и только если совместно множество* Γ^*.

Доказательство: Докажем, что из $\Delta, \exists x \mathcal{P} \to \mathcal{P}[c_\mathcal{P}/x] \vdash \mathcal{Q}$, где $\Delta \subset L^\sigma$ и $\mathcal{P}, \mathcal{Q} \in L^\sigma$, а $c_\mathcal{P}$ – «новый» (т. е. отсутствующий в сигнатуре σ и добавленный в соответствии с конструкцией σ^*) символ предметной константы, следует $\Delta \vdash \mathcal{Q}$.

Действительно, если $\Delta, \exists x \mathcal{P} \to \mathcal{P}[c_\mathcal{P}/x] \vdash \mathcal{Q}$, то $\Delta \vdash (\exists x \mathcal{P} \leftarrow \mathcal{P}[c_\mathcal{P}/x]) \to \mathcal{Q}$ в силу правила $(\to i)$. Но тогда $\Delta \vdash \exists x \mathcal{P} \leftarrow \mathcal{P}[y/x] \to \mathcal{Q}$, где y – символ предметной переменной, не входящий свободно ни в формулу $\mathcal{Q}$ и ни в одну из формул множества Δ (докажите это!). Из правила $(\forall i)$ следует при этом $\Delta \vdash \forall y(\exists x \mathcal{P} \to \mathcal{P}[y/x] \to \mathcal{Q})$. Но так как $\forall y(\exists x \mathcal{P} \to \mathcal{P}[y/x] \to \mathcal{Q}) \vdash \exists y(\exists x \mathcal{P} \to \mathcal{P}[y/x]) \to \mathcal{Q}$, а $\exists y(\exists x \mathcal{P} \to \mathcal{P}[y/x]) \to \mathcal{Q} \vdash (\exists x \mathcal{P} \to \exists y \mathcal{P}) \to \mathcal{Q}$ и $\vdash \exists x \mathcal{P} \to \exists y \mathcal{P}$ (докажите эти утверждения!), то $\Delta \vdash \mathcal{Q}$.

Пусть теперь Γ^* несовместно, т. е. $\Gamma^* \vdash \bot$. Это значит, что $\Gamma, \mathbf{R}_1, \ldots, \mathbf{R}_n \vdash \bot$ для какого-то конечного числа «добавленных» формул $\mathbf{R}_i$ вида $\mathbf{R}_i := \exists x \mathcal{P}_i \to \mathcal{P}[c_{\mathcal{P}_i}/x]$. Докажем индукцией по n, что тогда $\Gamma \vdash \bot$. Действительно, для $n = 0$ это утверждение тривиально. Но если оно верно для $n = k$, и $\Gamma, \mathbf{R}_1, \ldots, \mathbf{R}_{k+1} \vdash \bot$, то $\Gamma', \mathbf{R}_{k+1} \vdash \bot$, где $\Gamma' := \Gamma \cup \{\mathbf{R}_1, \ldots, \mathbf{R}_k\}$. Так как символ предметной константы $c_{\mathcal{P}_{k+1}}$ не входит ни в одну из формул Γ, то по только что доказанному $\Gamma' \vdash \bot$, а значит, $\Gamma \vdash \bot$ в силу предположения индукции.

Пусть теперь

$$\begin{array}{rclrclrcll} L_0 & := & L^\sigma, & \sigma_0 & := & \sigma, & \Gamma_0 & := & \Gamma, & \\ L_{k+1} & := & L_k^*, & \sigma_{k+1} & := & \sigma_k^*, & \Gamma_{k+1} & := & \Gamma_k^*, & k \in \mathbf{N}, \\ L_\omega & := & \bigcup_{k\in\mathbf{N}} L_k, & \sigma_\omega & := & \bigcup_{k\in\mathbf{N}} \sigma_k, & \Gamma_\omega & := & \bigcup_{k\in\mathbf{N}} \Gamma_k. & \end{array}$$

Лемма 6.4 *Пусть множество* Γ *совместно. Тогда множество* Γ_ω *совместно и содержит свидетелей.*

Доказательство: Рассмотрим произвольную формулу вида $\exists x\mathcal{Q} \in L^{\sigma_\omega}$. Тогда $\exists x\mathcal{Q} \in L_k$ для какого-то $k \in \mathbf{N}$, следовательно, найдется такой добавленный на $k+1$ шаге символ предметной константы $c_\mathcal{Q} \in \sigma_{k+1} \setminus \sigma_k$, что $\exists x\mathcal{Q} \to \mathcal{Q}[c_\mathcal{Q}/x] \in \Gamma_{k+1} \subset \Gamma_\omega$, а значит, множество Γ_ω содержит свидетелей.

Докажем теперь, что Γ_ω совместно. Предположим противное, т.е. $\Gamma_\omega \vdash \bot$. Значит, найдется такое конечное множество посылок $\Delta \subset \Gamma_\omega$ (листья дерева доказательства $\Gamma_\omega \vdash \bot$), что $\Delta \vdash \bot$. Но так как по определению последовательность множеств $\{\Gamma_i\}_{i\in\mathbf{N}}$ расширяющаяся и объединение всех множеств этой последовательности есть Γ_ω, то $\Delta \subset \Gamma_k$ для какого-нибудь $k \in \mathbf{N}$. Значит, $\Gamma_k \vdash \bot$, что противоречит лемме 6.3, в силу которой все Γ_i, $i \in \mathbf{N}$ совместны.

Следующая лемма, эквивалентная аксиоме выбора в теории множеств, чрезвычайно широко используется в математике. Она является ключевым элементом и доказательства теоремы о модели (а следовательно, и теоремы о полноте классической естественной дедукции).

Лемма 6.5 (Цорн) *Пусть частичный порядок* $(\Psi, <)$*, таков, что любой содержащийся в нем линейный порядок имеет максимальный элемент. Тогда* $(\Psi, <)$ *имеет максимальный элемент.*

Теорема 6.7 (Линденбаум) *Любое совместное множество формул содержится в некотором максимальном совместном множестве.*

Доказательство: Пусть $\Gamma \subset L^\sigma$ – заданное совместное множество формул. На множестве совместных подмножеств языка L^σ, содержащих Γ, введем отношение порядка следующим образом: будем говорить, что $\Gamma_1 < \Gamma_2$, если $\Gamma_1 \subset \Gamma_2$. Соответствующий частичный порядок обозначим $(\Psi, <)$. Рассмотрим произвольный линейный порядок $(F, <)$, содержащийся в $(\Psi, <)$. Докажем, что объединение Φ всех множеств формул из F, является максимальным элементом порядка $(F, <)$. Очевидно, Φ содержит Γ. С другой стороны, Φ совместно. Действительно, иначе бы $\Phi \vdash \bot$, а значит, нашлось бы такое конечное множество посылок $\Delta \subset \Phi$ (листья дерева доказательства $\Phi \vdash \bot$), что $\Delta \vdash \bot$. Но так как Φ – объединение расширяющегося семейства множеств F, то найдется такое множество формул $\Phi_0 \in F$, что $\Delta \subset \Phi_0$, а значит, $\Phi_0 \vdash \bot$, что противоречит совместности всех элементов F.

Таким образом, доказано, что любой линейный порядок $(F, <)$, содержащийся в $(\Psi, <)$, имеет максимальный элемент. Для доказательства существования максимального совместного множества, содержащего Γ (т. е. максимального элемента порядка $(\Psi, <)$), остается сослаться на лемму Цорна.

Теперь мы в состоянии легко доказать теорему о модели 6.5.

Доказательство теоремы 6.5 (о модели):
Пусть $\Gamma \subset L^\sigma$ – заданное совместное множество формул. Построим язык L_ω и множество формул $\Gamma_\omega \subset L_\omega$. В силу леммы 6.4 множество Γ_ω совместно и содержит свидетелей. По теореме Линденбаума найдется максимально совместное множество $\Gamma'_\omega \subset L_\omega$, содержащее Γ_ω (поэтому оно тем более будет содержать свидетелей). Это множество формул выполнимо ввиду леммы 6.2, а значит, тем более выполнимо и содержащееся в нем множество Γ.

Единственной неприятной особенностью конструкции доказательства теоремы о модели является то, что для языков с равенством предикатный символ равенства будет интерпретироваться в построенной модели некоторым бинарным отношением на соответствующем универсуме, которое, вообще говоря, будет отличным от отношения равенства, понимаемого в смысле совпадения элементов универсума. Однако это доказательство легко исправить с учетом требования интерпретации символа равенства отношением совпадения элементов универсума. Действительно, достаточно на множестве термов $TER(L_\omega)$ расширенного языка L_ω ввести отношение эквивалентности "$\sim$" следующим образом: будем говорить, что $t_1 \sim t_2$, если атомная формула $t_1 = t_2$ содержится во множестве Γ'_ω (проверьте, что это действительно отношение эквивалентности, т. е. оно рефлексивно, симметрично и транзитивно). Тогда в качестве универсума конструируемой модели выберем фактор-множество $M := TER(L_\omega)/\sim$ (т.е. множество классов эквивалентных термов). Обозначая класс термов, эквивалентных данному терму t, за $[t]$, положим $c^{\mathcal{M}} := \tilde{c}$ для каждого символа предметной константы $c \in \mathbf{Const}$, $f^{\mathcal{M}}([t_1], [t_2], \ldots, [t_n]) := [f(t_1, t_2, \ldots, t_n)]$ для каждого n-арного функционального символа $f \in \mathbf{Func}^n$,

$$A^{\mathcal{M}}([t_1], [t_2], \ldots, [t_n]) := \begin{cases} 1, & A(t_1, t_2, \ldots, t_n) \in \Gamma'_\omega \\ 0, & \text{иначе} \end{cases}$$

для каждого n-арного предикатного символа $A \in \mathbf{Pred}^n$, и, наконец, $\xi_\Gamma([x]) := [x]$ для любого символа предметной переменной $x \in Var$. Осталось проверить, что данное определение корректно и действительно задает модель всех одновременно формул множества Γ'_ω, а значит, и меньшего множества Γ. Проведите эту проверку самостоятельно в качестве упражнения, фактически только слегка поправляя доказательство леммы 6.2.

7 Основы теории моделей

Из самого факта существования корректных и полных формальных систем для языков логики первого порядка следует целый ряд весьма нетривиальных выводов о семантике этих языков. А именно, о том какие модели и сколько моделей (с точностью до изоморфизма) могут иметь множества формул языков логики первого порядка. В этой главе мы рассмотрим основные нетривиальные результаты о семантике языков логики первого порядка.

Теорема 7.1 (О семантической компактности)

(i) *Множество формул* $\Gamma \subset L^\sigma$ *выполнимо (то есть имеет модель) тогда и только тогда, когда любое его конечное подмножество выполнимо.*

(ii) Γ *логически выводит* $\mathcal{P}$ *тогда и только тогда, когда найдется такое конечное* $\Delta \subset \Gamma$*, что* $\Delta \models \mathcal{P}$.

Доказательство:

(i) Докажем, что если Γ выполнимо, то любое его конечное подмножество выполнимо. Если Γ выполнимо, то существует такая интерпретация, в которой все одновременно формулы Γ истинны. Значит, эта же интерпретация является моделью любого подмножества $\Delta \subset \Gamma$. Необходимость доказана. Теперь докажем достаточность. Пусть Γ невыполнимо, а все конечные подмножества Γ выполнимы, тогда, по теореме о модели, Γ несовместно, то есть $\Gamma \vdash \bot$. Но, в силу определения формальной системы, найдется такое конечное подмножество Γ (листья дерева вывода псевдоформулы $\bot$), что $\Delta \vdash \bot$. По теореме о корректности естественной дедукции Δ невыполнимо, что противоречит предположению.

(ii) Для доказательства этого пункта заметим, что в силу теоремы о корректности и полноте естественной дедукции $\Gamma \models \mathcal{P}$, если и только если $\Gamma \vdash \mathcal{P}$, последнее же, в силу определения формальной системы, возможно, если, и только если найдется такое конечное $\Delta \subset \Gamma$ (листья дерева доказательства формулы $\mathcal{P}$), что $\Delta \vdash_{\mathbf{ND}} \mathcal{P}$. Снова применяя теорему о корректности и полноте естественной дедукции получаем, что последнее эквивалентно $\Delta \models \mathcal{P}$.

Займемся теперь вопросом о том, какие модели и сколько разных (с точностью до изоморфизма) моделей может иметь множество формул $\Gamma \subset L^\sigma$ языка логики первого порядка. Здесь и далее мы будем говорить о конечных, счетных, более чем счетных моделях, имея в виду, соответственно, модели с конечным, счетным, более чем счетным универсумом. Вообще под мощностью модели будем понимать мощность универсума.

Теорема 7.2 (Лёвенгейма—Скулема "сверху вниз" или о понижении мощности модели)
Пусть множество формул $\Gamma \subset L^\sigma$ выполнимо. Тогда оно имеет модель мощности не превышающей мощность языка.

Доказательство: Так как множество Γ выполнимо, то оно совместно (в силу теоремы о корректности естественной дедукции). Рассмотрим теперь более подробно доказательство теоремы о модели. Эта теорема утверждает что любое выполнимое множество имеет модель. Там модель "кроилась" из термов расширенного языка $L^{\sigma *}$. В силу конструкции, $\#L^{\sigma *} \leq \#L^\sigma$, а значит и $\#TER(L^{\sigma *}) \leq \#L^\sigma$. Таким образом, в силу конструкции, использованной в доказательстве теоремы о модели, можно утверждать существование модели с мощностью, не превышающей $\#TER(L^{\sigma *})$, а значит и $\#L^\sigma$. $\square$

Теорема 7.3 (О переходе от конечной к бесконечной мощности)
Если множество формул $\Gamma \subset L^\sigma$ выполнимо в моделях сколь угодно большой конечной мощности, Γ выполнимо и в бесконечной модели.

Доказательство: Рассмотрим $\Gamma' := \Gamma \cup \{\mathcal{P}_{\geq i}\}_{i=1}^{\infty}$, где

$$\mathcal{P}_{\geq k} \;:=\; \exists x_1 \ldots \exists x_k \left(\neg x_1 = x_2 \wedge \neg x_2 = x_3 \wedge \ldots \wedge \neg x_1 = x_k\right). \tag{7.1}$$

Заметим, что формула $\mathcal{P}_{\geq k}$ выполнима во всех моделях, универсум которых содержит по меньшей мере k элементов, и только в них. В силу теоремы о компактности, для проверки выполнимости Γ' достаточно проверить выполнимость любого его конечного подмножества $\Delta \subset \Gamma'$. Однако, если $\Delta \subset \Gamma'$ конечно, то $\Delta \subset \Gamma \cup \{\mathcal{P}_{\geq i}\}_{i=1}^{n}$, для конечного $n \in \mathbf{N}$. Множество $\Gamma \cup \{\mathcal{P}_{\geq i}\}_{i=1}^{n}$ выполнимо в той модели Γ, которая содержит не менее k элементов. Существование такой модели предполагается в условии теоремы. Следовательно, в этой же модели тем более выполнимо и меньшее множество формул Δ, а значит и Γ' выполнимо. Выполнимость же Γ тривиально следует из выполнимости Γ'. $\square$

Теорема 7.4 (Лёвенгейма—Скулема "снизу вверх" или о повышении мощности модели)
Пусть $\Gamma \subset L^\sigma$ имеет бесконечную модель. Тогда, для любого множества A, Γ имеет модель, универсум которой имеет мощность не меньше $\#A$.

Доказательство: Дополним сигнатуру σ языка L^σ новыми символами констант вида c_a, для всех $a \in A$, так, чтобы среди добавленных символов не было бы символов исходной сигнатуры и разным элементам множества A соответствовали разные добавленные символы констант. Получим новую сигнатуру σ', такую что $\#\sigma' \geq \#A$. Таким образом $\#L^{\sigma'} \geq \#A$.

Рассмотрим множество $\Gamma' := \Gamma \cup \{\neg c_a = c_b : a, b \in A, a \neq b\}$. Рассмотрим произвольное конечное подмножество $\Delta \subset \Gamma'$. В силу конечности Δ, имеем

$$\Delta \subset \Gamma \cup \{\neg c_{a_i} = c_{b_j} : i, j \leq n\}$$

для некоторого $n \in \mathbf{N}$. По условию теоремы множество формул Γ имеет модель $\mathcal{M}$ с бесконечным универсумом. В этой модели закрепим за символами констант c_{a_i} элементы M таким образом, чтобы $c^{\mathcal{M}}_{a_i} \neq c^{\mathcal{M}}_{b_j}$ при $a_i \neq b_j$. В полученной алгебраической системе все формулы множества Δ будут истинны, иначе говоря, Δ выполнимо. Следовательно, по теореме о компактности, выполнимо и Γ'. Заметим теперь, что любая модель множества Γ' должна иметь мощность не меньшую, чем $\#A$, так как в ней истинны все формулы вида $c_a \neq c_b$, где $a, b \in A$ и $a \neq b$. Но эта же модель будет автоматически и моделью меньшего множества Γ, что и завершает доказательство теоремы. $\square$

Первое весьма нетривиальное приложение доказанных утверждений к арифметике Пеано отвечает на вопрос о существовании нестандартных моделей арифметики.

Следствие 7.1 *Формальная арифметика Пеано первого порядка $PA^{\models}_I$ имеет модели, неизоморфные стандартной, в том числе и модели сколь угодно большой мощности.*

Нетривиальность данного утверждения заключается в том, что арифметика Пеано первого порядка допускает бесконечное число разных версий натуральных чисел и действий над ними, в том числе и несчетных. Предлагаем читателю самому разобраться с тем, как устроен этот несчетный натуральный ряд. Автор не может себе этого представить. Несколько успокаивает то, что доказанные теоремы неконструктивны, поскольку они опираются на теорему о модели, для доказательства которой существенно использовалась аксиома выбора. Таким образом,

как и в теореме о модели модель совместного множества формул, существование которой утверждается в теореме, не может быть предъявлена в силу неконструктивности доказательства, так и здесь "странные" модели, существование которых утверждается теоремами Левенгейма–Скулема далеко не всегда могут быть явным образом сконструированы.

Интересно также сравнить утверждения следствия с теоремой Дедекинда для арифметики Пеано второго порядка. Приведенное следствие позволяет догадаться, что языки логики первого порядка обладают намного меньшей выразительной силой, например, охарактеризовать модель с точностью до изоморфизма при помощи аксиом языка логики первого порядка (как это было для языков второго порядка) невозможно. Действительно, по теореме Левенгейма–Скулема, любое множество аксиом для арифметических формул арифметики первого порядка, если только оно выполнимо в стандартной модели, будет выполнимо и в моделях со сколь угодно большими мощностями.

Теорема 7.5 (Лёвенгейма—Скулема—Тарского) *Пусть $\Gamma \subset L^\sigma$ имеет бесконечную модель, пусть A произвольное множество, такое что $\#A \geq \#L^\sigma$ (то есть $\#A$ не меньше мощности языка). Тогда Γ имеет модель с универсумом, равномощным A.*

Доказательство: Дополним сигнатуру σ новыми символами констант вида c_a для каждого $a \in A$, таким образом, чтобы разные элементам множества A соответствовали разным символам констант. Обозначим

$$\sigma' = \sigma \cup \{c_a \,:\, a \in A\}$$

$$\Gamma' = \Gamma \cup \{\neg c_a = c_b \,:\, a, b \in A, a \neq b\},$$

заметим, что $\Gamma' \subset L^{\sigma'}$. Множество Γ в силу предположения имеет бесконечную модель, следовательно, по теореме Левенгейма-Скулема "снизу вверх", оно имеет модель мощности, превосходящей $\#A$. Иначе говоря, в универсуме найдется достаточное количество различных элементов, которые можно поставить в соответствие новым константам вида c_a, чтобы таким образом получить модель множества Γ'.

Поскольку множество Γ', таким образом, выполнимо, у него найдется модель $(\mathcal{M}, \xi)$, такая что $\#\mathcal{M} < \#L^{\sigma'}$. С другой стороны, $\#\mathcal{M} \geq \#A$, поскольку в $(\mathcal{M}, \xi)$ истинны все формулы вида $\neg c_a = c_b$, где $a, b \in A$, $a \neq b$. Таким образом, получим

$$\#A \leq \#\mathcal{M} \leq \#L^{\sigma'} \leq \#\mathcal{A},$$

иначе говоря $\#\mathcal{M} = \#A$. $\square$

Обратимся ещё раз к вопросу о моделях формальной арифметики Пеано первого порядка, неизоморфных стандартной. Существование таких моделей уже утверждалось в следствии 7.1. Сейчас мы докажем несколько более сильное утверждение, а именно, что формальная арифметика Пеано первого порядка имеет счетную модель, неизоморфную стандартной.

Теорема 7.6 *Существует счетная нестандартная модель арифметики Пеано первого порядка* $PA_I^{\models}$.

Доказательство:

Дополним формальную арифметику Пеано всеми формулами вида $\neg x = \underline{n}$, где $\underline{1} := s(0), \underline{2} := s(\underline{1}), \underline{n} := s(\underline{n-1})$, а именно, определим

$$\Gamma' := PA_I^{\models} \cup \{\neg x = \underline{n}\}_{n=0}^{\infty},$$

где x – символ предметной переменной. Докажем выполнимость Γ', для чего воспользуемся теоремой о компактности. Рассмотрим произвольное конечное подмножество $\Delta \subset \Gamma'$. Имеем

$$\Delta \subset PA_I^{\models} \cup \{\neg x = \underline{n}\}_{n=0}^{k}$$

для некоторого конечного $k \in \mathbf{N}$. Очевидно, что множество $\{\neg x = \underline{n}\}_{n=0}^{k}$ имеет модель $(\mathcal{N}, \xi)$, где $\xi(x) := k+1$, а $\mathcal{N}$ – стандартная модель арифметики. Эта же интерпретация является, тем более, и моделью меньшего множества Δ. Мы доказали, таким образом, выполнимость любого конечного $\Delta \in \Gamma'$, а значит, в силу теоремы о компактности, и выполнимость Γ'. Рассмотрим модель Γ', существование которой мы только что доказали. Она не может быть конечной в силу того, что в ней должны быть одновременно истинны (PA_1) и (PA_2), то есть должна существовать инъективная, но не сюръективная функция, определенная на универсуме этой модели. Следовательно, по теореме Левенгейма-Скулема "сверху вниз" найдется и счетная модель $(\mathcal{M}, \xi)$ множества Γ' (она не может быть конечной по той же причине).

Осталось доказать, что $\mathcal{M}$ неизоморфна $\mathcal{N}$, то есть не существует биекции π между натуральным рядом и универсумом $\mathcal{M}$. Предположим, что она существует, а именно, существует биекция $\pi : \mathbf{N} \to M$, такая, что и для любого терма n выполнено $\pi\left(n^{\mathcal{N}}\right) = n^{\mathcal{M}}$. Тогда $\xi(x) \notin Im(\pi)$, иначе в данной модели не была бы верна одна из формул вида $\neg x = \underline{k}$, но последнее противоречит сюрьективности π. Следовательно, $\mathcal{M}$ неизморфна $\mathcal{N}$. $\square$

В отличие от результатов, сформулированных в следствии 7.1, утверждение теоремы 7.6 можно сравнительно легко проинтерпретировать. А именно, "версия" натурального ряда, существование которой утверждается в этой теореме, выглядит следующим образом. Сначала идут "обычные" натуральные числа, затем идет число $\xi^{\mathcal{M}}(x)$, которое не следует ни за каким "обычным" натуральным числом (заметим, что в стандартной модели таким свойством обладает только число 0). И далее, вслед за числом $\xi^{\mathcal{M}}(x)$ идут числа $s^{\mathcal{M}}(\xi^{\mathcal{M}}(x)), s^{\mathcal{M}}(s^{\mathcal{M}}(\xi^{\mathcal{M}}(x)))\ldots$ Таким образом, естественно считать такого рода числа, которые в этой "версии" натурального ряда находятся "правее" всех "обычных" натуральных чисел, бесконечно большими (они "больше" любого "обычного" натурального числа). На основе полученного таким образом натурального ряда можно построить, также как это делается с использованием привычного нам натурального ряда $\mathbf{N}$, новую версию целых, рациональных и вещественных чисел. Естественно, что в построенной таким образом версии вещественной оси найдутся как бесконечно большие, так и бесконечно малые числа (соответственно большие и меньшие по модулю всех "обычных" вещественных чисел). Использовать такую "необычную" (принято говорить *нестандартную*) версию чисел очень удобно для альтернативного построения математического анализа. Например, с использованием нестандартной вещественной оси можно "изгнать" из анализа "неудобоваримые" определения предела, бесконечно малой величины, а пользоваться лишь бесконечно малыми *числами*. При этом все определения, которые обычно даются с использованием достаточно тяжелого "языка ϵ, δ" существенно упрощаются. Математический анализ, построенный при помощи этого подхода, называется *нестандартным анализом.*

8 Сравнение языков логики разных порядков

Сформулированные нами в предыдущей главе результаты о моделях множества формул языков логики первого порядка позволяют получить нетривиальные выводы о сравнении выразительной силы логических языков. Начнем со следующего простого вопроса: можно ли при помощи формул языка логики первого или второго порядка охарактеризовать свойство модели быть конечной? Строгая постановка этого вопроса такова:

Вопрос 1 *Существует ли множество формул языка логики первого (соответственно, второго) порядка, истинное во всех конечных моделях и только в них? Напомним, что, говоря о мощности модели, мы имеем в виду мощность соответствующего универсума. То есть модель называется конечной (счетной,*

не более чем счетной), если соответствующим свойством обладает универсум модели.

Ответ на заданный выше вопрос для языков логики первого порядка, очевидно, отрицательный вследствие теоремы 7.3: если множество формул верно во всех конечных моделях, то оно будет иметь и бесконечную модель. В то же время в языке логики второго порядка данный факт можно выразить всего лишь одним предложением:

$$\mathcal{P}_{\text{fin}} := \forall f\,(\forall x \forall y\,(f\,(x) = f\,(y) \to x = y) \to \forall x \exists y\,(x = f\,(y)))$$

Здесь использован квантор всеобщности по "функциональной переменной", а именно, данная формула "говорит", что во всех моделях, в которых она истинна, любая инъекция является сюръекцией. Это и означает, что в универсуме модели данной формулы не может быть бесконечного числа элементов. Стоит напомнить, что, строго говоря, согласно нашему определению, в алфавите языка логики второго порядка нет специальных символов для функциональных переменных, а есть только символы для предикатных переменных, поэтому формулу $\mathcal{P}_{\text{fin}}$ нужно понимать как сокращенную запись формулы

$$\forall F(\underline{func}(F) \wedge \forall x \forall y \forall z(F(x,z) \wedge F(y,z) \to x = y) \to \forall x \exists y(F(y,x))),$$

где

$$\underline{func}(F) := \forall x \exists! y\, F(x,y),$$

(иначе говоря, формула $\underline{func}(F)$ "говорит" о том, что отношение, записанное символом предикатной переменной F, является графиком функции)

Вопрос, аналогичный вопросу 1, можно сформулировать и для других свойств модели, например, для свойства модели быть не более чем счетной. А именно:

Вопрос 2 *Существует ли множество формул языка логики первого (соответственно второго) порядка, истинное во всех не более чем счетных моделях и только в них?*

Опять-таки, ответ на этот вопрос для языков логики первого порядка отрицательный в силу теоремы Левенгейма–Скулема–Тарского 7.5, а именно, если у множества формул есть счетная модель, то у него есть и модель сколь угодно большой мощности. В то же время, для языков логики второго порядка можно

охарактеризовать свойство модели быть не более чем счетной одним предложением, а именно, предложением

$$\mathcal{P}_{count} := \exists z \exists f \forall X \left(X\left(z\right) \wedge \forall x \left(X\left(x\right) \rightarrow X\left(f\left(x\right)\right)\right) \rightarrow \forall x \left(X\left(x\right)\right)\right)$$

Здесь f снова символ "функциональной переменной", которая, строго говоря, в силу нашего определения, в языке логики второго порядка отсутствует, так что формулу $\mathcal{P}_{count}$ нужно понимать как сокращенную запись другой формулы, в которой вместо символа f присутствует символ предикатной переменной. Запишите соответствующую формулу самостоятельно, по аналогии с тем, как это было сделано для формулы $\mathcal{P}_{fin}$.

Можно предъявить сколь угодно много свойств моделей, которые не могут быть охарактеризованы никакими формулами языков логики первого порядка, но могут быть легко охарактеризованы формулами языков логики второго порядка. Например, формула $\mathcal{P}_{count} \wedge \neg \mathcal{P}_{fin}$ характеризует свойство модели быть счетной. В то же время соответствующее свойство не может быть охарактеризовано формулами языка логики первого порядка.

Упражнение 8.1 *Напишите предложение, которое характеризует свойство модели иметь более чем счетный универсум, иначе говоря, предложение, которое было бы верно во всех более чем счетных моделях и только в них. Можно ли охарактеризовать соответствующее свойство при помощи языка логики первого порядка с не более чем счетным алфавитом? С любым алфавитом?*

Любопытно отметить, что, тем не менее, свойство модели иметь *заданное* конечное число элементов может быть охарактеризовано и при помощи языка логики первого порядка. Например формула $\forall x \forall y (x = y)$ верна во всех моделях, универсум которых содержит ровно один элемент, и только в них.

Упражнение 8.2 *На языке логики первого порядка напишите предложения, характеризующие свойства модели иметь не более чем k элементов (k – заданное число), ровно k элементов, не менее чем k элементов.*

Приведенных рассуждений вполне достаточно, чтобы сформулировать следующие весьма сильные утверждения.

Теорема 8.1 *Для языков логики второго порядка теорема о компактности неверна.*

Доказательство: Предположим противное и рассмотрим множество формул

$$\Gamma := \left\{\mathcal{P}_{\text{fin}}\right\} \cup \{\mathcal{P}_{\geq k}\}_{k=1}^{\infty},$$

где формулы $\mathcal{P}_{\geq k}$ определены в (7.1). Пусть $\Delta \subset \Gamma$ конечно, тогда

$$\Delta \subset \left\{\mathcal{P}_{\text{fin}}\right\} \cup \{\mathcal{P}_{\geq k}\}_{k=1}^{m}$$

для некоторого конечного $m \subset \mathbf{N}$. Однако последнее множество формул истинно в любой модели, универсум которой имеет хотя бы m элементов, а значит, выполнимо и множество формул Δ. Тогда, в силу предположения о верности теоремы о компактности и произвольности подмножества Δ заключаем, что множество Γ также является выполнимым. Но тогда в модели Γ должно быть не менее чем k элементов для любого $k \in \mathbf{N}$ (так как в этой модели истинны все формулы $\mathcal{P}_{\geq k}$). И в то же время число элементов этой модели должно быть конечно, так как в ней верна формула $\mathcal{P}_{fin}$. Так как одновременно эти два условия невыполнимы, то мы пришли к противоречию. □

Теорема 8.2 *Для языков логики второго порядка неверны теоремы Левенгейма–Скулема о повышении мощности модели 7.4 и о понижении мощности модели 7.2.*

Доказательство: Если бы для языков логики второго порядка была верна теорема Левенгейма–Скулема о повышении мощности модели, то нельзя было бы написать множество формул, выражающее счетность модели. Если бы для языков логики второго порядка была верна теорема Левенгейма–Скулема о понижении мощности модели, то нельзя было бы написать множество формул, выражающее более чем счетность модели. □

Завершим эту главу наиболее сильным, на наш взгляд, результатом.

Теорема 8.3 *Для логики второго порядка не существует одновременно полной и корректной формальной системы.*

Доказательство: Предположение о существовании одновременно корректной и полной формальной системы влечет справедливость теоремы о компактности (в доказательстве теоремы о компактности для языков логики первого порядка использовался лишь факт существования одновременно корректной и полной формальной системы), что противоречит теореме 8.1. □

Требование корректности является необходимым для осмысленности формальной системы: формальная система строится для того, чтобы получать логические, то есть семантические, истины, поэтому некорректная формальная система, которая позволяет выводить в том числе формулы, не являющиеся истинными, не имеет никакой практической ценности. Только что доказанная теорема утверждает, таким образом, что осмысленная (т.е. корректная) формальная система для языка логики второго порядка не может быть полной. Иначе говоря, при помощи такой формальной системы мы не можем вывести *все* семантические истины. В то же время другого инструмента, пригодного для поиска на практике семантических следствий для заданного множества формул, кроме вывода при помощи некоторой формальной системы, нет. Поэтому утверждение теоремы 8.3 фактически является препятствием к широкому использованию языков логики второго порядка. Языки логики второго порядка являются, таким образом, "чересчур" выразительными, настолько, что их чрезмерная выразительная сила ограничивает возможность их применения. В этом смысле языки логики первого порядка являются вполне подходящими, так как инструмент для их использования (достаточно удобные формальные системы) существует, и в то же время, как показывает опыт, при помощи языка логики первого порядка можно записывать практически все важные естественнонаучные теории, хотя и нельзя охарактеризовать какую-нибудь серьезную модель однозначно.

9 Формальная теория множеств

В качестве еще одного примера языка логики первого порядка, находящего самые широкие применения в современной математике, рассмотрим язык теории множеств. Определим язык теории множеств как язык $L^{\in}$ логики первого порядка с равенством, с сигнатурой, содержащей лишь один символ, отличный от равенства – символ предиката принадлежности $\in$. Иначе говоря, $\sigma(L^{\in}) := \{=, \in\}$. Принято писать $x = y$ и $x \in y$ вместо $= (x, y)$ и $\in (x, y)$ соответственно. Например, мы будем считать формулы $x = y$, $\exists x \in y \wedge z \in q$ правильными формулами языка $L^{\in}$. Как и принято в математике, мы будем интерпретировать эти формулы соответственно как "множества x и y совпадают" и "существует множество x, принадлежащее множеству y, и множество z принадлежит множеству q". Несколько необычным с точки зрения наивной теории множеств является утверждение о том, что одно множество *принадлежит* другому. Привычнее говорить о том, что *элемент* принадлежит множеству. Однако заметим, что во введенном языке имеются символы предметных переменных только одного сорта, а именно – только для обозначения множеств (нет специального сорта переменных для обозначения

элементов множеств). Поэтому, имея дело с семантикой языка $L^{\in}$, мы будем интерпретировать все предметные переменные как "множества". Таким образом мы будем иметь дело с миром, состоящим только из одного типа объектов – "множеств". При этом нас не будет интересовать, насколько понятие "множества" как элемента интерпретирующего универсума соответствует интуитивному понятию множества как совокупности разных объектов. К этому вопросу мы еще вернемся в дальнейшем.

Несмотря на то, что введенный в рассмотрение язык $L^{\in}$ кажется весьма бедным, на нем можно выразить все привычные факты о множествах (а также, и всю математику – но об этом речь пойдет чуть позже). Например, "x подмножество y" можно записать в виде правильной формулы языка $L^{\in}$, которую будем обозначать $\underline{x \subset y}$, следующим образом:

$$\underline{x \subset y} := \forall z(z \in x \to z \in y).$$

Здесь и далее подчеркивание указывает на то, что мы имеем дело с сокращенным обозначением правильной формулы. Чуть позже мы еще займемся "кодированием" основных математических понятий в виде формул $L^{\in}$. А теперь покажем, что к перенесению основных интуитивных понятий о множествах на формальный язык $L^{\in}$ нужно подходить с большой осторожностью. Рассмотрим следующий пример.

Парадокс Рассела-Фреге. Мы привыкли формировать множества путем группирования элементов, обладающих заданным свойством (принято обозначать $\{x : P(x)\}$ множество элементов, обладающих свойством P). Попробуем формализовать такой способ формирования множеств на языке $L^{\in}$. А именно, логично предположить, что множество $z := \{x : \mathcal{P}(x)\}$ существует для любого "свойства" (т. е. формулы $L^{\in}$ с одной свободной переменной). Это легко записать в виде формулы

$$\exists z \forall x(x \in z \leftrightarrow \mathcal{P}(x)),$$

где $\#\mathbf{free}(\mathcal{P}) = 1$ (здесь и далее запись $\mathcal{A} \leftrightarrow \mathcal{B}$ понимается как сокращенная запись формулы $(\mathcal{A} \to \mathcal{B}) \wedge (\mathcal{B} \to \mathcal{A})$. Каким бы заманчивым с интуитивной точки зрения ни было это утверждение, оно ведет к абсурду. Действительно, выберем в качестве P свойство множества не принадлежать самому себе, то есть $\mathcal{P}(x) := \neg x \in x$. Тогда для множества $z := \{x : \neg x \in x\}$, очевидно, выполняется либо $z \notin z$, либо $z \in z$, причем в силу определения множества z в первом случае $z \in z$, а во втором $z \notin z$. С более формальной точки зрения это означает, что предложение

$$\mathcal{Q} := \exists z \forall x(x \in z \leftrightarrow \neg x \in x)$$

противоречиво.

Приведенный парадокс, который, несмотря на его название, был впервые обнаружен Г. Кантором, показывает что далеко не все интуитивно осмысленные предложения введенного формального языка теории множеств имеют право на существование. Поэтому для построения содержательной и осмысленной формальной теории множеств явно недостаточно интуиции, основанной на наивных представлениях о множествах. Традиционный способ выхода из такой ситуации – ограничить формальную теорию множеств утверждениями, выводимыми из достаточно простого, понятного и непротиворечивого набора аксиом. В то же время математика развивалась в течение по крайней мере последних двух с половиной тысяч лет и накопила за это время огромный набор фактов, давно ставших достоянием как собственно математики, так и всех использующих ее наук. Теория же множеств как основание математики появилась сравнительно недавно, начиная с работ Г. Кантора в 70-х годах 19 века. Поэтому система аксиом для формальной теории множеств кроме непротиворечивости должна обладать еще и следующим важным с прикладной точки зрения свойством: она не должна существенным образом обеднять создаваемую на ее основе формальную теорию множеств и математику в целом. В связи с особой важностью теории множеств для построения современной математики на протяжении 20 века было предпринято много попыток предоставить такой набор аксиом. Ни одна из предложенных аксиоматик не была абсолютно удачной, так что проблема формального обоснования современной математики до сих пор остается открытой. В то же время хотелось бы предостеречь от немедленных попыток взяться за решение этой проблемы. Дело в том, что, во-первых, существует несколько вполне удовлетворительных для практических целей аксиоматик (наиболее популярные среди них – аксиоматики Цермело-Френкеля и Геделя-Бернайса), а во-вторых, полное решение проблемы формального обоснования вряд ли что-либо изменит в развитии современной математики. Вскоре мы подробнее рассмотрим эти вопросы. А сейчас выпишем с небольшими комментариями аксиомы наиболее простой и часто используемой аксиоматики формальной теории множеств, предложенной *Цермело* и *Френкелем*.

9.1 Аксиоматика Цермело-Френкеля. Основные аксиомы

- **Аксиома объемности**.

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \leftrightarrow x = y) \qquad (ZF_1)$$

Эта аксиома говорит о том, что множество однозначно определяется своими элементами. Очень часто она используется в доказательстве единственности различных специальных множеств (например, пустого множества).

- **Аксиома пары**.

$$\forall x \forall y \exists z \forall v (v \in z \leftrightarrow v = x \vee v = y). \qquad (ZF_2)$$

Целесообразно записать ее в сокращенном виде, введя для множества z – пары элементов x и y обозначение

$$\underline{z = \{x, y\}} := \forall v (v = x \vee v = y \leftrightarrow v \in z).$$

Таким образом, (ZF_2) можно записать в виде

$$\forall x \forall y \exists z (\underline{z = \{x, y\}}),$$

то есть утверждается, что из любых двух элементов можно построить множество-пару.

- **Аксиома выделения**.

$$\forall x \exists y \left(\forall z \left(z \in y \leftrightarrow (z \in x) \wedge \mathcal{P}(z)\right)\right), \qquad x, y \notin \mathbf{free}(\mathcal{P}), \qquad \#\mathbf{free}(\mathcal{P}) = 1. \qquad (ZF_3)$$

Эта аксиома представляет собой исправленный вариант обсуждавшегося выше принципа, по которому можно формировать множества путем группирования элементов, обладающих заданным свойством. В исходном варианте, как было показано, этот принцип ведет к противоречию. Способ слегка подправить его с целью получить в действительности часто используемый в математике факт, очень прост – достаточно заметить, что на практике множества всегда формируются путем *выделения* элементов, обладающих заданным свойством, из заданного множества, а не просто путем группирования "всех вообще" элементов с заданным свойством. Так например, множество $\{n : n^2 - 1 = 0\}$ на самом деле получено выделением элементов из $\mathbf{N}$ (то есть правильнее было бы писать $\{n \in \mathbf{N} : n^2 - 1 = 0\}$). Такой способ исправления основного принципа формирования множества по заданному свойству его элементов был предложен Фреге и реализован в (ZF_3).

- **Аксиома множества подмножеств**. Для сокращения записи введем общепринятое обозначение для множества y всех подмножеств заданного множества x: $\underline{y = 2^x} := \forall z (\underline{z \subset x} \leftrightarrow z \in y)$. Заметим, что в данном определении использовано ранее введенное сокращение – формула $\underline{z \subset x}$. Рассматриваемая аксиома позволяет формировать новое множество как множество всех подмножеств заданного множества и может быть с использованием введенных обозначений записана в виде

$$\forall x \exists y (\underline{y = 2^x}). \qquad (ZF_4)$$

- **Аксиома суммы** говорит о существовании объединения произвольного множества множеств. Для удобства записи введем обозначение для объединения (иногда называемого также суммой) всех элементов множества x (напомним, что все объекты, с которыми мы работаем – множества):

$$\underline{y = \cup x} := \forall z(z \in y \leftrightarrow \exists v(v \in x \wedge z \in v)).$$

  С учетом введенного обозначения аксиома суммы записывается в виде

$$\forall x \exists y(\underline{y = \cup x}). \qquad (ZF_5)$$

Прежде чем рассмотреть оставшиеся четыре аксиомы Цермело-Френкеля, потренируемся в "кодировании" основных фактов о множествах на языке $L^{\in}$ и в их доказательстве с использованием уже введенных аксиом. Будем обозначать систему аксиом Цермело-Френкеля (кроме аксиомы выбора) ZF.

Пример 9.1 *Докажем существование и единственность пустого множества, то есть множества, не содержащего ни одного элемента. Для этого введем общепринятое обозначение:*

$$\underline{x = \emptyset} := \forall y(\neg y \in x).$$

Требуется доказать $ZF \vdash \exists! x(\underline{x = \emptyset})$. *Напомним, что* $\exists! x\, \mathcal{P}(x)$ *– общепринятое сокращение формулы*

$$\exists x\, \mathcal{P}(x) \wedge \forall y \forall x(\mathcal{P}(y) \wedge \mathcal{P}(x) \to x = y).$$

Доказательство:

Существование. Аксиома (ZF_3) записывается в виде

$$\forall x \exists y \forall z(z \in y \leftrightarrow z \in x \wedge (\neg z = z)).$$

Применяя правило $(\forall e)$, получаем $(ZF_3) \vdash \exists y\, \mathcal{R}$, где

$$\mathcal{R} := \forall z(z \in y \leftrightarrow z \in x \wedge (\neg z = z)).$$

Теперь докажем $R \vdash \forall z(\neg z \in y)$. Это доказательство удобно представить в виде

дерева

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\forall z(z \in y \leftrightarrow z \in x \wedge (\neg z = z))}{z \in y \leftrightarrow z \in x \wedge (\neg z = z)}\ (\forall e)}{z \in y \rightarrow z \in x \wedge (\neg z = z)}\ (\wedge e) \qquad [z \in y]_1}{z \in x \wedge (\neg z = z)}\ (m.p.)}{\neg z = z}}{\dfrac{\bot}{\neg z \in y}\ 1,\ (\neg i)}\ (\forall i)}{\forall z(\neg z \in y)}$$

Осталось объединить две "ветви" для завершения доказательства:

$$\dfrac{\dfrac{(ZF_3)}{\exists y\, \mathcal{R}} \qquad \dfrac{[\mathcal{R}]_2}{\forall z(\neg z \in y)}}{\exists y \forall z(\neg z \in y)}\ 2$$

(здесь применено одновременно несколько правил; мы предоставляем читателям возможность самим убедиться в корректности соответствующего перехода).

Единственность. Надо доказать

$$ZF \vdash \forall x \forall y(\forall z(\neg z \in y) \wedge \forall z(\neg z \in x) \rightarrow (x = y)).$$

Представим доказательство в виде дерева

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall z(\neg z \in x) \wedge \forall z(\neg z \in y)]_1}{\forall z(\neg z \in x)}}{\neg z \in x} \qquad \dfrac{\dfrac{[\forall z(\neg z \in x) \wedge \forall z(\neg z \in y)]_1}{\forall z(\neg z \in y)}}{\neg z \in y}}{\neg z \in x \wedge \neg z \in y}}{z \in x \leftrightarrow z \in y} \qquad \dfrac{(ZF_1)}{\forall z\ \ (z \in x \leftrightarrow z \in y) \rightarrow (x = y)}}{\forall z\ \ (z \in x \leftrightarrow z \in y)}}{x = y}\ 1}{\forall z(\neg z \in x) \wedge \forall z(\neg z \in y) \rightarrow x = y}}{\forall x \forall y\ \ (\forall z(\neg z \in x) \wedge \forall z(\neg z \in y) \rightarrow x = y)}$$

Предоставляем читателю определить, какие правила применены на каждом шаге доказательства, а также заполнить недостающие фрагменты. После этого останется объединить доказательство существования с доказательством единственности при помощи правила $(\wedge i)$. $\square$.

Упражнение 9.1 *Доказать*

(A) $ZF \vdash \forall x \forall y \exists! z(\underline{z = x \cup y})$, *где*

$$\underline{z = x \cup y} := \forall v(v \in z \leftrightarrow v \in x \vee v \in y)$$

(существование и единственность объединения множеств).

(B) $ZF \vdash \forall x \exists! y(\underline{y = \{x\}})$, *где*

$$\underline{y = \{x\}} := \underline{y = \{x, x\}}$$

(существование и единственность одноэлементного множества, содержащего заданный элемент).

Указание:

(A) Для доказательства существования использовать аксиому суммы, примененную к множеству-паре $\{x, y\}$. Существование последнего гарантируется аксиомой пары. Для доказательства единственности использовать аксиому объемности.

(B) Использовать аксиому пары и аксиому объемности.

Упражнение 9.2 *Введем упорядоченную пару как пару с выделенным первым элементом:*

$$\underline{x = (y, z)} := \underline{x = \{\{y\}, \{y, z\}\}}.$$

Доказать

$$ZF \vdash \forall y \forall z \exists x(\underline{x = (y, z)}).$$

Указание: Для доказательства существования упорядоченной пары (y, z) использовать уже доказанные факты существования одноэлементного множества $\{y\}$ и пары $\{y, z\}$, затем еще раз сослаться на существования пары, элементами которой будут только что построенные множества. Для доказательства единственности использовать аксиому объемности.

Упражнение 9.3

(C) Введем следующее обозначение для векторов, обобщающее понятие упорядоченной пары:

$$\underline{x = (x_1, ..., x_n)} := \underline{x = (x_1, (x_2, ..., x_n))}.$$

Докажите $ZF \vdash \forall x_1 \forall x_2 \exists! y(\underline{y = x_1 \times x_2})$, *где*

$\underline{y = x_1 \times \ldots \times x_n} := \forall u(u \in y \leftrightarrow \exists z_1 ... \exists z_n(z_1 \in x_1 \wedge \ldots \wedge z_n \in x_n \wedge \underline{u = (z_1, \ldots, z_n)}))$

(существование и единственность декартова произведения множеств).

(D) Доказать $ZF \vdash \forall x(\neg \underline{x = \emptyset}) \exists! y(\underline{y = \cap x})$, *где*

$$\underline{y = \cap x} := \forall z(z \in y \leftrightarrow \forall v(v \in x \rightarrow z \in v))$$

(существование и единственность пересечения произвольного числа множеств).

(E) Доказать $ZF \vdash \forall x \forall y \exists! z(\underline{z = x \cap y})$, *где*

$$\underline{z = x \cap y} := \forall v(v \in z \leftrightarrow (v \in x \wedge v \in y)).$$

Указание:

(F) Рассмотрим случай только элементов в произведении, поскольку техника доказательства в других случаях аналогична. Единственность следует из аксиомы объемности, а существование из аксиомы выделения, примененной к множеству $x := 2^{2^{x_1 \cup x_2}}$, *и свойству* $\mathcal{P} := \exists z_1 \exists z_2(z_1 \in x_1 \wedge z_2 \in x_2 \wedge \underline{z = (z_1, z_2)})$.

(G) Для доказательства существования применить аксиому выделения к множеству $\cup x$ *и свойству* $\mathcal{P} := \forall v(v \in x \rightarrow z \in v)$ *Единственность следует из аксиомы объемности.*

(H) Применить (E) *к паре* (x, y).

- **Аксиома замены**. Можно создавать новое множество как множество значений некоторой функции.

$$\forall x(\forall y \forall z \forall w((y \in x \wedge P(y, z) \wedge P(y, w)) \rightarrow z = w) \rightarrow$$
$$\exists r \forall s(s \in r \leftrightarrow \exists t(t \in x \wedge P(t, s)))). \qquad (ZF_6)$$

9.2 Отношение порядка

Перед обсуждением остальных аксиом Цермело-Френкеля рассмотрим понятие порядка. Введем следующее определение:

Определение 9.1 *Частичным порядком называется пара $(A, <)$, где A – множество, а $<$ – двуместное отношение на A (напомним, что n-местное отношение на A это просто подмножество A^n, то есть $<$ это подмножество $A \times A$), обладающее следующими свойствами:*

(i) $y \not< y$ *для всех* $y \in A$,

(ii) Из $x < y$ *и* $y < z$ *следует* $x < z$ *для всех* $x, y, z \in A$.

В этом случае говорят также, что отношение $<$ частично упорядочивает множество A либо что A частично упорядоченно отношением $<$.

Следуя традиции, мы используем значок $<$ (а не букву) как знак отношения частичного порядка и называем это отношение “меньше”.

Определение 9.2 *Частичный порядок $(A, <)$ называется линейным, если все элементы множества A сравнимы отношением $<$, иначе говоря, если для всех $a \in A, b \in A$ выполнено либо $a < b$, либо $b < a$, либо $a = b$. В этом случае говорят также, что отношение $<$ является отношением линейного порядка на A, или что A является множеством, линейно упорядоченным отношением $<$.*

Пусть $(A, <)$ – частичный порядок. Очевидно, что любое $B \subset A$ также частично упорядоченно отношением $<$. Элемент $x \in B$ называется *минимальным* элементом множества B, если не существует никакого меньшего его элемента этого множества. Элемент $x \in B$ называется *наименьшим* элементом множества B, если он меньше всех элементов этого множества. Заметим, что наименьший элемент множества автоматически является и его минимальным элементом, однако обратное, вообще говоря, неверно. Например, во множестве коробок определим отношение порядка таким образом, что коробка A меньше коробки B, если ее можно поместить внутрь коробки B. Ясно, что при таком определении необязательно все коробки являются соизмеримыми, то есть полученный порядок не обязательно является линейным, (например, если в рассматриваемом множестве коробок найдутся такие две, что ни одна из них не помещается внутрь другой).

При этом наименьшей коробкой является та, которая помещается во все остальные, а минимальной та, в которую не помещается ни одна коробка.

Определение 9.3 *Порядок $(A, <)$ называется фундированным, если любое подмножество $B \subset A$ содержит минимальный элемент. В этом случае говорят также, что частично упорядоченное множество A является фундированным. Фундированный линейный порядок называется полным. В этом случае говорят также, что множество A вполне упорядочено отношением $<$.*

Вот некоторые примеры частичных порядков:

Пример 9.2

(A) Множество натуральных чисел $\mathbf{N}$ со стандартным отношением $<$ – полный порядок.

(B) Множество $\mathbf{Z}$ (целых чисел), также со стандартным отношением $<$ – не является полным порядком, хотя и является линейным порядком.

(C) Множество комплексных чисел $\mathbf{C}$ со следующим отношением порядка $(z_1 < z_2 \leftrightarrow Re(z_1) < Re(z_2))$ является частичным, но не является даже линейным порядком.

(D) Множество целых положительных чисел $\mathbf{Z}_+$ с отношением $<$, введенным следующим образом: $x < y$ если x делит y. Такой порядок является частичным, но не является линейным порядком.

(E) Для некоторого множества X, рассмотрим множество всех его подмножеств 2^X, упорядочим его отношением включения, а именно $x < y$ если $x \subset y$ и $x \neq y$. Такой порядок в общем случае не является линейным.

(F) Над множеством A^* слов над алфавитом A, где алфавит частично упорядочен отношением $<_A$, определим лексикографический порядок следующим образом: $x < y$ если либо длина (число символов) слова x меньше длины слова y, либо, если их длины одинаковы и $x' <_A y'$, где x' и y' – первые различающиеся буквы. Например, если A – латинский алфавит, $<_A$ – порядок следования букв в алфавите, то лексикографический порядок будет полным, причем для множества слов A^* верно, например, что $z <_{A^*} fish$ и $home <_{A^*} last$. Но если A – вещественные числа, то лексикографический порядок будет линейным, но не будет полным.

Справедливо следующее утверждение:

Теорема 9.1 *В любой модели системы аксиом Цермело-Френкеля следующие три свойства частичных порядков $(A, <)$ эквивалентны:*

(i) Порядок $(A, <)$ является фундированным.

(ii) Не существует бесконечной строго убывающей последовательности $x_0 > x_1 > x_2 > \ldots > x_k > \ldots$ элементов множества A.

(iii) Для множества X верен принцип математической индукции в следующей форме: если (при каждом $x \in X$) из истинности для всех $y < x$ следует истинность $\mathcal{P}(x)$, то свойство $\mathcal{P}$ верно при всех x.

Доказательство: Теорему будем доказывать по частям. Перейдем к доказательству эквивалентности первых двух свойств. Рассмотрим бесконечную убывающую последовательность $x_0 > x_1 > x_2 > \ldots$. Очевидно, что множество ее значений не имеет минимального элемента (следующий элемент найдется для любого элемента, так как последовательность бесконечная, и он еще меньше, так как она убывающая). Поэтому (i) влечет (ii). И обратно, если X непустое множество, не имеющее минимального элемента, то бесконечную убывающую последовательность можно строить следующим образом. Зафиксируем некий элемент $x \in X$, он не минимальный по предположению, тогда берем меньший элемент $x_1 < x$, $x_1 \in X$, таким образом получаем бесконечную убывающую последовательность $\{x_i\}_{i=1}^{\infty}$.

Теперь выведем принцип математической индукции из существования минимального элемента в любом подмножестве. Пусть $\mathcal{P}(x)$ – свойство элементов множества X, верное не для всех элементов $x \in X$. Рассмотрим множество тех элементов, для которых свойство $\mathcal{P}$ неверно. Множество B непусто по предположению. Пусть x_0 - минимальный элемент множества B. Тогда для всех $x < x_0$ свойство $\mathcal{P}(x)$ выполнено, так как элементов меньших x_0 в множестве B нет. Но тогда по предположению должно быть выполнено и $\mathcal{P}(x_0)$, таким образом мы пришли к противоречию.

И последнее: из принципа математической индукции следует существование минимального элемента в любом непустом множестве. Пусть B - множество, в котором нет минимальных элементов. Докажем что B пусто: в качестве $\mathcal{P}(x)$ возьмем свойство $x \in B$. Тогда, если $\mathcal{P}(x)$ верно для всех $x < x_0$, то никакой элемент, меньший x_0, не лежит в B. Значит, если бы x_0 лежал в B, то он был бы там минимальным, таким образом, мы пришли к противоречию. $\square$

9.3 Аксиома регулярности

Теперь мы можем сформулировать еще одну, весьма важную аксиому системы аксиом Цермело-Френкеля, называемую аксиомой регулярности, или фундирования (the foundation axiom). Эта аксиома записывается следующим образом:

$$\forall x \left(\neg x = \emptyset \to \exists y \left(y \in x \wedge \underline{y \cap x = \emptyset}\right)\right), \qquad (ZF_7)$$

где $\underline{y \cap x = \emptyset}$ – сокращенное написание формулы

$$\underline{z \cap y = \emptyset} := \exists r \left(\underline{r = z \cap y} \wedge \underline{r = \emptyset}\right).$$

Эта аксиома является несколько искусственной и никогда явным образном не используется в привычной нам математике. Она утверждает, что каждое непустое множество X содержит элементы, минимальные по отношению к отношению принадлежности $\in$ (а не включения $\subseteq$). С интуитивной точки зрения мы бы хотели, чтобы все наши множества строились из пустого множества $\emptyset$. Поэтому мы хотим избавиться от бесконечных последовательностей множеств, убывающих по отношению к порядку, определенному отношением принадлежности $\in$. Аксиома регулярности (ZF_7) утверждает таким образом, что никакое множество, в этом смысле, не может иметь бесконечной "глубины". В привычной нам математике мы имеем дело с натуральными, рациональными, действительными числами, функциями и т.п. В дальнейшем мы покажем, что все эти объекты явным образом строятся из пустого множества $\emptyset$.

Условие, налагаемое аксиомой регулярности на отношение принадлежности $\in$, очень похоже на понятие фундированного порядка. Правда, стоит иметь в виду, что отношение принадлежности не упорядочивает все множество, например, хотя бы потому, что из $x = y$ не следует, что $x \notin y$ либо $y \notin x$.

Требование справедливости данной аксиомы является весьма сильным, и, в частности, исключает из возможных моделей аксиоматики Цермело-Френкеля всевозможные экзотические объекты, такие как множество всех множеств или множество всех множеств не содержащих себя в качестве элемента. Действительно, если бы существовало множество A всех множеств, не содержащих самого себя, то есть $x \in A$, если и только если $x \notin x$, то оно содержало бы бесконечную ("бездонную") последовательность множеств, включающихся друг в друга. Вот строгая формулировка и доказательство этого утверждения.

Предложение 9.1. $ZF \vdash \forall x(\neg x \in x)$

Доказательство: Докажем теперь, что никакое множество не принадлежит самому себе. Воспользуемся аксиомой регулярности и уже доказанным фактом существования одноэлементного множества $\{x\}$, а также тем, что
$ZF \vdash \forall x(\underline{x \in \{x\}})$, где

$$\underline{x \in \{x\}} := \exists y(x \in y \wedge \underline{y = \{x\}})$$

(докажите этот факт самостоятельно). Дерево доказательства формулы $\forall x(\neg x \in x)$ выглядит следующим образом.

$$\dfrac{\dfrac{\dfrac{\dfrac{[y \in \{x\} \wedge \forall z(z \in \{x\} \to \neg z \in x)]_1}{\forall z(z \in \{x\} \to \neg z \in x)}(\wedge e)}{z \in \{x\} \to \neg z \in x}(\forall e)}{x \in \{x\} \qquad x \in \{x\} \to \neg x \in x}\,z{=}x\,(\to e) \qquad \dfrac{\forall v(\exists y(y \in v) \to \exists y(y \in v \wedge \forall z(z \in v \to \neg z \in y)))}{\exists y(y \in \{x\}) \to \exists y(y \in \{x\} \wedge \forall z(z \in \{x\} \to \neg z \in y))}\,\forall e, v{=}\{x\}\,(\to e)}{\dfrac{\neg x \in x}{\forall x(\neg x \in x)}\,\forall i \qquad \dfrac{\exists y(y \in \{x\}) \qquad (\exists y)(y \in \{x\} \wedge \forall z(z \in \{x\} \to \neg z \in y))}{\forall x(\neg x \in x)}\,1,(\exists e)}$$

Упражнение 9.4 *Докажите, что в модели аксиоматики Цермело-Френкеля не существует множества всех множеств. Иначе говоря,*

$$ZF \vdash \neg\exists x \forall y(y \in x).$$

Указание: *Если бы такое множество существовало, то оно содержало бы себя, что противоречит предложению 9.1.*

9.4 Аксиома бесконечности

Рассмотренные до сих пор аксиомы системы аксиом Цермело-Френкеля позволяли конструировать различные математические объекты, например, конечные вектора, отношения, отображения как некоторые специальные множества. Однако, легко заметить, что все множества, которые мы таким образом конструировали, были конечными. Так, например, мы доказали существование пустого множества в любой модели системы аксиом Цермело-Френкеля. Следовательно, хотя бы в силу аксиомы множества подмножеств (ZF_4), существует и одоэлементное множество $2^{\emptyset}$, а также трех (четырех, пяти) элементные множества, и

вообще множества с любым конечным числом элементов. Действительно, среди аксиом, которые позволяли формировать новые множества, лишь аксиома пары (ZF_2), аксиома множества подмножеств (ZF_4) и аксиома суммы (ZF_5) позволяли формировать множества, имеющие больше элементов, чем было в исходных множествах, остальные же (например, аксиома выделения (ZF_3)) позволяли лишь уменьшать число элементов в формируемых множествах. Таким образом, пользуясь сформулированными до сих пор аксиомами, мы не сможем вырваться из мира конечных множеств, а, значит, мы не можем утверждать, опираясь на эти аксиомы, существование многих привычных математических объектов, таких как, например, множество натуральных (вещественных, комплексных) чисел и, вообще, любые другие бесконечные множества. Вообще говоря, это не является принципиальным ограничением для построения математики, а именно, можно построить "конечную" математику, то есть оперирующую исключительно с конечными объектами. Однако надо сказать, что такая конечная математика будет существенно беднее общепринятой, так что отказ от последней ради исключения из нее бесконечных множеств создает весьма значительные сложности. Иначе говоря, хотя без бесконечных множеств "прожить" и можно, но это существенно менее удобно: представьте себе, например, как определить вещественную функцию, не используя понятия бесконечных множеств. Впрочем, в этих рассуждениях мы оставили в стороне философский вопрос о том, существуют ли на самом деле бесконечные множества: в окружающей нас природе мы, очевидно не можем указать ни на какой конкретный пример бесконечного множества, а лишь на сколь угодно большие, но все же конечные множества. Иначе говоря, в житейских ситуациях мы вряд ли когда либо можем встретиться с действительной (актуальной) бесконечностью (то есть с действительно бесконечным множеством). И в то же время встречаемся со сколь угодно большими множествами, то есть с потенциальной бесконечностью.

Для того, чтобы ввести в формируемую нами теорию бесконечные множества, предназначена специальная аксиома системы аксиом Цермело-Френкеля, называемая аксиомой бесконечности и записываемая следующим образом:

$$\exists x(\emptyset \in x \wedge \forall v(v \in x \to \underline{\{v\} \cup v \in x})) \qquad (ZF_8)$$

Данная аксиома утверждает существование множества, содержащего по крайней мере все элементы вида $\underline{0} := \emptyset$, $\underline{1} := \{\emptyset\} \ldots \underline{2} := \{\emptyset\} \cup \{\{\emptyset\}\}$ то есть все элементы вида

$$\underline{k} = \underline{k-1} \cup \{\underline{k-1}\}, \qquad k \in \mathbf{N}.$$

Такое множество, очевидно, является бесконечным (по крайней мере счетным). Стоит отметить, что мы не можем сказать ничего более определенного о мощности данного множества. В частности, мы не можем утверждать, что это множе-

ство счетно, так как аксиома бесконечности не гарантирует, что в нем содержатся *только* элементы вида $\underline{k}$.

С использованием аксиомы бесконечности мы получаем множество новых объектов, и жизнь сразу делается более "приятной". В частности можно сравнительно легко доказать существование самых разных привычных объектов современной математики. Для примера мы построим в следующем параграфе множество натуральных чисел и, вместе с ним, фактически стандартную модель арифметики. Натуральные числа мы будем отождествлять с только что введенными элементами вида $\underline{k}$, где $k \in \mathbf{N}$, а "множество натуральных чисел" со множеством, содержащим все "натуральные числа", то есть множества $\underline{k}$, $k \in \mathbf{N}$, и только их. Такое множество очевидно содержится в бесконечном множестве, существование которого гарантируется аксиомой бесконечности (ZF_8). Таким образом, множество "натуральных чисел" можно получить, применяя к последнему множеству аксиому выделения (ZF_3).

Этой конструкции посвящен следующий параграф, в котором попутно вводятся более общие весьма важные объекты, обобщающие как понятие чисел, так и множества натуральных чисел, называемые порядковыми числами или ординалами.

9.5 Ординалы и стандартная модель арифметики

Понятие ординала или порядкового числа – является естественным обобщением понятия натурального числа, точнее, является "мерой величины" всевозможных, в том числе бесконечных, порядков в той же мере, в какой натуральные числа могут использоваться для измерения величины конечных порядков. Это понятие чрезвычайно важно в теории множеств и математике вообще. Поскольку конструкция ординалов естественным образом связана с возможностью сравнения между собой разных порядков, то нам необходимо для начала определить, что мы понимаем под одинаковыми (точнее, будем говорить *изоморфными*) порядками.

Определение 9.4 *Порядки $(X, <_X)$ и $(Y, <_Y)$ изоморфны, если существует биекция $f : X \to Y$, сохраняющая порядок, то есть такая что из $x_1 <_X x_2$ следует $f(x_1) <_Y f(x_2)$.*

Мы будем писать $(X, <_X) \sim (Y, <_Y)$, если порядки $(X, <_X)$ и $(Y, <_Y)$ изоморфны. В этом же случае мы будем писать просто $X \sim Y$, позволяя себе некоторую вольность отождествления порядка с соответствующим упорядоченным множеством, если ясно, какое отношение порядка имеется в виду. Рассмотрим некоторые примеры.

Пример 9.3

(A) Рассмотрим множество натуральных чисел $\mathbf{N}$ *со стандартным порядком и множество четных чисел* **Even** *с тем же самым порядком. Очевидно, что соответствующие порядки изоморфны: изоморфизм осуществляется биекцией* $f : \mathbf{N} \to \mathbf{Even}$*, определяемой формулой* $f(x) = 2x$*.*

(B) Рассмотрим множества натуральных чисел $\mathbf{N}$ *со стандартным порядком и множество* $X := \mathbf{N} \cup \{\xi\} = \{0, 1, 2, 3, 4 \ldots, \xi\}$*. В последнем множестве порядок определяется следующим образом:* $x <_X y$*, если либо* $\{x, y\} \subset \mathbf{N}$ *и* $x <_{\mathbf{N}} y$ *в смысле стандартного порядка на множестве* $\mathbf{N}$*, либо* $x \in \mathbf{N}, y = \xi$*. Соответствующие порядки не являются изоморфными, несмотря на то что сами множества* X *и* $\mathbf{N}$ *равномощны. Иначе говоря, между* X *и* $\mathbf{N}$ *существует биекция, но никакая биекция не может сохранять порядок. Докажем это от противного. Пусть* $f : X \to \mathbf{N}$ *– биекция, сохраняющая порядок. Тогда* $f(x) < f(\xi)$ *для любого* $x \in \mathbf{N}$*, что противоречит сюръективности* f*.*

Если $(Y, <)$ – частичный порядок, то под начальным отрезком $\hat{y}$ этого порядка, соответствующим элементу $y \in Y$, будем понимать множество $\hat{y} = \{x \in Y, x < y\}$ с тем же самым отношением порядка $<$. Стоит отметить несколько простейших свойств начальных отрезков (поупражняйтесь в их доказательстве):

(i) начальный отрезок полного порядка является полным порядком;

(ii) если Y – частичный порядок, а $\hat{y}$ – его начальный отрезок, то $\hat{y}$ также можно рассматривать как порядок (отношение порядка унаследовано от Y). Тогда любой начальный отрезок порядка $\hat{y}$ является начальным отрезком порядка Y;

(iii) объединение любого числа начальных отрезков одного и того же линейного порядка является начальным отрезком того же порядка;

(iv) из любых двух начальных отрезков полного порядка один обязательно является подмножеством другого.

Теперь введем следующее определение.

Определение 9.5 *Будем говорить, что*

(i) порядки $(X, <_X)$ *и* $(Y, <_Y)$ *имеют одинаковый порядковый тип, если* $X \sim Y$*;*

(ii) порядок $(X, <_X)$ *имеет строго больший порядковый тип, чем* $(Y, <_Y)$*, если существует* $y \in Y$*, такой что* $\hat{y} \neq Y$ *и* $X \sim \hat{y}$*. В этом случае будем писать* $X \succ Y$*;*

(iii) порядок $(X, <_X)$ *имеет строго меньший порядковый тип, чем* $(Y, <_Y)$*, если порядок* $(Y, <_Y)$ *имеет строго больший порядковый тип, чем* $(X, <_X)$*, то есть существует* $x \in X$*, такой что* $\hat{x} \neq X$ *и* $Y \sim \hat{x}$*. В этом случае будем писать* $X \prec Y$*.*

В последнем примере в пункте (A) оба порядка имеют одинаковый порядковый тип, а в пункте (B) порядковый тип **N** меньше порядкового типа X. Справедливо следующее утверждение.

Теорема 9.2 (Бернштейна) *В предположении непротиворечивости системы аксиом Цермело-Френкеля* **ZF** *для любых двух полных порядков верно ровно одно из следующих утверждений:*

(i) X *и* Y *имеют одинаковый порядковый тип;*

(ii) X *имеет строго больший порядковый тип, чем* Y*;*

(iii) Y *имеет строго больший порядковый тип, чем* X*.*

Доказательство: Упражняйтесь, либо загляните в [4].

В “наивной”, то есть неаксиоматизированной теории множеств обычно вводят понятие ординала как порядкового типа всех изоморфных между собой порядков. Говоря более строгим языком, это означает, что таким образом определяемый ординал является классом эквивалентности всех изоморфных между собой порядков. Например, ординал $\underline{1}$ должен быть классом всех порядков, изоморфных порядку $\{\emptyset\}$, ординал $\underline{2}$ должен быть классом всех порядков, изоморфных порядку $\{\emptyset, \underline{1}\}$, где $\underline{1} > \emptyset$. Однако, в строгой теории множеств, которую мы пытаемся строить, подобное “определение” понятия ординала не может быть реализовано. А именно, для того чтобы доказать существование хоть какого-нибудь ординала как класса всех изоморфных порядков, необходимо выделить этот ординал с использованием аксиомы выделения (ZF_3) из некоторого достаточно большого

множества, которому принадлежат *все* порядки. Достаточно легко заключить, что само существование подобного чересчур "большого" множества весьма проблематично. Для того, чтобы обойти это затруднение, Дж. фон Нейман предложил определить понятие ординала слегка по-другому, так что ординал, введенный согласно новому определению, автоматически оказывался бы множеством. Для описания этой конструкции введем следующие определения.

Определение 9.6 *Множество x называется транзитивным, если для всех y, таких что $y \in x$, и z, таких что $z \in y$, выполнено $z \in x$.*

Иначе говоря, на языке теории множеств формула

$$\underline{Trans(x)} := \forall y \forall z (z \in y \wedge y \in x \to z \in x)$$

"говорит" о том, что x – транзитивное множество.

Определение 9.7 *Ординалом будем называть транзитивное множество, вполне упорядоченное отношением принадлежности $\in$ между своими элементами.*

Стоит отметить, что на произвольном множестве отношение принадлежности $\in$, вообще говоря, не задает даже частичного порядка. Однако на транзитивном множестве это отношение является отношением частичного порядка.

На рассматриваемом нами языке теории множеств формула

$$\underline{Linord(x, \in)} := \forall y \forall z (y \in x \wedge z \in x \to z \in y \vee y \in z \vee y = z)$$

"говорит" о том, что множество x упорядочено отношением принадлежности $\in$, а формула

$$\underline{Found(x, \in)} := (\underline{v \subset x} \to \exists w (w \in v \wedge \forall q (q \in v \to (w \in q \vee w = q)))),$$

"говорит" о том, что отношение принадлежности $\in$ превращает x в фундированное множество.

Тогда формула

$$\underline{Ord(x)} := \underline{Trans(x)} \wedge \underline{Linord(x, \in)} \wedge \underline{Found(x, \in)}$$

"говорит" о том, что x – ординал.

Пример 9.4 *Следующие множества является ординалами:*

$$\underline{0} := \emptyset,\ \underline{1} := \{\underline{0}\},\ \underline{2} := \underline{1} \cup \{\underline{1}\}, \ldots, \underline{k} := \underline{k-1} \cup \{\underline{k-1}\}, \ldots \qquad k \in \mathbf{N}.$$

Все такие ординалы называются конечными ординалами.

Определенные таким образом ординалы можно, в силу теоремы Бернштейна, сравнивать между собой, более того, в силу этой же теоремы, ординалами можно пользоваться как естественной мерой величины полных порядков. А именно, справедливо следующее утверждение.

Теорема 9.3 *Если система аксиом Цермело-Френкеля* **ZF** *не является противоречивой, то любой полный порядок изоморфен единственному ординалу* α*.*

$$(Y, <) \sim (\alpha, \in)$$

В цели данной книги не входит подробное изложение теории множеств, будь то наивной или аксиоматической, а лишь иллюстрация применения математической логики для описания различных математических теорий, в том числе теории множеств. Поэтому мы приведем здесь лишь немногие основные свойства ординалов без доказательства, предлагая читателям самим поупражняться в их доказательстве. В случае трудностей, а также при желании более углубленно изучить теорию множеств, мы рекомендуем обращаться к [4], [6].

В связи с этим для начала мы предлагаем читателю в качестве упражнения доказать теорему 9.3. Помочь в этом могут следующие свойства ординалов:

(i) любое ограниченное семейство ординалов имеет точную верхнюю грань;

(ii) класс всех ординалов вполне упорядочен отношением принадлежности $\in$ между своими элементами;

(iii) начальный отрезок ординала также является ординалом;

(iv) изоморфные ординалы совпадают.

Обратите внимание, что мы говорим о *классе*, а не о множестве всех ординалов. Действительно, не трудно показать (см. ниже), что *множества* всех ординалов не существует. Однако понятие частичной (линейной, полной) упорядоченности очевидно можно применять не только к множествам, но и к произвольным совокупностям объектов (классам).

С использованием вышеприведенных свойств доказательство теоремы 9.3 можно провести по следующей схеме.

Доказательство теоремы 9.3:
Обозначим через α_- точную верхнюю грань множества тех ординалов α, которые имеют строго меньший порядковый тип, чем Y, т.е.

$$\alpha_- := \sup\{\alpha : \ \alpha \prec Y\}.$$

Из определения α_- следует $\alpha_- + 1 \succcurlyeq Y$, где формула $\alpha \succcurlyeq \beta$ означает, что либо $\alpha \succ \beta$, либо $\alpha \sim \beta$, поскольку иначе выполнялось бы $\alpha_- + 1 \prec Y$, что противоречило бы определению α_-. Но выражение

$$Y \preccurlyeq \alpha_- + 1$$

означает, что Y изоморфен некоторому начальному отрезку $\alpha_- + 1$ (который, по свойству (iii), является ординалом), или самому $\alpha_- + 1$. Единственность ординала α следует из свойства (iv).

Упражнение 9.5 *Докажите, что любое вполне упорядоченное множество изоморфно единственному начальному отрезку* $[0, \alpha)$ *в классе всех ординалов (образованному всеми ординалами, меньшими* α*).*

Упражнение 9.6 *Докажите, что в предположении непротиворечивости системы аксиом Цермело-Френкеля* **ZF** *не существует* множества *всех ординалов. Данное утверждение известно под названием парадокса Бурали-Форти.*

Теперь введем следующее определение.

Определение 9.8 *Ординал* α *будем называть непосредственно следующим за ординалом* β *и писать* $\alpha = \beta + 1$*, если* $\alpha = \beta \cup \{\beta\}$*. Предельным ординалом будем называть ординал, который не следует непосредственно ни за каким ординалом.*

Формула

$$\underline{Limord(x)} := \underline{Ord(y)} \wedge \neg\exists y(\underline{Ord(x)} \wedge \underline{x = y + 1}),$$

где $\underline{x = y + 1} := \underline{x = y \cup \{y\}}$, "говорит" о том, что x – предельный ординал. Очевидно, что $\underline{0}$ является предельным ординалом, а каждый конечный ординал $\underline{k}$, где $k \in \mathbf{N}$, отличный от $\underline{0}$, непосредственно следует за ординалом $\underline{k-1}$.

Определение 9.9 *Минимальным бесконечным ординалом (или первым счетным ординалом) называется предельный ординал ω_0, которому не предшествует никакой предельный ординал, кроме $\emptyset$.*

Таким образом, формула

$$\underline{x = \omega_0} := \neg x = \underline{0} \wedge (\underline{Limord(x)} \wedge \forall y(y \in x \rightarrow \neg \underline{Limord(x)}))$$

"говорит" о том, что ω_0 является первым счетным ординалом.

С учетом введенных обозначений можно записать свойство конечности ординала следующей формулой:

$$\underline{Fin(x)} := \exists y(\underline{y = \omega_0} \wedge x \in y).$$

Данная формула истинна, если и только если множество, соответствующее в модели аксиом Цермело-Френкеля символу x, является конечным ординалом (это можно принять за формулировку определения конечного ординала). Ординалы, не являющиеся конечными, называются бесконечными.

Используя аксиоматику Цермело-Френкеля **ZF**, мы можем показать существование стандартной модели арифметики Пеано. Практически все для этого уже подготовлено. А именно, в качестве универсума рассмотрим $N := \omega_0$ определим

$$s^{\mathcal{N}}(\alpha) = \alpha + 1,\ 0^{\mathcal{N}} := \emptyset.$$

Таким образом, натуральные числа оказываются просто конечными ординалами. Осталось определить операции суммирования $+^{\mathcal{N}}$ и умножения $*^{\mathcal{N}}$ и проверить выполнение аксиом Пеано. Читателю предоставляется возможность поупражняться в этом или прочитать об этом в любом стандартном курсе теории множеств ([4], [6]). Таким образом доказывается следующий фундаментальный результат:

Теорема 9.4 *В предположении непротиворечивости аксиоматики Цермело-Френкеля* **ZF** *существует стандартная модель арифметики Пеано.*

Кстати, интересно отметить, что ординал $\omega_0 + 1$ представляет собой не что иное, как порядок $(X, <_X)$ из примера 9.3 (В). В качестве упражнения рекомендуем читателю представить себе как выглядит ординал $\omega_0 + k$. Продолжим рассмотрение структуры класса всех ординалов. Множество ω_0 является предельным ординалом и образовано объединением всех конечных ординалов, которые естественным

образом отождествляются с натуральными числами, однако ряд ординалов не исчерпывается таким образом. Так, за ординалом ω_0 следует $\omega_0 + 1$, за последним $\omega_0 + 2$, и так далее. Так, что существуют ординалы

$$\omega_0 + 1,\ \omega_0 + 2, \ldots, \omega_0 + k, \ldots \qquad\qquad k \in \mathbf{N}.$$

Вслед за приведенными выше ординалами, очевидно, найдется следующий предельный ординал ω_1, являющийся первым предельным ординалом несчетной мощности (поупражняйтесь в доказательстве этого утверждения), также ω_1 называют первым несчетным ординалом. За ним следуют ординалы $\omega_1 + 1,\ \omega_1 + 2$, и далее в ряду ординалов найдется следующий предельный ординал ω_2, и так далее. Таким образом, ряд ординалов выглядит так:

$$\underline{0}, \underline{1}, \underline{2}, ..., \omega_0, \omega_0 + 1, \omega_0 + 2, ..., \omega_1, \omega_1 + 1, \omega_1 + 2, ..., \omega_2, ...$$

Мы, естественно, привели здесь лишь начальный отрезок этого ряда.

Понятие ординала, позволяющее легко сравнивать порядки, может быть адаптировано и для сравнения множеств по мощности. Введем для этого следующее определение.

Определение 9.10 *Кардиналом называется ординал, не равномощный ни одному из меньших (предыдущих) ординалов.*

Иначе говоря, формула

$$\underline{Card(x)} := \underline{Ord(x)} \wedge \forall y(y \in x \to \neg(\underline{y \sim x}))$$

означает, что x является кардиналом. Формула $\underline{y \sim x}$ означает, что множества y и x равномощны (выпишите "полную версию" этой формулы самостоятельно).

Так, $\underline{0}$, $\underline{1}$, $\underline{2}$ и все конечные ординалы являются кардиналами. Также являются кардиналами ω_0 и ω_1, однако, например, $\omega_0 + 1,\ \omega_0 + 2$, и вообще $\omega_0 + k$, где $k \in \mathbf{N}$, не являются кардиналами, так как все они имеют счетную мощность, и равномощны меньшему ординалу ω_0. Кардиналы являются естественной мерой мощности множеств в той же мере, в той же мере, в какой ординалы являются мерой "величины" порядков. Для обозначения кардиналов часто используются буквы древнееврейского алфавита. Так, ω_0 и ω_1, рассматриваемые как кардиналы, обычно обозначают $\aleph_0$ и $\aleph_1$, соответственно, и при этом о них говорят, что это, соответственно счетный и первый несчетный кардиналы (мощности).

9.6 Аксиома выбора

Сформулируем, наконец, последнюю, наиболее нетривиальную из аксиом Цермело-Френкеля – аксиому выбора. Данная аксиома утверждает, что существует функция (называемая *функцией выбора*), которая каждому множеству из набора ставит в соответствие ровно один элемент этого множества. Это утверждение кажется весьма тривиальным, однако оно может быть выведено из других аксиом Цермело-Френкеля лишь для конечных наборов множеств. Предположение же его справедливости для произвольного набора множеств (впрочем, не вполне произвольного: эти наборы должны быть *множествами*) ведет к целому ряду нетривиальных следствий, иногда, казалось бы, противоречащих здравому смыслу. Поскольку в теории, которую мы строим, все объекты являются множествами (в том числе функции и "наборы" множеств, с которыми мы можем работать), то формальная запись данной аксиомы несколько менее интуитивна, чем ее словесное описание.

Для упрощения записи введем формулу

$$\underline{Disjoint(x)} := \forall u \forall v \ \ (u \in x \wedge v \in x \wedge \neg u = v \rightarrow \underline{u \cap v = \emptyset}),$$

которая "говорит" о том, что x состоит из попарно непересекающихся множеств.

С помощью этого сокращения аксиому выбора можно записать в следующем, сравнительно компактном виде:

$$\forall x \ \ (\neg \underline{\emptyset \in x} \wedge \underline{Disjoint(x)} \rightarrow \exists y \ \ (\forall w \ \ (w \in x \leftrightarrow \exists! \ \ z(z \in w \cap y)))) \qquad (AC)$$

Здесь утверждается существование множества y, имеющего ровно по одному общему множеству с каждым из элементов исходного множества x, при условии, что x непусто и его элементы – попарно непересекающиеся множества.

В наши цели не входит подробное обсуждение аксиомы выбора. Интересующийся читатель может обратится, например, к [6] или [5]. Здесь отметим только, что аксиома выбора является одним из краеугольных камней современной математики в том смысле, что многие фундаментальные утверждения последней (скажем, целый ряд важных результатов математического анализа) справедливы исключительно в предположении истинности аксиомы выбора. В то же время, интересным следствием данной аксиомы является парадокс Банаха-Тарского, который утверждает, что любое тело (например, шар) может быть разрезано на конечное число непересекающихся частей, из которых можно потом составить два тела, равных исходному. Это утверждение кажется противоречащим здравому смыслу, так как если бы подобное разбиение было бы осуществимо, то легко можно

было бы осуществить известное евангельское чудо, а именно "накормление верующих двумя рыбами и пятью ячменными хлебами" (Евангелие от Иоанна 6:13-14). Однако в доказательстве данного утверждения существенным образом используется аксиома выбора. Последняя является весьма неконструктивной, так как в ней утверждается существование "функции выбора", но не приводится алгоритма построения этой функции. А значит, любые доказательства, которые существенным образом используют аксиому выбора, в том числе и доказательство парадокса Банаха-Тарского, неконструктивны. Поэтому, например, невозможно привести никакого алгоритма деления тела на составные части, утверждаемого в формулировке парадокса, хотя и можно утверждать существование соответствующего разбиения.

Следует отметить, что аксиома выбора является еще одной аксиомой создания множеств, наряду с аксиомами выделения (ZF_3), пары (ZF_2), суммы (ZF_5), множества подмножеств (ZF_1) и замены (ZF_6). Аксиоматику Цермело-Френкеля с аксиомой выбора обозначают **ZFC**. Отметим, что (AC) не зависит от остальных аксиом **ZF**.

9.7 Теория множеств и основания математики

Материала предыдущего параграфа должно быть вполне достаточно, чтобы убедиться в том, что рассматриваемого нами "примитивного" языка теории множеств (мы называем его "примитивным", поскольку это язык логики первого порядка, в котором сигнатура состоит всего из двух предикатных символов – равенства $=$ и принадлежности $\in$) и системы аксиом Цермело-Френкеля вполне достаточно, чтобы описать и построить практически всю современную математику. Так, этих инструментов было достаточно для построения натуральных чисел и основных действий над ними. Отталкиваясь от этих понятий, можно построить целые числа (целое число можно определить, например, как пару натуральных чисел), рациональные числа (как пары целых чисел) и, наконец, действительные числа, вектора, комплексные числа, геометрические фигуры (как множества векторов), функциональные пространства и так далее. Соответствующие построения проводятся "по нарастающей" (целые числа строятся на основе натуральных, рациональные на основе целых, вещественные на основе рациональных и т.д.). Несколько неожиданным и, возможно, даже не вполне соответствующим интуитивному представлению о математических объектах оказывается то, что в любой модели построенной таким образом математики все объекты (числа, вектора, функции, геометрические фигуры, и т.д.) оказываются множествами, и даже, более того, все без исключения построены на основе одного объекта –

пустого множества $\emptyset$. То, что построенные таким образом математические объекты оказываются, на первый взгляд, не имеющими отношения к реальной жизни (например, натуральные числа, построенные как конечные ординалы, не имеют отношения к практическому подсчету предметов) можно считать платой за строгость обоснования факта существования всех математических объектов. Кому-то такая плата, приводящая к формализации математики и её кажущемуся "отрыву от реальной жизни", может показаться чрезмерной. В то же время, на наш взгляд, требование формализованности и строгости рассуждений никогда не может чрезмерным, а опасность работы с плохо определенными "интуитивными" понятиями проявляется в многочисленных парадоксах, некоторые примеры которых были приведены в данной главе.

Поскольку, как мы уже убедились, математика может быть построена на теоретико-множественных основаниях, возникает естественный вопрос о том, насколько прочными могут быть такого рода основания. А именно, является ли аксиоматика теории множеств (например, аксиоматика Цермело-Френкеля **ZFC**) непротиворечивой? Из непротиворечивости последней следовала бы непротиворечивость и всей математики. К сожалению, однако, до настоящего времени непротиворечивость аксиоматики Цермело-Френкеля не была ни доказана, ни опровергнута. Не лучшим образом обстоит дело и с другими популярными аксиоматическими теориями множеств, которые также предлагались для построения оснований математики. Поэтому вопрос "строгого обоснования" математики, как ни странно, на сегодняшний день в известной мере является вопросом веры или доверия к многотысячелетнему опыту математиков и "пользователей" математического аппарата (за все известное в истории время использования математического аппарата противоречия получить не удалось, поэтому есть шанс, что математика является непротиворечивой). К сожалению, дело обстоит в известной мере еще хуже, ибо даже в предположении непротиворечивости математики ни системы аксиом Цермело-Френкеля, ни какой-либо другой системы аксиом, достаточно богатой, чтобы построить современную математику, и, в то же время, достаточно "обозримой" (такой, которую можно описать конструктивным образом, как например, мы описали **ZFC**) не хватит, чтобы доказать непротиворечивость этой системы аксиом. Иначе говоря, в предположении непротиворечивости **ZFC**, пользуясь только аксиомами **ZFC**, нельзя доказать непротиворечивость **ZFC**. Данный результат является следствием второй теоремы Геделя о неполноте формальных теорий (кстати, выводимой из системы аксиом **ZFC**, как и вся та математическая логика, которую мы строим).

Другим важным вопросом является вопрос о том, достаточно ли системы аксиом Цермело-Френкеля для описания *всей* современной математики. Иначе говоря, все ли интересные математические объекты и теории могут быть описаны в рам-

ках теории множеств, построенной на базе аксиом **ZFC**? Ответ на этот вопрос также отрицательный, хотя ситуация здесь не настолько трагична, в том смысле, что для построения весьма значительной части современной математики достаточно системы аксиом Цермело-Френкеля с аксиомой выбора. Есть однако, весьма интересные и важные, в том числе в приложениях, утверждения, которые не выводятся из **ZFC**. К числу таких утверждений относится, например, *континуум-гипотеза*, заключающаяся в том, что множество вещественных чисел $\mathbf{R}$ равномощно $\aleph_1$, то есть

$$\#\mathbf{R} = \aleph_1 \qquad (CH)$$

Заметим, что из аксиоматики **ZFC** можно вывести, что $\#\mathbf{R} \geq \aleph_1$, однако в отношении континуум-гипотезы (CH) справедливо следующее утверждение, доказанное К. Геделем и П. Коэном.

Теорема 9.5 *Если* **ZFC** *непротиворечива, то*

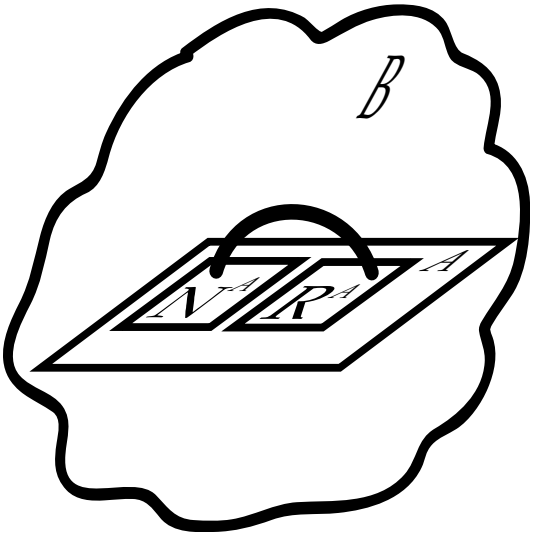
$$\mathbf{ZFC} \nvdash CH \qquad и$$

$$\mathbf{ZFC} \nvdash \neg CH.$$

Иначе говоря, в этом случае континуум-гипотеза является независимым относительно аксиоматики Цермело-Френкеля утверждением.

В связи с возможностью построения математики на теоретико-множественных основаниях возникает естественный вопрос о том, как устроены модели математики, содержащие все мыслимые математические объекты. Очевидно, что, модель математики, построенной на системе аксиом Цермело-Френкеля, существует, если и только если **ZF** непротиворечива (нетривиальная часть этого утверждения следует из теоремы о модели 6.5). Однако, в этом случае все модели математики будут бесконечными (так как они должны содержать хотя бы все ординалы, число которых бесконечно), поэтому, в силу теоремы Левенгейма-Скулема о повышении мощности модели 7.4, в этом случае математика будет иметь сколь угодно много неизоморфных между собой моделей (с универсумами сколь угодно большой мощности). Но наиболее интересные и нетривиальные результаты дает теорема Левенгейма-Скулема о понижении мощности модели 7.2: в предположении непротиворечивости аксиоматики **ZFC** построенная с её помощью математика будет иметь модель $\mathcal{A}$ со счетным универсумом. Данное утверждение кажется абсурдным: каким образом в счетном универсуме может уместиться принципиально несчетное число объектов, например, хотя бы несчетное множество вещественных чисел? Тем не менее данный парадокс, называемый парадоксом *Скулема*, является кажущимся. На самом деле счетность или несчетность множества определяется наличием биекции между данным множеством и

ω_0 (напомним, последнее можно считать просто множеством натуральных чисел). Множество вещественных чисел в любой модели математики, в том числе и в модели со счетным универсумом, является несчетным (данный факт, доказанный еще Кантором, сравнительно легко выводится из аксиоматики **ZFC**). Иначе говоря, это означает, что *в данной модели* нет объекта, соответствующего биекции между $\mathbf{R}^{\mathcal{A}}$ и ${\omega_0}^{\mathcal{A}}$. В то же время, поскольку универсум $\mathcal{A}$ счетен, то можно рассматривать его в качестве подмножества некоторой большей модели математики $\mathcal{B}$, универсум которой несчетен. В этой большей модели $\mathbf{R}^{\mathcal{A}}$ и ${\omega_0}^{\mathcal{A}}$ являются равномощными (поскольку оба они являются счетными множествами), то есть в ней имеется объект (множество), соответствующий биекции между $\mathbf{R}^{\mathcal{A}}$ и ${\omega_0}^{\mathcal{A}}$, однако этот объект отсутствует в меньшей модели $\mathcal{A}$. То есть понятия конечности, счетности, несчетности на самом деле зависят от модели.



Данная ситуация проиллюстрирована на рисунке, где модель $\mathcal{A}$ изображена в виде “плоского мира”, а $\mathcal{B}$ в виде “объемного мира”. Биекция между $\mathbf{R}^{\mathcal{A}}$ и ${\omega_0}^{\mathcal{A}}$ изображена в виде мостика между $\mathbf{R}^{\mathcal{A}}$ и ${\omega_0}^{\mathcal{A}}$, который существует только в “объемном мире” (из “плоского мира” он недоступен).

Литература

[1] Дж. Шенфилд, *Математическая логика*, “Наука”,Москва, 1975.

[2] *Математическая теория логического вывода*, под редакцией А. В. Иделсона и Г .Е. Минца, “Наука”,Москва, 1967.

[3] И. А. Лавров, Л. Л. Максимова, *Задачи по математической логике и теории алгоритмов*, “Наука”,Москва, 1984.

[4] Н. К. Верещагин и А. Шень, *Начала теории множеств*, МЦНМО, Москва, 1999.

[5] K. Hrbacek and T. Jech, *Introduction to Set Theory*, Marcel Dekker, Inc., New York, 1999.

[6] Пол Дж. Коэн, *Теория множеств и континуум-гипотеза*, “Мир”, Москва, 1969.

Максим Алексеевич Коротков
Евгений Олегович Степанов
Основы формальных логических языков
Учебное пособие

В авторской редакции
Компьютерная верстка К. А. Ворошилов
М. А. Коротков
Дизайн обложки Я. А. Иванов

Редакционно-издательский отдел СПб ГИТМО (ТУ)
Зав. РИО Н. Ф. Гусарова

Лицензия ИД №00408 от 05.11.99
Подписано к печати 15.01.03
Тиражирование на ризографе.
Тираж 100 экз.