

Управление культуры
Администрации города Екатеринбурга

Муниципальное бюджетное образовательное учреждение
высшего профессионального образования
«Екатеринбургская академия современного искусства»
(институт)

В. Б. Репницкий, А. Я. Овсянников
Основы математической логики

Учебное пособие

*Допущено Учебно-методическим объединением
по образованию в области прикладной информатики
в качестве учебного пособия для студентов, обучающихся
по направлению "Прикладная информатика"*

Екатеринбург
ЕАСИ
2015

УДК 510.6

ББК 22.12

Рецензенты:

доктор физико-математических наук, профессор, директор Регионального учебно-научного центра “Интеллектуальные системы и информационная безопасность” В. А. Баранский;

доктор физико-математических наук, профессор кафедры алгебры и дискретной математики Уральского федерального университета Б. М. Верников

Репницкий В. Б., Овсянников А. Я.

Основы математической логики: учебное пособие /
В. Б. Репницкий, А. Я. Овсянников. — Екатеринбург:
Екатеринбургская академия современного искусства, 2015. — 123 с.
ISBN 978-5-904440-42-8

В пособии излагаются первоначальные сведения из основных разделов курса “математическая логика”: логики высказываний, логики предикатов и аксиоматического метода. Предназначено для студентов, обучающихся по направлению подготовки “Прикладная информатика”.

УДК 510.6

ББК 22.12

ISBN 978-5-904440-42-8

© Репницкий В. Б., Овсянников А. Я., 2015

© Екатеринбургская академия
современного искусства, 2015

Оглавление

Предисловие	5
Глава 1. Логика высказываний и булевы функции	8
§ 1.1. Формулы логики высказываний и их интерпретации	8
§ 1.2. Отношение равносильности на множестве ФЛВ. Законы логики высказываний	11
§ 1.3. Логическое следование. Анализ рассуждений.	13
§ 1.4. Виды теорем. Обоснование некоторых методов доказательства в математике	16
§ 1.5. Булевы функции. Полные системы логических связей .	18
§ 1.6. Дизъюнктивные нормальные формы	22
§ 1.7. Принцип двойственности. Конъюнктивные нормальные формы	24
§ 1.8. Полные и замкнутые классы булевых функций. Теорема Поста	27
§ 1.9. Приложение логики высказываний к анализу релейно-контактных схем	34
Глава 2. Логика предикатов	38
§ 2.1. Предикаты	38
§ 2.2. Кванторы и их геометрическая интерпретация	43
§ 2.3. Формулы логики предикатов. Модели и интерпретации	48
§ 2.4. Законы логики предикатов	53
§ 2.5. Предваренные нормальные формы	58
§ 2.6. Проблема разрешения для общезначимости и выполнимости ФЛП	60
§ 2.7. Приложение логики предикатов к анализу рассуждений	66
Глава 3. Аксиоматический метод	70
§ 3.1. Формальные теории	71

§ 3.2. Теории первого порядка. Теорема о непротиворечивости.....	75
§ 3.3. Теорема о дедукции.....	84
§ 3.4. Обращение теоремы о непротиворечивости.....	88
§ 3.5. Теоремы об адекватности, полноте и компактности. Теорема Лёвенгейма-Сколема.....	95
§ 3.6. Теории первого порядка с равенством.....	97
§ 3.7. Основные проблемы формальных теорий.....	101
3.7.1. Проблема непротиворечивости.....	101
3.7.2. Проблема независимости аксиом.....	107
3.7.3. Проблемы категоричности и полноты. Теорема Гёделя о неполноте.....	111
3.7.4. Проблема разрешимости.....	118
Литература.....	122

Предисловие

Математическая логика относится к дисциплинам, образующим “математический фундамент” информатики. Она используется в программировании, при построении запросов к реляционным базам данных и доказательстве правильности компьютерных программ. Закономерно, что математическая логика присутствует в учебных планах всех профилей подготовки, связанных с направлением “Прикладная информатика”.

Настоящее пособие посвящено изложению математической логики для студентов ЕАСИ, обучающихся по указанному направлению. При этом мы надеемся, что оно может оказаться полезным и студентам других вузов соответствующей специализации.

Учебное пособие состоит из трех глав, отражающих основные темы курса – логику высказываний, логику предикатов и аксиоматический метод. Первая глава посвящена первоначальным понятиям математической логики – высказываниям и связкам (логическим операциям), способам построения на языке формул сложных высказываний из более простых, а также основным законам, которым высказывания подчиняются. Особое внимание уделяется булевым функциям, естественным образом возникающим в логике высказываний, и свойствам полноты и замкнутости классов, образуемых ими. Ключевым результатом здесь является теорема Поста, характеризующая полные классы булевых функций. Рассматриваются приложения логики высказываний к анализу рассуждений и анализу простейших технических устройств, таких как релейно-контактные (переключательные) схемы. Во второй главе мы обобщаем язык логики высказываний понятием предиката, обобщающим понятие высказывания, и вводим новые операции на предикатах – кванторы. Цель этой главы – научить студентов правильно записывать различные определения и утверждения на языке формул

логики предикатов, корректно с помощью соответствующих законов их преобразовывать, а также умело использовать определяемое здесь понятие логического следования при анализе различного рода рассуждений, проверка правильности которых “не подвластна” более бедному языку логики высказываний. В третьей главе рассматривается аксиоматический метод в математике, первопричины его зарождения, а также обсуждаются основные проблемы, здесь возникающие. Пристальное внимание внутри этого метода мы уделяем понятию синтаксической выводимости формул логики первого порядка и его связи с понятием логического следования (семантической выводимости). Одним из основных результатов в этом направлении является приводимая нами с доказательством теорема Гёделя о полноте для теорий первого порядка, которая устанавливает адекватность понятия теоремы в этих теориях понятию логически общезначимой формулы в них. К исследуемым в данном пособии проблемам формальных теорий относятся проблемы их непротиворечивости, категоричности, полноты и разрешимости, а также проблема независимости их аксиом. Особое место здесь мы отводим доказанной Гёделем теореме о неполноте формальной арифметики (и более общо, неполноте любой “разумной” аксиоматизации элементарной арифметики на языке логики первого порядка), ее исключительной роли в основаниях математики.

Указанная выше последовательность изложения материала, будучи совершенно естественной, приводит иногда к необходимости дублирования некоторых понятий. Например, понятия формулы, интерпретации и логического следования определяются последовательным обобщением в каждой главе. В определении указанных понятий, а также в целом ряде других определений и доказательств ключевую роль играет принцип математической индукции; предполагается, что читатель достаточно хорошо владеет этим принципом. К тому же от читателя требуется владение материалом некоторых фундаментальных дисциплин, изучаемых студентами по направлению “Прикладная информатика”: алгебры, геометрии и математического анализа. Наличие большого количества примеров, в том числе и из этих дисциплин, поможет читателю глубже усвоить язык и методы математической логики.

Авторы помнят высказывание Козьмы Пруткова о том, что “нельзя объять необъятное”. Поэтому в настоящее пособие по причинам ограниченности объема не были включены, к сожалению, некоторые не менее важные с точки зрения приложений разделы

современной математической логики. Так, в главе “Логика предикатов” естественно было бы подробно рассмотреть довольно “сильный” *метод резолюций*, помогающий определять общезначимость формул логики предикатов и играющий заметную роль в *теории автоматического доказательства теорем*. Его изложение заслуживает отдельного пособия. В третьей главе, посвященной аксиоматическому методу, дополнительный интерес представляет знакомство с алгебраическими методами, основанными на понятии *ультрапроизведения* алгебраических систем. Обо всем этом студенты могут прочитать, например, в книгах [6, 14, 22] из прилагаемой литературы. В качестве еще одного “самодостаточного” раздела математической логики выступает *теория алгоритмов*. С ее основными результатами и методами читатель может ознакомиться в учебниках [3, 7, 15].

Авторы выражают искреннюю благодарность Михаилу Шушпанову за помощь в оформлении данного пособия.

Глава 1

Логика высказываний и булевы функции

Логика как наука о законах и формах мышления имеет многовековую историю. Математическая же логика сформировалась сравнительно недавно — на рубеже девятнадцатого и двадцатого столетий — в результате применения к логике математических методов.

Учение о высказываниях, называемое логикой высказываний, является исторически первой и наиболее простой частью математической логики. Его законы служат отправной точкой в овладении более трудными разделами данного предмета. В этой главе мы поймем, как эти законы применяются при проверке на корректность различного рода умозаключений, а также увидим, как они могут использоваться в далеких, на первый взгляд, от логики высказываний отраслях знаний, а именно, в технике — при анализе релейно-контактных схем.

§ 1.1. Формулы логики высказываний и их интерпретации

Основным объектом изучения логики высказываний являются высказывания и логические связки. Под высказыванием будем понимать повествовательное предложение, про которое можно сказать, что оно истинно или ложно. Например, предложения “Екате-

ринбург – крупный административный центр Урала” и “Волга впадает в Черное море” являются высказываниями, различающимися лишь тем, что первое из них истинно, а второе ложно. В дальнейшем мы отвлечемся от содержания высказываний и будем интересоваться только их истинностными значениями. Высказывания будем обозначать большими латинскими буквами A, B, C, \dots , именуемыми *логическими переменными*, а их значения, т.е. истину или ложь, соответственно цифрами **1** и **0**, именуемыми *логическими константами*.

В русском языке из простых высказываний более сложные конструируются с помощью слов “не”, “и”, “или”, “если ..., то ...”, “тогда и только тогда, когда ...”. В логике им соответствуют символы, называемые *логическими связками*: частице “не” соответствует символ \neg (отрицание), союзу “и” — символ \wedge (конъюнкция), союзу “или” — символ \vee (дизъюнкция), конструкции “если ..., то ...” — символ \longrightarrow (импликация), конструкции “тогда и только тогда, когда ...” — символ \longleftrightarrow (эквиваленция).

Мы обычно записываем высказывания в виде предложений русского языка. В математической логике высказывания принято записывать в виде *формул логики высказываний* (сокращенно ФЛВ). Определим ФЛВ индукцией по длине, т.е. количеству используемых в них логических связок:

- (i) логические константы **0**, **1** являются ФЛВ;
- (ii) логические переменные A, B, C, \dots являются ФЛВ;
- (iii) если F и G — ФЛВ, то выражения вида $\neg F$, $(F \wedge G)$, $(F \vee G)$, $(F \longrightarrow G)$ и $(F \longleftrightarrow G)$ также являются ФЛВ;
- (iv) других формул нет.

Первые два пункта (i) и (ii) являются базой индуктивного определения ФЛВ, пункт (iii) — его шагом, показывающим, как из формул меньшей длины с помощью логических связок строятся формулы большей длины. Пункт (iv) в определении ФЛВ необходим и подчеркивает, что каждая ФЛВ получается только лишь по одному из правил (i), (ii), (iii). Так, выражения $((A \longrightarrow B) \vee C) \longleftrightarrow (\neg C \longrightarrow \mathbf{0})$ и $((\neg A \vee \mathbf{1}) \wedge (\neg \neg A \vee \mathbf{0})) \longrightarrow (B \longleftrightarrow \neg B)$ — ФЛВ, а выражение $(\vee(A \longleftrightarrow B) \neg C)$ не является ФЛВ.

В целях упрощения записи формул договоримся о силе логических связок: $\neg, \wedge, \vee, \longrightarrow, \longleftrightarrow$; здесь связки расположены по убыванию их силы слева направо. Пользуясь этим соглашением, некоторые скобки в формулах будем опускать; внешние скобки также писать не будем. Например, приведенные выше две формулы

можно было бы записать в виде: $(A \rightarrow B) \vee C \leftrightarrow \neg C \rightarrow \mathbf{0}$ и $(\neg A \vee \mathbf{1}) \wedge (\neg \neg A \vee \mathbf{0}) \rightarrow (B \leftrightarrow \neg B)$.

Зная истинностные значения высказываний A и B , мы можем (в соответствии со здравым смыслом) найти истинностные значения высказываний $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \leftrightarrow B$. Например, совершенно естественно считать, что $\neg A$ истинно в том и только в том случае, если A ложно, а $A \wedge B$ истинно тогда и только тогда, когда оба высказывания A и B истинны. Эти интуитивные представления лежат в основе следующей таблицы, позволяющей в конечном счете вычислять истинностные значения сколь угодно сложных высказываний:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Из таблицы видно, что высказывание $A \rightarrow B$ ложно тогда и только тогда, когда A истинно, а B ложно. A называется *посылкой*, а B *следствием*. Таким образом, если посылка A ложна, то высказывание $A \rightarrow B$ всегда истинно независимо от того, истинно или нет следствие B . Это свойство импликации кратко формулируется так: “из лжи следует все, что угодно”. Такое понимание импликации позволяет смотреть на бессмысленное в обычной речи предложение “если соль сладкая, то сахар белый” как на вполне приемлемое с точки зрения математической логики высказывание, которое является истинным.

Интерпретацией одной или нескольких ФЛВ называется произвольное отображение множества их логических переменных в множество логических констант. Пусть F – ФЛВ с множеством логических переменных X и $\phi : X \rightarrow \{\mathbf{0}, \mathbf{1}\}$ – некоторая интерпретация F . *Истинностное значение* $\phi(F)$ формулы F при интерпретации ϕ определяется индукцией по длине F :

(i) если $F = \mathbf{1}$ или $F = \mathbf{0}$, то соответственно $\phi(F) = \mathbf{1}$ или $\phi(F) = \mathbf{0}$;

(ii) если $F = A$ – логическая переменная, то $\phi(F) = \phi(A)$;

(iii) если $F = \neg G$ или $F = G \wedge H$, или $F = G \vee H$, или $F = G \rightarrow H$, или $F = G \leftrightarrow H$, то соответственно $\phi(F) = \neg\phi(G)$ или $\phi(F) = \phi(G) \wedge \phi(H)$, или $\phi(F) = \phi(G) \vee \phi(H)$, или $\phi(F) = \phi(G) \rightarrow \phi(H)$, или $\phi(F) = \phi(G) \leftrightarrow \phi(H)$ (см. таблицу выше).

Нетрудно видеть, что если в формулу F входит n логических переменных, то F имеет в точности 2^n попарно различных интерпретаций. Таблицу, в которой для каждой интерпретации формулы F указывается ее истинностное значение, принято называть *таблицей истинности* для F . Ниже приведена таблица истинности для ФЛВ $F = (A \rightarrow B \wedge C) \wedge (\neg A \rightarrow \neg B)$; каждая из восьми ее строк соответствует конкретной интерпретации.

A	B	C	$\neg A$	$\neg B$	$B \wedge C$	$A \rightarrow B \wedge C$	$\neg A \rightarrow \neg B$	F
1	1	1	0	0	1	1	1	1
1	1	0	0	0	0	0	1	0
1	0	1	0	1	0	0	1	0
1	0	0	0	1	0	0	1	0
0	1	1	1	0	1	1	0	0
0	1	0	1	0	0	1	0	0
0	0	1	1	1	0	1	1	1
0	0	0	1	1	0	1	1	1

Как видим, ФЛВ может принимать различные истинностные значения в зависимости от интерпретации. ФЛВ называется *тавтологией* (соответственно *противоречием*), если при любой интерпретации она истинна (соответственно ложна). ФЛВ называется *выполнимой*, если для некоторой интерпретации она принимает значение 1. Из определения немедленно вытекает, что множество всех ФЛВ разбивается на два непересекающихся класса: класс выполнимых формул и класс противоречий. Первый из них содержит тавтологии в качестве собственного подкласса. Приведенная выше ФЛВ F , не будучи тавтологией, является выполнимой формулой.

§ 1.2. Отношение равносильности на множестве ФЛВ. Законы логики высказываний

Будем говорить, что две ФЛВ F и G равносильны, и писать $F \equiv G$, если для любой интерпретации ϕ этих формул $\phi(F) = \phi(G)$. Очевидно, отношение равносильности на множестве всех ФЛВ рефлексивно, симметрично и транзитивно и, следовательно, является *отношением эквивалентности*, разбивающим это множество на классы равносильных формул. Примерами таких классов могут служить класс тавтологий и класс противоречий, ибо на тавтологию и на противоречие можно смотреть как на формулы, равносильные соответственно формулам **1** и **0**.

Приведем на языке равносильности формул наиболее важные законы логики высказываний (здесь F , G , H — произвольные ФЛВ).

1. *Законы коммутативности:*

$$F \wedge G \equiv G \wedge F,$$

$$F \vee G \equiv G \vee F,$$

$$F \leftrightarrow G \equiv G \leftrightarrow F.$$

2. *Законы ассоциативности:*

$$F \wedge (G \wedge H) \equiv (F \wedge G) \wedge H,$$

$$F \vee (G \vee H) \equiv (F \vee G) \vee H.$$

3. *Законы дистрибутивности:*

$$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H),$$

$$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H).$$

4. *Законы идемпотентности:*

$$F \wedge F \equiv F,$$

$$F \vee F \equiv F.$$

5. *Законы поглощения:*

$$F \wedge (F \vee G) \equiv F,$$

$$F \vee (F \wedge G) \equiv F.$$

6. *Закон двойного отрицания:*

$$\neg\neg F \equiv F.$$

7. *Закон импликации:*

$$F \longrightarrow G \equiv \neg F \vee G.$$

8. *Закон контрапозиции:*

$$F \longrightarrow G \equiv \neg G \longrightarrow \neg F.$$

9. *Законы де Моргана (двойственности):*

$$\neg(F \wedge G) \equiv \neg F \vee \neg G,$$

$$\neg(F \vee G) \equiv \neg F \wedge \neg G.$$

10. *Закон исключенного третьего:*

$$F \vee \neg F \equiv \mathbf{1}.$$

11. *Закон противоречия:*

$$F \wedge \neg F \equiv \mathbf{0}.$$

12. *Закон эквиваленции:*

$$F \leftrightarrow G \equiv (F \longrightarrow G) \wedge (G \longrightarrow F).$$

13. $F \vee \mathbf{1} \equiv \mathbf{1}$, $F \wedge \mathbf{1} \equiv F$, $F \vee \mathbf{0} \equiv F$, $F \wedge \mathbf{0} \equiv \mathbf{0}$.

Разумеется, каждый из этих законов нуждается в проверке, которая осуществляется с помощью простого сравнения таблиц истинности соответствующих ФЛВ. Например, сравнивая таблицы истинности формул $\neg(F \wedge G)$ и $\neg F \vee \neg G$ (см. ниже), получаем один из законов де Моргана: $\neg(F \wedge G) \equiv \neg F \vee \neg G$. Проверка остальных законов логики высказываний предоставляется читателю.

F	G	$F \wedge G$	$\neg(F \wedge G)$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	1

и

F	G	$\neg F$	$\neg G$	$\neg F \vee \neg G$
1	1	0	0	0
1	0	0	1	1
0	1	1	0	1
0	0	1	1	1

Учитывая законы ассоциативности, введем еще одно соглашение по экономии скобок: будем опускать скобки в конъюнкции и дизъюнкции, содержащих более двух членов. Так, вместо формул $(A \wedge B) \wedge C$ и $(A \vee B) \vee (C \vee D)$ будем писать $A \wedge B \wedge C$ и $A \vee B \vee C \vee D$.

Знание основных законов логики высказываний позволяет *упрощать* ФЛВ, т.е. по данной ФЛВ находить равносильную ей ФЛВ наиболее простого вида.

ПРИМЕР. Упростить формулу $\neg A \wedge \neg(\neg A \wedge \neg B) \longrightarrow B$.

Выпишем последовательность равносильных формул, указав для удобства над каждым знаком \equiv номер примененного закона:

$$\begin{aligned} \neg A \wedge \neg(\neg A \wedge \neg B) \longrightarrow B &\equiv^7 \neg(\neg A \wedge \neg(\neg A \wedge \neg B)) \vee B \equiv^9 \\ (\neg \neg A \vee \neg \neg(\neg A \wedge \neg B)) \vee B &\equiv^6 (A \vee (\neg A \wedge \neg B)) \vee B \equiv^3 \\ (A \vee \neg A) \wedge (A \vee \neg B) \vee B &\equiv^{10} \mathbf{1} \wedge (A \vee \neg B) \vee B \equiv^{13} \\ (A \vee \neg B) \vee B &\equiv^2 A \vee (\neg B \vee B) \equiv^{10} A \vee \mathbf{1} \equiv^{13} \mathbf{1}. \end{aligned}$$

Поскольку данная формула равносильна **1**, заключаем, что она является тавтологией.

§ 1.3. Логическое следование. Анализ рассуждений

Понятие логического следования является одной из формализаций доказательства теорем, имеющих, как правило, такую формулировку: пусть выполнены утверждения A_1, \dots, A_n ; тогда выполняется утверждение B . Дадим необходимое определение.

Пусть Γ – некоторое множество ФЛВ и F – произвольная ФЛВ. Будем говорить, что F логически следует из Γ , если для любой интерпретации множества формул $\Gamma \cup \{F\}$ из того, что каждая формула из Γ истинна, вытекает, что и F истинна. В этом случае будем писать $\Gamma \models F$ (в противном случае – $\Gamma \not\models F$). Пользуясь определением логического следования, читатель легко может проверить, что, например, $A, A \rightarrow B \models B$, в то время как $B, A \rightarrow B \not\models A$. Очевидно, для любых ФЛВ F и G имеем $F \equiv G$ тогда и только тогда, когда $F \models G$ и $G \models F$.

Если множество Γ состоит из достаточно большого числа формул, то пользоваться непосредственно определением для доказательства того, что $\Gamma \models F$, не совсем удобно. В этом случае полезна следующая теорема.

ТЕОРЕМА. Для любых ФЛВ F_1, \dots, F_n, G выполнено:

- а) $F_1, \dots, F_n \models G$ в том и только в том случае, если формула $F_1 \wedge \dots \wedge F_n \rightarrow G$ является тавтологией;
 б) $F_1, \dots, F_n \models G$ в том и только в том случае, если формула $F_1 \wedge \dots \wedge F_n \wedge \neg G$ является противоречием.

Доказательство. а). Пусть $F_1, \dots, F_n \models G$ и ϕ – произвольная интерпретация формулы $F_1 \wedge \dots \wedge F_n \rightarrow G$. Тогда если для некоторого $i \in \{1, \dots, n\}$ выполнено $\phi(F_i) = \mathbf{0}$, то $\phi(F_1 \wedge \dots \wedge F_n) = \mathbf{0}$ и, следовательно, $\phi(F_1 \wedge \dots \wedge F_n \rightarrow G) = \mathbf{1}$. Если же для каждого $i \in \{1, \dots, n\}$ имеем $\phi(F_i) = \mathbf{1}$, то ввиду $F_1, \dots, F_n \models G$ выполнено $\phi(G) = \mathbf{1}$ и потому $\phi(F_1 \wedge \dots \wedge F_n \rightarrow G) = \mathbf{1}$. Так как интерпретация ϕ выбрана произвольно, заключаем, что формула $F_1 \wedge \dots \wedge F_n \rightarrow G$ является тавтологией.

Обратно, пусть $F_1 \wedge \dots \wedge F_n \rightarrow G$ – тавтология и $\phi(F_i) = \mathbf{1}$ при $i = 1, \dots, n$. Тогда $\phi(F_1 \wedge \dots \wedge F_n) = \mathbf{1}$ и $\phi(F_1 \wedge \dots \wedge F_n \rightarrow G) = \mathbf{1}$, откуда $\phi(G) = \mathbf{1}$. Ввиду произвольности ϕ это означает, что $F_1, \dots, F_n \models G$.

б). Заметим, что $\neg(F_1 \wedge \dots \wedge F_n \rightarrow G) \equiv \neg(\neg(F_1 \wedge \dots \wedge F_n) \vee G) \equiv \neg\neg(F_1 \wedge \dots \wedge F_n) \wedge \neg G \equiv F_1 \wedge \dots \wedge F_n \wedge \neg G$. Поэтому формула $F_1 \wedge \dots \wedge F_n \rightarrow G$ будет тавтологией тогда и только тогда, когда формула $F_1 \wedge \dots \wedge F_n \wedge \neg G$ будет противоречием. Отсюда и из доказанного утверждения “а” следует, что $F_1, \dots, F_n \models G$ в том и только в том случае, если $F_1 \wedge \dots \wedge F_n \wedge \neg G$ – противоречие.

Из утверждения “а” этой теоремы вытекает, что для ФЛВ F и G условие $F \models G$ равносильно тому, что $F \rightarrow G$ – тавтология, т.е. отношение логического следования и импликация тесным обра-

зом связаны между собой. Это иногда приводит к путанице данных понятий, что, конечно, недопустимо.

Покажем, как понятие логического следования используется при анализе некоторых рассуждений. В приводимых ниже примерах требуется проверить правильность логического заключения.

ПРИМЕР 1. Наша футбольная команда либо выигрывает матч, либо проигрывает, либо сводит его к ничьей. Если матч выигран или проигран, то он не перенесен. Команда матч не выиграла и не свела его к ничьей. Следовательно, матч не перенесен и проигран.

Введем необходимые обозначения:

A — “матч выигран”,

B — “матч проигран”,

C — “матч закончился ничьей”,

D — “матч перенесен”.

Тогда входящие в данное рассуждение высказывания можно переписать соответственно в виде: $A \vee B \vee C$, $A \vee B \rightarrow \neg D$, $\neg A \wedge \neg C$ и $\neg D \wedge B$. Спрашивается, верно ли, что

$$A \vee B \vee C, A \vee B \rightarrow \neg D, \neg A \wedge \neg C \models \neg D \wedge B ?$$

Для ответа на этот вопрос рассмотрим произвольную интерпретацию ϕ такую, что $\phi(A \vee B \vee C) = \mathbf{1}$, $\phi(A \vee B \rightarrow \neg D) = \mathbf{1}$, $\phi(\neg A \wedge \neg C) = \mathbf{1}$, и проверим равенство $\phi(\neg D \wedge B) = \mathbf{1}$. Действительно, по условию $\phi(\neg A \wedge \neg C) = \neg\phi(A) \wedge \neg\phi(C) = \mathbf{1}$, откуда имеем $\phi(A) = \phi(C) = \mathbf{0}$. Отсюда и из равенства $\phi(A \vee B \vee C) = \mathbf{1}$ получаем, что $\phi(B) = \mathbf{1}$. Учитывая теперь условие $\phi(A \vee B \rightarrow \neg D) = \mathbf{1}$, делаем вывод: $\mathbf{1} = \phi(A) \vee \phi(B) \rightarrow \phi(\neg D) = \mathbf{1} \rightarrow \phi(\neg D)$, т.е. $\phi(\neg D) = \mathbf{1}$, $\phi(D) = \mathbf{0}$. Поэтому $\phi(\neg D \wedge B) = \phi(\neg D) \wedge \phi(B) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. Таким образом, указанное логическое следование справедливо, а значит, рассуждение корректно.

ПРИМЕР 2. Кривая является или эллипсом, или параболой, или гиперболой. Если кривая — эллипс или гипербола, то она центральна. Данная кривая не эллипс и не парабола. Следовательно, она центральна и является гиперболой.

Обозначим через A (соответственно B и C) высказывание “данная кривая является эллипсом” (соответственно “параболой” и “гиперболой”), а через D — высказывание “кривая центральна”. Мы хотим проверить, верно или нет, что $A \vee B \vee C$, $A \vee C \rightarrow D$, $\neg A \wedge \neg B \models$

$D \wedge C$. Для этого ввиду утверждения “б” доказанной теоремы достаточно проверить, будет ли формула

$$F = (A \vee B \vee C) \wedge (A \vee C \longrightarrow D) \wedge (\neg A \wedge \neg B) \wedge \neg(D \wedge C)$$

противоречием. Упростим формулу F с помощью равносильных преобразований следующим образом:

$$\begin{aligned} F &\equiv^1 (A \vee B \vee C) \wedge (\neg A \wedge \neg B) \wedge (A \vee C \longrightarrow D) \wedge \neg(D \wedge C) \equiv^{7,9} \\ &(A \vee B \vee C) \wedge \neg(A \vee B) \wedge (\neg(A \vee C) \vee D) \wedge (\neg D \vee \neg C) \equiv^{3,9} \\ &(((A \vee B) \wedge \neg(A \vee B)) \vee (C \wedge \neg(A \vee B))) \wedge ((\neg A \wedge \neg C) \vee D) \\ &\wedge (\neg D \vee \neg C) \equiv^{11,9} \\ &(\mathbf{0} \vee (C \wedge \neg A \wedge \neg B)) \wedge ((\neg A \wedge \neg C) \vee D) \wedge (\neg D \vee \neg C) \equiv^{13,3} \\ &C \wedge \neg A \wedge \neg B \wedge (\neg A \vee D) \wedge (\neg C \vee D) \wedge (\neg D \vee \neg C) \equiv^{1,5,3} \\ &C \wedge \neg A \wedge \neg B \wedge (\neg C \vee (D \wedge \neg D)) \equiv^{11,13} C \wedge \neg A \wedge \neg B \wedge \neg C \equiv^{1,11} \\ &\mathbf{0} \wedge \neg A \wedge \neg B \equiv^{13} \mathbf{0}. \end{aligned}$$

Получили, что формула F , будучи равносильной $\mathbf{0}$, является противоречием. Отсюда заключаем, что $A \vee B \vee C$, $A \vee C \longrightarrow D$, $\neg A \wedge \neg B \models D \wedge C$, т.е. рассуждение корректно.

§ 1.4. Виды теорем. Обоснование некоторых методов доказательства в математике

Большинство доказываемых в математике теорем можно записать в виде формулы $P \longrightarrow Q$, где P — посылка теоремы, являющаяся, как правило, конъюнкцией одного или нескольких условий, а Q — ее заключение. По отношению к теореме $P \longrightarrow Q$, которая называется *прямой*, теоремы вида $Q \longrightarrow P$, $\neg P \longrightarrow \neg Q$ и $\neg Q \longrightarrow \neg P$ называются соответственно *обратной*, *противоположной* и *обратной к противоположной* теоремами. Ввиду закона контрапозиции прямая теорема $P \longrightarrow Q$ равносильна обратной к противоположной теореме $\neg Q \longrightarrow \neg P$, а обратная теорема $Q \longrightarrow P$ равносильна противоположной теореме $\neg P \longrightarrow \neg Q$. Вместе с тем, легко построить пример, когда прямая теорема верна, а обратная к ней нет.

Один из распространенных методов доказательства в математике основан как раз на равносильности прямой и обратной к противоположной теорем: доказательство утверждения вида $P \longrightarrow Q$ сводится к проверке импликации $\neg Q \longrightarrow \neg P$. Докажем этим методом, что *если (P) множество M состоит из $n+1$ -го натурального числа, то (Q) в M найдутся два числа, разность которых делится на n* . Предположим, что ($\neg Q$) разность любых двух чисел из

M не делится на n . Это означает, что числа из M при делении на n дают попарно различные остатки. Так как множество чисел $\{0, 1, 2, \dots, n-1\}$ исчерпывает всевозможные остатки при делении на n , получаем, что M состоит не более чем из n натуральных чисел и, следовательно, выполнено $\neg P$.

Второй популярный метод доказательства – *метод доказательства от противного* (хорошо известна шутка: если не знаешь, как доказывать, – доказывай от противного). Суть этого метода состоит в том, что, доказывая утверждение P , допускают (от противного) истинность утверждения $\neg P$ и из этого предположения получают одновременно истинность как некоторого утверждения Q , так и его отрицания $\neg Q$. На базе данного противоречия делают вывод, что имеет место P . Обоснование этого метода заключается в проверке логического следования $\neg P \rightarrow Q, \neg P \rightarrow \neg Q \models P$. В самом деле, имеем $(\neg P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q) \wedge \neg P \equiv (P \vee Q) \wedge (P \vee \neg Q) \wedge \neg P \equiv (P \vee (Q \wedge \neg Q)) \wedge \neg P \equiv (P \vee \mathbf{0}) \wedge \neg P \equiv P \wedge \neg P \equiv \mathbf{0}$, т.е. формула $(\neg P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q) \wedge \neg P$ является противоречием, а потому по теореме из предыдущего параграфа выполнено $\neg P \rightarrow Q, \neg P \rightarrow \neg Q \models P$.

Докажем, например, методом от противного, что (P) число $\sqrt{2}$ иррационально. Предположим, что $(\neg P)$ число $\sqrt{2}$ является рациональным, т.е. представимо в виде $\sqrt{2} = n/m$, где n и m – некоторые натуральные числа. Рассмотрим множество M всех пар (n, m) взаимно простых натуральных чисел, таких, что $\sqrt{2} = n/m$, и через Q обозначим высказывание “ M – пустое множество”. Проверим сначала импликацию $\neg P \rightarrow Q$. Действительно, для любых чисел n и m , если $\sqrt{2} = n/m$, то $2m^2 = n^2$, откуда следует, что n должно быть четным, т.е. $n = 2n_1$ для некоторого натурального n_1 . Тогда $2m^2 = n^2 = 4n_1^2$, и значит, $m^2 = 2n_1^2$, откуда уже вытекает четность числа m . Мы получили, что условие $\sqrt{2} = n/m$ влечет делимость обоих чисел n и m на два, т.е. (Q) множество M пусто. С другой стороны, для любой пары натуральных чисел n и m , если $\sqrt{2} = n/m$ и $n = dn', m = dm'$, где $d = \text{НОД}(n, m)$, то $\sqrt{2} = n'/m'$, причем числа n' и m' уже взаимно просты. Таким образом, имеет место и импликация $\neg P \rightarrow \neg Q$, где $\neg Q$ – высказывание “множество M не пусто”. Полученное противоречие доказывает, что число $\sqrt{2}$ иррационально.

Два приведенных метода относятся к типу так называемых *косвенных* доказательств, ибо построены на предположении об истинности отрицания доказываемого утверждения. Методы, не ис-

пользующие отрицания доказываемого утверждения, относятся к типу *прямых* доказательств. Таковыми являются два оставшихся метода из приводимых нами. Первый из них — *метод разбора случаев* — базируется на логическом следовании $P_1 \vee \dots \vee P_n, P_1 \longrightarrow Q, \dots, P_n \longrightarrow Q \models Q$ и заключается в том, что утверждение Q доказывается в каждом из случаев P_1, \dots, P_n , исчерпывающих все возможности. Для его обоснования достаточно проверить, что формула $F = (P_1 \vee \dots \vee P_n) \wedge (P_1 \longrightarrow Q) \wedge \dots \wedge (P_n \longrightarrow Q) \wedge \neg Q$ является противоречием. Действительно,

$$\begin{aligned} F &= (P_1 \vee \dots \vee P_n) \wedge (P_1 \longrightarrow Q) \wedge \dots \wedge (P_n \longrightarrow Q) \wedge \neg Q \equiv \\ &(P_1 \vee \dots \vee P_n) \wedge (\neg P_1 \vee Q) \wedge \dots \wedge (\neg P_n \vee Q) \wedge \neg Q \equiv \\ &(P_1 \vee \dots \vee P_n) \wedge \neg Q \wedge ((\neg P_1 \wedge \dots \wedge \neg P_n) \vee Q) \equiv \\ &(P_1 \vee \dots \vee P_n) \wedge \neg Q \wedge \neg((P_1 \vee \dots \vee P_n) \wedge \neg Q) \equiv \mathbf{0}. \end{aligned}$$

В качестве примера докажем, что (Q) для любого натурального n число $n^5 - n$ делится на пять. В самом деле, заметим, что $n^5 - n = n(n-1)(n+1)(n^2+1)$ и рассмотрим пять случаев $(P_1 - P_5)$ в зависимости от того, какой из остатков от нуля до четырех дает число n при делении на пять. В каждом из этих случаев один из сомножителей $n, n-1, n+1, n^2+1$, а следовательно, и само число $n^5 - n$ делится на пять, откуда вытекает доказываемое утверждение Q .

Наконец, последний метод — *метод построения цепочки импликаций* — основан на очевидном логическом следовании: $P_1, P_1 \longrightarrow P_2, \dots, P_{n-1} \longrightarrow P_n \models P_n$. Он неявно присутствует практически в любом математическом утверждении и поэтому не нуждается в дополнительных примерах.

§ 1.5. Булевы функции. Полные системы логических связей

Пусть M — произвольное множество. Напомним, что n -й *декартовой степени* M^n *множества* M называется множество всех упорядоченных n -к элементов из M , т.е.

$M^n = \{(a_1, \dots, a_n) \mid a_i \in M, i = 1, \dots, n\}$. Так, взяв в качестве M множество логических констант, имеем по определению

$$\{\mathbf{0}, \mathbf{1}\}^n = \{(X_1, \dots, X_n) \mid X_i = \mathbf{0} \text{ или } X_i = \mathbf{1}, i = 1, \dots, n\}.$$

Булевой функцией от n переменных называется произвольное отображение n -й декартовой степени множества логических констант в множество логических констант. Далее для словосочетания “булева функция” будем использовать сокращение БФ. В сущ-

ности, мы уже имели дело с БФ, когда вычисляли истинностные значения ФЛВ при конкретных интерпретациях. Рассмотрим ФЛВ $X_1 \vee X_2 \rightarrow X_3$. Ей соответствует БФ $f(X_1, X_2, X_3)$ такая, что, например, $f(\mathbf{1}, \mathbf{1}, \mathbf{1}) = \mathbf{1}$ и $f(\mathbf{0}, \mathbf{0}, \mathbf{0}) = \mathbf{1}$, а $f(\mathbf{1}, \mathbf{1}, \mathbf{0}) = \mathbf{0}$ и $f(\mathbf{0}, \mathbf{1}, \mathbf{0}) = \mathbf{0}$. Если БФ $f(X_1, X_2, X_3)$ определена с помощью некоторой ФЛВ F , то говорят, что она задана *аналитически*, и в этом случае пишут $f(X_1, \dots, X_n) = F$. Приведенную выше БФ мы могли бы записать в виде $f(X_1, X_2, X_3) = X_1 \vee X_2 \rightarrow X_3$. БФ можно задавать также *табличным способом*. Очевидно, всякую БФ, заданную аналитически, можно определить с помощью таблицы истинности соответствующей ФЛВ. Поставим следующий естественный вопрос: *всякая ли БФ (заданная табличным способом) определяется аналитически?* Ответ на этот вопрос оказывается положительным и содержится в приводимой ниже теореме о представлении БФ.

Пусть X – логическая переменная и $A \in \{\mathbf{0}, \mathbf{1}\}$. Введем следующее обозначение:

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

Выражение X^A , т.е. X или $\neg X$, принято называть *литерой* переменной X . *Элементарной конъюнкцией* называется конъюнкция одной или нескольких литер различных переменных. Например, выражения X и $\neg X \wedge Y \wedge \neg Z$ суть элементарные конъюнкции, а $X \wedge \neg X$ и $X \wedge \neg Y \vee \neg Z$ таковыми не являются. Две элементарные конъюнкции мы не различаем, если одна из них получается из другой перестановкой литер переменных.

ЛЕММА 1. *Для любой интерпретации ϕ переменной X выполнено $\phi(X^A) = \mathbf{1}$ тогда и только тогда, когда $\phi(X) = A$.*

Справедливость этого утверждения наглядно иллюстрируется следующей таблицей:

X	A	X^A
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$

ЛЕММА 2. *Для любой интерпретации ϕ элементарной конъюнкции $X_1^{A_1} \wedge X_2^{A_2} \wedge \dots \wedge X_n^{A_n}$ выполнено $\phi(X_1^{A_1} \wedge X_2^{A_2} \wedge \dots \wedge X_n^{A_n}) = \mathbf{1}$ тогда и только тогда, когда $\phi(X_i) = A_i$ для каждого $i = 1, 2, \dots, n$.*

Доказательство. Равенство $\phi(X_1^{A_1} \wedge X_2^{A_2} \wedge \dots \wedge X_n^{A_n}) = \mathbf{1}$ равносильно тому, что $\phi(X_1^{A_1}) = \phi(X_2^{A_2}) = \dots = \phi(X_n^{A_n}) = \mathbf{1}$, а это, по лемме 1, имеет место в том и только в том случае, если $\phi(X_1) = A_1$, $\phi(X_2) = A_2$, ..., $\phi(X_n) = A_n$.

Теперь мы можем доказать основной результат данного параграфа.

ТЕОРЕМА о представлении БФ. Пусть $f(X_1, \dots, X_n)$ — БФ. Тогда если f принимает хотя бы один раз значение $\mathbf{1}$, то она представима в виде

$$f(X_1, \dots, X_n) = \bigvee_{f(A_1, \dots, A_n)=\mathbf{1}} (X_1^{A_1} \wedge \dots \wedge X_n^{A_n}). \quad (*)$$

В противном случае имеет место очевидное равенство

$$f(X_1, \dots, X_n) = X_1 \wedge \neg X_1.$$

Доказательство. Мы хотим проверить, что левая и правая части равенства (*) совпадают для любой интерпретации $\phi(X_i) = S_i (i = 1, \dots, n)$ при условии, что $\{(A_1, \dots, A_n) \mid f(A_1, \dots, A_n) = \mathbf{1}\} \neq \emptyset$. Рассмотрим два случая.

Случай 1. $f(S_1, \dots, S_n) = \mathbf{1}$. Тогда ввиду леммы 2 имеем $\phi(X_1^{S_1} \wedge \dots \wedge X_n^{S_n}) = \mathbf{1}$, и поскольку правая часть равенства (*) содержит элементарную конъюнкцию $X_1^{S_1} \wedge \dots \wedge X_n^{S_n}$, дизъюнкция $\bigvee_{f(A_1, \dots, A_n)=\mathbf{1}} (X_1^{A_1} \wedge \dots \wedge X_n^{A_n})$ истинна при данной интерпретации ϕ .

Случай 2. $f(S_1, \dots, S_n) = \mathbf{0}$. Тогда если элементарная конъюнкция $X_1^{A_1} \wedge \dots \wedge X_n^{A_n}$ входит в правую часть равенства (*), то $f(A_1, \dots, A_n) = \mathbf{1}$ и, следовательно, $\phi(X_i) = S_i \neq A_i$ для некоторого индекса $i \in \{1, \dots, n\}$. В силу леммы 2 это означает, что $\phi(X_1^{A_1} \wedge \dots \wedge X_n^{A_n}) = \mathbf{0}$. Таким образом, дизъюнкция в правой части равенства (*) берется по элементарным конъюнкциям, каждая из которых ложна при интерпретации ϕ , а потому сама она ложна при этой интерпретации. Теорема доказана.

ПРИМЕР. Построить формулу, задающую БФ f от переменных X_1, X_2, X_3 , которая принимает значение $\mathbf{1}$ тогда и только тогда, когда большинство ее переменных принимает значение $\mathbf{1}$.

Для удобства выпишем таблицу значений функции f (достаточно указать строки, когда f истинна).

X_1	X_2	X_3	$f(X_1, X_2, X_3)$
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1

По доказанной теореме имеем $f(X_1, X_2, X_3) = (X_1^1 \wedge X_2^1 \wedge X_3^1) \vee (X_1^1 \wedge X_2^1 \wedge X_3^0) \vee (X_1^1 \wedge X_2^0 \wedge X_3^1) \vee (X_1^0 \wedge X_2^1 \wedge X_3^1) = (X_1 \wedge X_2 \wedge X_3) \vee (X_1 \wedge X_2 \wedge \neg X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3) \vee (\neg X_1 \wedge X_2 \wedge X_3)$.

Система логических связок M называется *полной*, если всякая БФ может быть представлена в виде некоторой ФЛВ, содержащей лишь связки из M . Учитывая теорему о представлении БФ, получаем, что система связок $\{\neg, \wedge, \vee\}$ является полной. Закономерен вопрос: существуют ли полные системы, содержащие меньшее число логических связок? Для ответа на него обратимся к следующему очевидному утверждению: *пусть M – полная система логических связок и K – некоторая система связок; тогда если каждая связка из M может быть выражена через связки из K , то система связок K так же полна.*

Если в качестве M возьмем множество $\{\neg, \wedge, \vee\}$, а в качестве K – любое из множеств $\{\neg, \wedge\}$, $\{\neg, \vee\}$, $\{\neg, \longrightarrow\}$, то поскольку $X \vee Y \equiv \neg X \longrightarrow Y$ и $X \wedge Y \equiv \neg(X \longrightarrow \neg Y)$, заключаем, что множества $\{\neg, \wedge\}$, $\{\neg, \vee\}$ и $\{\neg, \longrightarrow\}$ являются полными системами логических связок. Вместе с тем, легко понять, что ни одна из связок \neg , \wedge , \vee , \longrightarrow , \longleftarrow в отдельности не образует полную систему.

Наряду с уже известными связками (легко воспринимаемыми нашей интуицией) в логике рассматриваются и другие. Выделим из них: *стрелку Пирса* (\downarrow) и *штрих Шеффера* ($|$).

A	B	$A \downarrow B$	$A B$
1	1	0	0
1	0	0	1
0	1	0	1
0	0	1	1

Читателю предоставляется возможность самому проверить, что $\neg X \equiv X \downarrow X$, $X \wedge Y \equiv (X \downarrow X) \downarrow (Y \downarrow Y)$ и $\neg X \equiv X | X$, $X \vee Y \equiv (X | X) | (Y | Y)$. Отсюда и из полноты систем связок $\{\neg, \wedge\}$ и $\{\neg, \vee\}$ вытекает полнота одноэлементных систем связок $\{\downarrow\}$ и $\{| \}$.

Заметим, что связки \downarrow и $|$ следующим образом выражаются через \neg , \wedge и \vee : $X \downarrow Y \equiv \neg X \wedge \neg Y$, $X | Y \equiv \neg X \vee \neg Y$.

§ 1.6. Дизъюнктивные нормальные формы

ФЛВ называется *дизъюнктивной нормальной формой* (сокращенно ДНФ), если она является дизъюнкцией одной или нескольких различных элементарных конъюнкций. Ниже мы увидим, что всякая выполнимая ФЛВ равносильными преобразованиями приводится к некоторой ДНФ, и этим объясняется важность вычленения ДНФ в классе всех ФЛВ. Однако для одной и той же ФЛВ могут существовать несколько попарно различных ДНФ, к которым она приводится. Ситуация не изменится, если даже потребовать, чтобы все эти ДНФ были от одного и того же набора переменных. Например, формула $F = (A \vee B) \wedge (A \vee \neg C)$ приводится равносильными преобразованиями как к ДНФ вида $F_1 = A \vee (B \wedge \neg C)$, так и к ДНФ вида $F_2 = (A \wedge \neg B) \vee (B \wedge \neg C) \vee (A \wedge B)$. В этом смысле более “привлекательными” являются так называемые *совершенные дизъюнктивные нормальные формы* (сокращенно СДНФ). ДНФ называется СДНФ, если каждая ее элементарная конъюнкция зависит от одного и того же набора логических переменных. Докажем основной результат данного пункта.

ТЕОРЕМА О СДНФ. *Всякая выполнимая ФЛВ равносильна некоторой СДНФ, причем последняя определяется однозначно с точностью до перестановки элементарных конъюнкций и по набору переменных.*

Доказательство. Пусть F – произвольная выполнимая ФЛВ от переменных X_1, \dots, X_n . Обозначим через $f(X_1, \dots, X_n)$ соответствующую ей БФ. Так как формула F выполнима, функция f принимает хотя бы один раз значение $\mathbf{1}$. Отсюда и из теоремы о представлении БФ вытекает, что $F \equiv \bigvee_{f(A_1, \dots, A_n)=\mathbf{1}} (X_1^{A_1} \wedge \dots \wedge X_n^{A_n})$. Ясно, что выписанная справа формула является СДНФ. Покажем единственность существования такой СДНФ для формулы F . Пусть G и H – две СДНФ от переменных X_1, \dots, X_n , причем $G \equiv H$. Тогда мы можем записать эти формулы в виде $G = \bigvee_{(A_1, \dots, A_n) \in T_G} (X_1^{A_1} \wedge \dots \wedge X_n^{A_n})$ и $H = \bigvee_{(A_1, \dots, A_n) \in T_H} (X_1^{A_1} \wedge \dots \wedge X_n^{A_n})$, где T_G и T_H – некоторые подмножества множества $\{\mathbf{0}, \mathbf{1}\}^n$. Из леммы 2 следует, что для любой интерпретации $\phi : X_i \mapsto S_i (i = 1, \dots, n)$ формулы G (соответственно формулы H) имеем $\phi(G) = \mathbf{1}$ (соответственно $\phi(H) = \mathbf{1}$) в том и только в том случае, если $(S_1, \dots, S_n) \in T_G$ (соответственно $(S_1, \dots, S_n) \in T_H$). Ввиду равносильности формул G и H получаем $T_G = T_H$, и потому $G = H$. Этим доказана единственность СДНФ

для F , а вместе с ней и теорема.

Существуют два способа приведения ФЛВ F к равносильной ей СДНФ. Первый из них содержится, по существу, в доказательстве теоремы и состоит в построении требуемой СДНФ *по таблице истинности* формулы F ; при этом используется формула (*) из теоремы о представлении БФ.

ПРИМЕР 1. Привести ФЛВ $F = (A \leftrightarrow B) \rightarrow C$ к СДНФ табличным способом.

Имеем:

A	B	C	$A \leftrightarrow B$	F
1	1	1	1	1
1	1	0	1	0
1	0	1	0	1
1	0	0	0	1
0	1	1	0	1
0	1	0	0	1
0	0	1	1	1
0	0	0	1	0

По таблице истинности находим, что $F \equiv (A^1 \wedge B^1 \wedge C^1) \vee (A^1 \wedge B^0 \wedge C^1) \vee (A^1 \wedge B^0 \wedge C^0) \vee (A^0 \wedge B^1 \wedge C^1) \vee (A^0 \wedge B^1 \wedge C^0) \vee (A^0 \wedge B^0 \wedge C^1) = (A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$.

Второй способ – способ приведения к СДНФ *равносильными преобразованиями*. Он состоит в следующем:

- 1) с помощью законов эквиваленции и импликации “избавляемся” в исходной ФЛВ F от логических связок \leftrightarrow и \rightarrow ;
- 2) применяя законы де Моргана, дистрибутивности и двойного отрицания, приводим формулу к ДНФ;
- 3) от ДНФ к СДНФ переходим, “добавляя” в каждую элементарную конъюнкцию X недостающие логические переменные: если в X не входит переменная A , то заменяем X на равносильную ей формулу $(X \wedge A) \vee (X \wedge \neg A)$; при необходимости с помощью закона идемпотентности добиваемся того, чтобы все элементарные конъюнкции в формуле были попарно различны.

ПРИМЕР 2. Привести равносильными преобразованиями к СДНФ формулу F из примера 1.

$$\begin{aligned}
F = (A \leftrightarrow B) \rightarrow C &\equiv^{12} (A \rightarrow B) \wedge (B \rightarrow A) \rightarrow C \equiv^7 \\
(\neg A \vee B) \wedge (\neg B \vee A) \rightarrow C &\equiv^7 \neg((\neg A \vee B) \wedge (\neg B \vee A)) \vee C \equiv^9 \\
(\neg\neg A \wedge \neg B) \vee (\neg\neg B \wedge \neg A) \vee C &\equiv^6 (A \wedge \neg B) \vee (B \wedge \neg A) \vee C \equiv (A \wedge \neg B \wedge \\
C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) &\vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge C) \vee (\neg A \wedge C) \equiv \\
(A \wedge \neg B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee &(\neg A \wedge B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge B \wedge \\
C) \vee (A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) &\vee (\neg A \wedge \neg B \wedge C) \equiv^4 (A \wedge \neg B \wedge C) \vee (A \wedge \\
\neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (\neg A &\wedge B \wedge \neg C) \vee (A \wedge B \wedge C) \vee (\neg A \wedge \neg B \wedge C).
\end{aligned}$$

Как видим, искомые СДНФ в примерах 1 и 2 совпадают с точностью до перестановки элементарных конъюнкций.

Из доказательства теоремы о СДНФ вытекает, что число интерпретаций ФЛВ F , при которых F истинна, равно числу элементарных конъюнкций в СДНФ, равносильной F . Отсюда получаем важное следствие.

СЛЕДСТВИЕ. ФЛВ F является тавтологией тогда и только тогда, когда равносильная ей СДНФ содержит в точности 2^n элементарных конъюнкций, где n — число логических переменных в F .

ПРИМЕР 3. Доказать, что формула $F = \neg B \vee \neg(A \rightarrow \neg B) \vee (\neg A \wedge B)$ — тавтология.

Равносильными преобразованиями приводим F к СДНФ:

$$\begin{aligned}
F = \neg B \vee \neg(A \rightarrow \neg B) \vee (\neg A \wedge B) &\equiv \neg B \vee \neg(\neg A \vee \neg B) \vee (\neg A \wedge B) \\
\equiv \neg B \vee (A \wedge B) \vee (\neg A \wedge B) &\equiv (A \wedge \neg B) \vee (\neg A \wedge \neg B) \vee (A \wedge B) \vee (\neg A \wedge B).
\end{aligned}$$

Применяя следствие, заключаем, что F — тавтология.

§ 1.7. Принцип двойственности. Конъюнктивные нормальные формы

Пусть ФЛВ F содержит лишь логические связи \neg , \wedge , \vee . Обозначим через F^* формулу, полученную из F заменой: \wedge на \vee , \vee на \wedge , A на $\neg A$, $\neg A$ на A (A — логическая переменная в F), **1** на **0** и **0** на **1**. Формула F^* называется двойственной к F . Например, для $F = \neg(A \wedge B \vee C) \wedge \mathbf{1} \vee \neg C$ имеем $F^* = (\neg((\neg A \vee \neg B) \wedge \neg C) \vee \mathbf{0}) \wedge C$. Справедливо следующее утверждение.

ПРЕДЛОЖЕНИЕ (принцип двойственности). Для любой ФЛВ F , содержащей лишь связи \neg , \wedge , \vee , выполнено $F^* \equiv \neg F$.

Доказательство. Проведем индукцию по длине формулы F . База индукции, т.е. когда F — логическая константа или переменная, очевидна. Предположим, что принцип двойственности имеет место

для всех формул, длина которых меньше, чем длина F , и покажем, что он верен и для формулы F . Разберем ряд случаев в зависимости от вида формулы F .

Случай 1. $F = \neg G$. Тогда $F^* = (\neg G)^* \equiv \neg(G^*) \equiv \neg(\neg G) = \neg F$.

Случай 2. $F = G \wedge H$. Тогда $F^* = G^* \vee H^* \equiv \neg G \vee \neg H \equiv \neg(G \wedge H) = \neg F$.

Случай 3. $F = G \vee H$. Тогда $F^* = G^* \wedge H^* \equiv \neg G \wedge \neg H \equiv \neg(G \vee H) = \neg F$. Предложение доказано.

СЛЕДСТВИЕ. Для любых ФЛВ F и G , содержащих лишь связки \neg , \wedge , \vee , выполнено $F \equiv G$ тогда и только тогда, когда $F^* \equiv G^*$.

Доказательство. Имеем $F \equiv G$ тогда и только тогда, когда $\neg F \equiv \neg G$, что ввиду $F^* \equiv \neg F$ и $G^* \equiv \neg G$ эквивалентно $F^* \equiv G^*$.

ФЛВ называется *конъюнктивной нормальной формой* (сокращенно КНФ), если она двойственна некоторой ДНФ. Аналогично определяются *совершенные конъюнктивные нормальные формы* (сокращенно СКНФ). Очевидно, ФЛВ F является СКНФ в том и только в том случае, если она имеет вид:

$$F = \bigwedge_{(A_1, \dots, A_n) \in T_F} (X_1^{A_1} \vee \dots \vee X_n^{A_n}),$$

где $T_F \subseteq \{\mathbf{1}, \mathbf{0}\}^n$. Выражение вида $X_1^{A_1} \vee \dots \vee X_n^{A_n}$ называется *элементарной дизъюнкцией*. Справедлив следующий аналог теоремы о СДНФ.

ТЕОРЕМА О СКНФ. *Всякая ФЛВ, не являющаяся тавтологией, равносильна некоторой СКНФ, причем последняя определяется однозначно с точностью до перестановки элементарных дизъюнкций и по набору переменных.*

Доказательство. Пусть ФЛВ F не является тавтологией. Тогда $\neg F$ – выполнимая формула, откуда по теореме о СДНФ $\neg F \equiv G$ для некоторой СДНФ G . Учитывая принцип двойственности, получаем $F \equiv \neg G \equiv G^*$, т.е. F равносильна СКНФ G^* . Докажем теперь единственность существования такой СКНФ для формулы F . В самом деле, пусть $F \equiv G_1$ и $F \equiv G_2$, где обе ФЛВ G_1 и G_2 суть СКНФ от того же набора логических переменных, что и F . Тогда $G_1 \equiv G_2$, и в силу следствия из принципа двойственности $G_1^* \equiv G_2^*$. Отсюда ввиду того, что обе формулы G_1^* и G_2^* являются СДНФ, имеем $G_1^* = G_2^*$, и потому $G_1 = G_2$. Теорема доказана.

Рассмотрим два способа приведения ФЛВ к СКНФ.

ПРИМЕР 1. Привести ФЛВ $F = (B \rightarrow \neg C) \wedge (A \wedge C \rightarrow B)$ к СКНФ табличным способом.

Выпишем таблицу истинности формулы F .

A	B	C	F
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	1

Каждой интерпретации $\phi: \begin{matrix} A & B & C \\ S_1 & S_2 & S_3 \end{matrix}$ формулы F , такой, что $\phi(F) = \mathbf{0}$, в искомой СКНФ соответствует элементарная дизъюнкция вида $A_{S_1} \vee B_{S_2} \vee C_{S_3}$, где

$$X_S = \begin{cases} \neg X & , \text{ если } S = \mathbf{1}, \\ X & , \text{ если } S = \mathbf{0} \end{cases}$$

(это легко понять из соображений двойственности, см. пример 1 из §1.6). Поэтому имеем

$$F \equiv (A_1 \vee B_1 \vee C_1) \wedge (A_1 \vee B_0 \vee C_1) \wedge (A_0 \vee B_1 \vee C_1) = \\ (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee \neg B \vee \neg C).$$

ПРИМЕР 2. Привести равносильными преобразованиями к СКНФ формулу F из примера 1.

$$F = (B \rightarrow \neg C) \wedge (A \wedge C \rightarrow B) \equiv (\neg B \vee \neg C) \wedge (\neg A \vee \neg C \vee B) \equiv \\ (\neg A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C).$$

Так как число интерпретаций ФЛВ, при которых она ложна, совпадает с числом элементарных дизъюнкций в равносильной ей СКНФ (см. пример 1), получаем

СЛЕДСТВИЕ. ФЛВ F является противоречием тогда и только тогда, когда равносильная ей СКНФ содержит в точности 2^n элементарных дизъюнкций, где n — число логических переменных в F .

ПРИМЕР 3. Доказать, что формула $F = A \wedge (A \rightarrow B) \wedge (A \rightarrow \neg B)$ — противоречие.

Равносильными преобразованиями приводим F к СКНФ:

$$F = A \wedge (A \rightarrow B) \wedge (A \rightarrow \neg B) \equiv A \wedge (\neg A \vee B) \wedge (\neg A \vee \neg B) \equiv (A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B) \wedge (\neg A \vee \neg B).$$

Применяя следствие, заключаем, что F – противоречие.

§ 1.8. Полные и замкнутые классы булевых функций. Теорема Поста

В этом параграфе логические переменные будем обозначать строчными латинскими буквами: $X = \{x_1, x_2, \dots\}$ – счетное множество. Каждую логическую переменную x_i рассматриваем как БФ, определенную равенством $f(x_i) = x_i$. Две БФ $f(x_{i_1}, x_{i_2}, \dots, x_{i_n})$ и $g(x_{j_1}, x_{j_2}, \dots, x_{j_m})$ мы считаем *равными*, если для любого отображения $\varphi : X \rightarrow \{0, 1\}$ справедливо $f(\varphi(x_{i_1}), \varphi(x_{i_2}), \dots, \varphi(x_{i_n})) = g(\varphi(x_{j_1}), \varphi(x_{j_2}), \dots, \varphi(x_{j_m}))$. Пусть для БФ $f(x_{i_1}, x_{i_2}, \dots, x_{i_n})$ имеет место $1 \leq i_1, \dots, i_n \leq N$. Определим БФ $g(x_1, x_2, \dots, x_N)$, полагая $g(a_1, a_2, \dots, a_N) = f(a_{i_1}, a_{i_2}, \dots, a_{i_n})$ для всех $a_1, a_2, \dots, a_N \in \{0, 1\}$. Очевидно, что $f(x_{i_1}, x_{i_2}, \dots, x_{i_n}) = g(x_1, x_2, \dots, x_N)$. Таким образом, некоторые переменные могут входить в БФ фиктивно. Заметим также, что две БФ от любого числа переменных, принимающие постоянное значение 0 (соответственно 1) при любом наборе значений логических переменных, равны. Таким образом, имеются две БФ-константы, которые можно считать имеющими любое конечное множество переменных.

Обозначим через \mathfrak{F} множество всех БФ. Пусть $f(x_1, \dots, x_n), g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m) \in \mathfrak{F}$. БФ $h(x_1, \dots, x_m)$ называется *суперпозицией* БФ f, g_1, \dots, g_n , если для любых $y_1, \dots, y_m \in \{0, 1\}$ имеет место равенство $h(y_1, \dots, y_m) = f(g_1(y_1, \dots, y_m), \dots, g_n(y_1, \dots, y_m))$. Будем записывать это следующим образом: $h = f(g_1, \dots, g_n)$. Отметим, что x_1, \dots, x_m включает в себя совокупность всех переменных, от которых фактически зависит по крайней мере одна из БФ g_1, \dots, g_n . Например, если $f(x_1, x_2) = x_1 \vee x_2$, $g_1(x_1, x_2, x_3) = x_1 \wedge x_2$, $g_2(x_1, x_2, x_3) = \neg x_3$, то $f(g_1, g_2) = x_1 \wedge x_2 \vee \neg x_3$.

Подмножества множества \mathfrak{F} будем называть *классами* БФ и обозначать готическими буквами. Класс \mathfrak{H} называется *замкнутым относительно суперпозиции*, если вместе с любыми БФ $f(x_1, \dots, x_n), g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m) \in \mathfrak{H}$ он содержит также и БФ $f(g_1, \dots, g_n)$.

Класс БФ, содержащий множество X всех логических переменных, называется *замкнутым*, если он замкнут относительно суперпозиции. Легко видеть, что пересечение любого непустого семейства замкнутых классов БФ также будет замкнутым классом. Очевидно, что класс всех БФ \mathfrak{F} является замкнутым. *Замыкание* $C(\mathfrak{H})$ произвольного класса БФ \mathfrak{H} мы определим как пересечение всех замкнутых классов БФ, содержащих \mathfrak{H} . Другими словами, $C(\mathfrak{H})$ есть наименьший по включению замкнутый класс БФ, содержащий \mathfrak{H} . Легко понять, что замыкание $C(\mathfrak{H})$ состоит в точности из тех БФ, которые получаются из БФ класса \mathfrak{H} и всех логических переменных последовательным применением операции суперпозиции. Очевидно также, что класс БФ замкнут тогда и только тогда, когда он совпадает со своим замыканием.

Класс БФ \mathfrak{H} называется *полным*, если $C(\mathfrak{H}) = \mathfrak{F}$. Цель этого параграфа — получение необходимых и достаточных условий полноты класса БФ (теорема Поста) и описание максимальных по включению собственных (т.е. отличных от \mathfrak{F}) замкнутых классов БФ.

Примерами полных классов БФ являются, в силу их определения, все полные системы логических связей. В частности, справедливо следующее утверждение.

ПРЕДЛОЖЕНИЕ. *Множество БФ, определяемых логическими связками $\{\vee, \wedge, \neg\}$, является полным классом.*

Как будет установлено ниже, максимальными собственными замкнутыми классами БФ будут следующие пять классов и только они. Проверка того, что каждый из этих классов содержит все логические переменные, предоставляется читателю.

1. Класс \mathfrak{T}_0 БФ, *сохраняющих 0*. Это означает, что $f(x_1, \dots, x_n) \in \mathfrak{T}_0$ тогда и только тогда, когда $f(\mathbf{0}, \dots, \mathbf{0}) = \mathbf{0}$. Очевидно, что класс \mathfrak{T}_0 является собственным замкнутым классом БФ.

2. Класс \mathfrak{T}_1 БФ, *сохраняющих 1*. Это означает, что $f(x_1, \dots, x_n) \in \mathfrak{T}_1$ тогда и только тогда, когда $f(\mathbf{1}, \dots, \mathbf{1}) = \mathbf{1}$. Очевидно, что класс \mathfrak{T}_1 является собственным замкнутым классом БФ.

3. Класс \mathfrak{S} *самодвойственных* БФ. БФ $f(x_1, \dots, x_n)$ называется *самодвойственной*, если $\forall x_1, \dots, x_n \in \{\mathbf{0}, \mathbf{1}\}$ имеет место равенство $f(\neg x_1, \dots, \neg x_n) = \neg f(x_1, \dots, x_n)$. Так как БФ, принимающая постоянное значение (константа), не является самодвойственной, класс \mathfrak{S} является собственным. Убедимся, что он является замкнутым. Пусть $f(x_1, \dots, x_n), g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m) \in \mathfrak{S}$ и

$h = f(g_1, \dots, g_n)$. Тогда $\forall x_1, \dots, x_m \in \{0, 1\}$ имеет место

$$\begin{aligned} h(\neg x_1, \dots, \neg x_m) &= f(g_1(\neg x_1, \dots, \neg x_m), \dots, g_n(\neg x_1, \dots, \neg x_m)) = \\ &= f(\neg g_1(x_1, \dots, x_m), \dots, \neg g_n(x_1, \dots, x_m)) = \\ &= \neg f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m)) = \neg h(x_1, \dots, x_m). \end{aligned}$$

Следовательно, $h \in \mathfrak{S}$ и класс самодвойственных БФ является замкнутым.

4. Класс \mathfrak{M} *монотонных* БФ. Для определения монотонной функции введем отношение частичного порядка \leq на множестве $\{0, 1\}^n$ следующим образом. Положим $0 < 1$. Пусть $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \{0, 1\}^n$. Тогда по определению $(a_1, \dots, a_n) < (b_1, \dots, b_n)$, если для всех $i = 1, \dots, n$ имеет место $a_i \leq b_i$ и существует натуральное число $k \leq n$ такое, что $a_k < b_k$. Как обычно, $(a_1, \dots, a_n) \leq (b_1, \dots, b_n)$ означает, что либо $(a_1, \dots, a_n) < (b_1, \dots, b_n)$, либо $(a_1, \dots, a_n) = (b_1, \dots, b_n)$.

БФ $f(x_1, \dots, x_n)$ называется *монотонной*, если для любых $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \{0, 1\}^n$ из $(a_1, \dots, a_n) \leq (b_1, \dots, b_n)$ следует $f(a_1, \dots, a_n) \leq f(b_1, \dots, b_n)$. Класс монотонных БФ является собственным, так как отрицание не является монотонной функцией. Легко понять, что суперпозиция монотонных функций будет монотонной функцией. Следовательно, класс \mathfrak{M} является собственным замкнутым классом БФ.

5. Класс \mathfrak{L} *линейных* БФ. Для определения этих функций требуется понятие *многочлена Жегалкина*. Определим на множестве $\{0, 1\}$ операцию \oplus сложения по модулю 2 следующим образом: положим по определению $0 \oplus 1 = 1 \oplus 0 = 1$, $0 \oplus 0 = 1 \oplus 1 = 0$. Для этой операции справедливы следующие свойства, легко проверяемые непосредственно:

$$\begin{aligned} x \oplus y &= y \oplus x; \\ (x \oplus y) \oplus z &= x \oplus (y \oplus z); \\ x \oplus 0 &= x; \\ x \oplus x &= 0; \\ x \wedge (y \oplus z) &= (x \wedge y) \oplus (x \wedge z); \\ x \oplus 1 &= \neg x. \end{aligned}$$

Многочлены Жегалкина можно определить аналогично ФЛВ (см. §1.1), используя логические константы, переменные и, вместо логических связок, операции \oplus, \wedge . При этом операцию \wedge называют *умножением* и обозначают точкой или опускают знак этой операции. Используя свойства операции \oplus , приведенные выше, и закон

идемпотентности для конъюнкции (умножения), легко проверить, что любой многочлен Жегалкина может быть записан либо как $\mathbf{0}$, либо в виде суммы одночленов: константы $\mathbf{1}$, некоторых логических переменных x_{i_1}, \dots, x_{i_m} и некоторых произведений вида $x_{i_1} \cdots x_{i_m}$, где $m \geq 2$ и логические переменные x_{i_1}, \dots, x_{i_m} различны. Эта запись аналогична записи обычного многочлена от нескольких переменных. Назовем ее *канонической записью* многочлена Жегалкина.

ТЕОРЕМА (о представлении БФ многочленом Жегалкина). *Любая БФ от n переменных однозначно представима многочленом Жегалкина в канонической записи от переменных x_1, \dots, x_n .*

Доказательство. Заметим сначала, что дизъюнкция $x \vee y$ может быть представлена многочленом Жегалкина: $x \vee y = \neg(\neg x \wedge \neg y) = \mathbf{1} \oplus (\mathbf{1} \oplus x)(\mathbf{1} \oplus y) = \mathbf{1} \oplus \mathbf{1} \oplus x \oplus y \oplus xy = x \oplus y \oplus xy$, т.е.

$$x \vee y = x \oplus y \oplus xy. \quad (1)$$

Применяя теорему о СДНФ, заключаем, что любая БФ от n переменных, не являющаяся константой $\mathbf{0}$, выражается многочленом Жегалкина, который получается из СДНФ заменой отрицания и дизъюнкции через сложение и умножение. Приводя полученный многочлен к канонической записи и принимая во внимание, что константа $\mathbf{0}$ — каноническая запись нулевого многочлена Жегалкина, получаем требуемое представление для БФ.

Для доказательства единственности достаточно подсчитать количество различных канонических записей многочленов Жегалкина от n переменных и убедиться, что оно равно 2^{2^n} — количеству всех булевых функций от n переменных. Количество одночленов вида $x_{i_1} \cdots x_{i_m}$ от n переменных равно биномиальному коэффициенту $C_n^m = \frac{n!}{m!(n-m)!}$. Таким образом, общее количество ненулевых одночленов равно $1 + \sum_{m=1}^n C_n^m = 2^n$. Поскольку каждый одночлен может встречаться или не встречаться в канонической записи многочлена Жегалкина от n переменных, общее число канонических записей равно числу всевозможных строк длины 2^n , составленных из нулей и единиц, т.е. равно 2^{2^n} .

БФ называется *линейной*, если в канонической записи ее многочлена Жегалкина отсутствуют произведения переменных, т.е. эта запись имеет вид $b \oplus x_{i_1} \oplus \dots \oplus x_{i_m}$, где $b \in \{\mathbf{0}, \mathbf{1}\}$. Очевидно, что линейные функции образуют собственный класс булевых функций. Легко проверить также, что суперпозиция линейных функций является линейной функцией. Для этого любую линейную функцию,

переменные которой находятся среди x_1, \dots, x_n , следует записать в виде $a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n \oplus b$, где $a_1, a_2, \dots, a_n, b \in \{0, 1\}$. Таким образом, \mathfrak{L} — собственный замкнутый класс БФ.

ТЕОРЕМА ПОСТА. *Произвольный класс БФ является полным тогда и только тогда, когда он содержит БФ, не сохраняющую $\mathbf{0}$, БФ, не сохраняющую $\mathbf{1}$, несамодвойственную БФ, немонопотонную БФ, нелинейную БФ.*

Доказательство этой теоремы опирается на ряд лемм. Напомним, что *константой* называется булева функция $g(x)$ такая, что $g(\mathbf{0}) = g(\mathbf{1})$.

ЛЕММА 1. *Если БФ f несамодвойственна, то класс $C(\{f, \neg\})$ содержит константу.*

Доказательство. Пусть БФ $f(x_1, \dots, x_n)$ несамодвойственна. По определению это означает, что существуют такие $a_i \in \{0, 1\}$ ($i = 1, \dots, n$), что $f(\neg a_1, \dots, \neg a_n) \neq \neg f(a_1, \dots, a_n)$. Поскольку $f(a_1, \dots, a_n) \in \{0, 1\}$, заключаем, что $f(\neg a_1, \dots, \neg a_n) = f(a_1, \dots, a_n)$. Рассмотрим БФ $g(x_1) = f(x_1^{a_1}, \dots, x_1^{a_n})$. Напомним, что $x_1^{a_i} = x_1$ при $a_i = 1$ и $x_1^{a_i} = \neg x_1$ при $a_i = 0$. Ясно, что $g(x_1) \in C(\{f, \neg\})$. Так как $\mathbf{0}^{a_i} = \neg a_i$ и $\mathbf{1}^{a_i} = a_i$, имеем $g(\mathbf{0}) = f(\mathbf{0}^{a_1}, \dots, \mathbf{0}^{a_n}) = f(\neg a_1, \dots, \neg a_n) = f(a_1, \dots, a_n) = f(\mathbf{1}^{a_1}, \dots, \mathbf{1}^{a_n}) = g(\mathbf{1})$. Таким образом, $g(\mathbf{0}) = g(\mathbf{1})$, т.е. $g(x_1)$ — константа, что и требовалось доказать.

ЛЕММА 2. *Если БФ f немонопотонна, то класс $C(\{f, \mathbf{0}, \mathbf{1}\})$ содержит отрицание.*

Доказательство. Пусть БФ $f(x_1, \dots, x_n)$ немонопотонна. По определению это означает, что существуют такие $a_i, b_i \in \{0, 1\}$ ($i = 1, \dots, n$), что $(a_1, \dots, a_n) < (b_1, \dots, b_n)$ и $f(a_1, \dots, a_n) > f(b_1, \dots, b_n)$. Следовательно, $f(a_1, \dots, a_n) = \mathbf{1}$ и $f(b_1, \dots, b_n) = \mathbf{0}$. Скажем, что вектор (c_1, \dots, c_n) *покрывается* вектором (d_1, \dots, d_n) , если $(c_1, \dots, c_n) < (d_1, \dots, d_n)$ и не существует вектора (e_1, \dots, e_n) со свойством $(c_1, \dots, c_n) < (e_1, \dots, e_n) < (d_1, \dots, d_n)$. Будем обозначать это следующим образом: $(c_1, \dots, c_n) \prec (d_1, \dots, d_n)$. Из определения частичного порядка \leq на множестве $\{0, 1\}^n$ следует, что $(c_1, \dots, c_n) \prec (d_1, \dots, d_n)$ тогда и только тогда, когда существует число m , $0 < m \leq n$ такое, что $c_i = d_i$ для всех $i \in \{1, \dots, n\} \setminus \{m\}$ и $c_m = \mathbf{0}$, $d_m = \mathbf{1}$. Легко понять, что если $(a_1, \dots, a_n) < (b_1, \dots, b_n)$, то от (a_1, \dots, a_n) до (b_1, \dots, b_n) существует цепочка векторов из

множества $\{\mathbf{0}, \mathbf{1}\}^n$, в которой каждый вектор покрывается последующим. Так как $f(a_1, \dots, a_n) = \mathbf{1}$ и $f(b_1, \dots, b_n) = \mathbf{0}$, для некоторых (c_1, \dots, c_n) , (d_1, \dots, d_n) имеет место $(a_1, \dots, a_n) \leq (c_1, \dots, c_n) \prec (d_1, \dots, d_n) \leq (b_1, \dots, b_n)$, причем $f(c_1, \dots, c_n) = \mathbf{1}$ и $f(d_1, \dots, d_n) = \mathbf{0}$. Пусть $c_m = \mathbf{0}$, $d_m = \mathbf{1}$ и $c_i = d_i$ для всех $i \in \{1, \dots, n\} \setminus \{m\}$. Положим $g(x) = f(c_1, \dots, c_{m-1}, x, c_{m+1}, \dots, c_n)$. Тогда $g(\mathbf{1}) = \mathbf{0}$ и $g(\mathbf{0}) = \mathbf{1}$, т.е. $g(x) = \neg x$. Ясно, что $g(x) \in C(\{f, \mathbf{0}, \mathbf{1}\})$. Это завершает доказательство леммы.

ЛЕММА 3. *Если БФ f нелинейна, то класс $C(\{f, \neg, \mathbf{0}, \mathbf{1}\})$ содержит конъюнкцию и дизъюнкцию.*

Доказательство. Пусть БФ $f(x_1, \dots, x_n)$ нелинейна, т.е. $f(x_1, \dots, x_n) = x_{i_1} \cdots x_{i_m} \oplus \dots$, где m — наибольшее натуральное число такое, что соответствующее произведение встречается в записи $f(x_1, \dots, x_n)$ в виде многочлена Жегалкина, причем $m \geq 2$. Подставим в многочлен, представляющий f , вместо переменных x_1, \dots, x_n переменные x_1, x_2 и константы так, что вместо x_{i_1} подставляется x_1 , вместо x_{i_2} — переменная x_2 , вместо x_{i_k} при $3 \leq k \leq m$ — константа $\mathbf{1}$ и вместо x_j при $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_m\}$ — константа $\mathbf{0}$. В результате получим функцию $g(x_1, x_2) = x_1 x_2 \oplus a x_1 \oplus b x_2 \oplus c$ из класса $C(\{f, \mathbf{0}, \mathbf{1}\})$. Рассмотрим возможные случаи для констант a, b, c . Так как $\wedge \in C(\{\neg, \vee\})$ и $\vee \in C(\{\neg, \wedge\})$, нам достаточно установить, что конъюнкция или дизъюнкция содержится в классе $C(\{g, \neg, \mathbf{0}, \mathbf{1}\})$.

Случай 1. $a = b = c = \mathbf{0}$. Тогда $g(x_1, x_2) = x_1 x_2 = x_1 \wedge x_2$, что и требуется.

Случай 2. $a = \mathbf{0}$, $b = \mathbf{1}$, $c = \mathbf{0}$. Тогда $g(x_1, x_2) = x_1 x_2 \oplus x_2 = (x_1 \oplus \mathbf{1})x_2 = (\neg x_1) \wedge x_2$ и $g(\neg x_1, x_2) = (\neg \neg x_1) \wedge x_2 = x_1 \wedge x_2$.

Случай 3. $a = \mathbf{1}$, $b = \mathbf{0}$, $c = \mathbf{0}$. Этот случай рассматривается аналогично предыдущему.

Случай 4. $a = \mathbf{0}$, $b = \mathbf{1}$, $c = \mathbf{1}$. Тогда $g(x_1, x_2) = x_1 x_2 \oplus x_2 \oplus \mathbf{1} = (x_1 \oplus \mathbf{1})x_2 \oplus \mathbf{1} = \neg(\neg x_1 \wedge x_2) = x_1 \vee \neg x_2$ и $g(x_1, \neg x_2) = x_1 \vee x_2$.

Случай 5. $a = \mathbf{1}$, $b = \mathbf{0}$, $c = \mathbf{1}$. Этот случай рассматривается аналогично предыдущему.

Случай 6. $a = b = \mathbf{1}$, $c = \mathbf{0}$. Тогда $g(x_1, x_2) = x_1 x_2 \oplus x_1 \oplus x_2 = x_1 \vee x_2$ в силу формулы (1).

Случай 7. $a = b = c = \mathbf{1}$. Тогда $g(x_1, x_2) = x_1 x_2 \oplus x_1 \oplus x_2 \oplus \mathbf{1} = (x_1 \oplus \mathbf{1})(x_2 \oplus \mathbf{1}) = (\neg x_1) \wedge (\neg x_2)$. Следовательно, $g(\neg x_1, \neg x_2) = x_1 \wedge x_2$.

Случай 8. $a = b = \mathbf{0}$, $c = \mathbf{1}$. Тогда $g(x_1, x_2) = x_1 x_2 \oplus \mathbf{1} = \neg(x_1 \wedge x_2) = \neg x_1 \vee \neg x_2$. Следовательно, $g(\neg x_1, \neg x_2) = x_1 \vee x_2$.

Доказательство леммы закончено.

Доказательство теоремы Поста.

Пусть \mathfrak{K} — полный класс БФ. Тогда ни одно из включений $\mathfrak{K} \subseteq \mathfrak{T}_i$ ($i = 0, 1$), $\mathfrak{K} \subseteq \mathfrak{S}$, $\mathfrak{K} \subseteq \mathfrak{M}$, $\mathfrak{K} \subseteq \mathfrak{L}$ невозможно, так как все классы \mathfrak{T}_i ($i = 0, 1$), \mathfrak{S} , \mathfrak{M} , \mathfrak{L} являются собственными замкнутыми. Следовательно, \mathfrak{K} должен содержать по функции, не принадлежащей каждому из указанных классов, что и требуется доказать.

Пусть теперь \mathfrak{K} — класс БФ, содержащий функции $f_i \notin \mathfrak{T}_i$, ($i = 0, 1$), $f_2 \notin \mathfrak{S}$, $f_3 \notin \mathfrak{M}$, $f_4 \notin \mathfrak{L}$. Докажем, что $\{\neg, \wedge, \vee\} \subset C(\mathfrak{K})$. Тогда полнота класса \mathfrak{K} будет следовать из предложения.

Положим $g(x) = f_0(x, \dots, x)$ и $h(x) = f_1(x, \dots, x)$. Тогда $g(\mathbf{0}) = \mathbf{1}$ и $h(\mathbf{1}) = \mathbf{0}$. Рассмотрим два возможных случая.

Случай 1. $g(\mathbf{1}) = \mathbf{0}$ или $h(\mathbf{0}) = \mathbf{1}$. Тогда $g(x) = \neg x$ или $h(x) = \neg x$, т.е. $\neg \in C(\mathfrak{K})$. Согласно лемме 1 класс $C(\{\neg, f_3\})$ содержит константу, поэтому $\{\mathbf{0}, \mathbf{1}\} \subset C(\mathfrak{K})$. В силу леммы 3 $\{\wedge, \vee\} \subset C(\{\neg, f_4, \mathbf{0}, \mathbf{1}\})$ и потому $\{\neg, \wedge, \vee\} \subset C(\mathfrak{K})$.

Случай 2. $g(\mathbf{1}) = \mathbf{1}$ и $h(\mathbf{0}) = \mathbf{0}$. Тогда g — константа $\mathbf{1}$, h — константа $\mathbf{0}$. Согласно лемме 2 имеем $\neg \in C(\{f_3, \mathbf{0}, \mathbf{1}\})$, а по лемме 3 $\{\wedge, \vee\} \subset C(\{\neg, f_4, \mathbf{0}, \mathbf{1}\})$. Следовательно, включение $\{\neg, \wedge, \vee\} \subset C(\mathfrak{K})$ выполнено и в этом случае.

Теорема Поста доказана.

СЛЕДСТВИЕ. Все максимальные замкнутые классы БФ исчерпываются классами \mathfrak{T}_i ($i = 0, 1$), \mathfrak{S} , \mathfrak{M} , \mathfrak{L} .



Доказательство. Нам достаточно установить, что произвольный собственный замкнутый класс БФ содержится в одном из классов \mathfrak{T}_i ($i = 0, 1$), \mathfrak{S} , \mathfrak{M} , \mathfrak{L} . Предположим, что \mathfrak{K} — замкнутый класс БФ, который не содержится ни в одном из пяти указанных классов. Тогда этот класс содержит БФ $f_i \notin \mathfrak{T}_i$ ($i = 0, 1$), $f_2 \notin \mathfrak{S}$, $f_3 \notin \mathfrak{M}$, $f_4 \notin \mathfrak{L}$. Следовательно, по теореме Поста класс \mathfrak{K} является полным. Так как \mathfrak{K} — замкнутый класс БФ, он совпадает с классом всех БФ, т.е. не является собственным. Следствие доказано.


ЗАМЕЧАНИЕ. Как мы отмечали в §1.5, операция, являющаяся стрелкой Пирса, образует полную систему логических связок и, следовательно, она определяет полный одноэлементный класс БФ. Этот факт не противоречит теореме Поста, поскольку легко проверить, что стрелка Пирса одновременно удовлетворяет всем требованиям этой теоремы: она не сохраняет $\mathbf{0}$ и $\mathbf{1}$, не самодвойственна, не монотонна и не линейна. Все это можно сказать и про штрих Шеффера.

§ 1.9. Приложение логики высказываний к анализу релейно-контактных схем

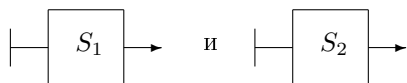
Впервые на возможность применения логики высказываний для описания действия технических устройств было обращено внимание в связи с рассмотрением электрических релейно-контактных схем. Остановимся на этом подробнее.

Контактом мы будем называть устройство, которое в процессе работы может находиться в двух состояниях: *замкнутом* или *разомкнутом*. Обозначать контакты будем (так же, как и логические переменные) большими латинскими буквами. Если два контакта находятся всегда в одинаковом состоянии, то мы их не различаем и обозначаем одной и той же буквой. Если контакт Y замкнут тогда и только тогда, когда контакт X разомкнут, то вместо Y пишем $\neg X$. Определим индукцией по числу вхождений контактов понятие *релейно-контактной схемы* (для простоты будем пользоваться также термином “*контактная схема*”):

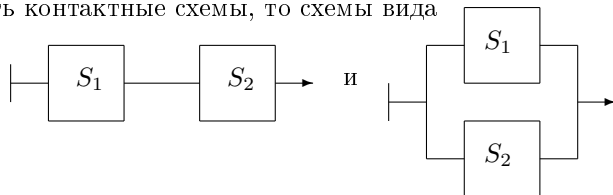
(0) схемы вида  и  являются контактными; первая из них всегда замкнута, вторая – разомкнута;

(1) для любого контакта Y схема  является контактной; она замкнута, если Y замкнут, и разомкнута в противном случае;

(2) если



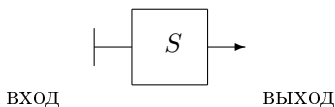
суть контактные схемы, то схемы вида



также являются контактными; при этом говорят, что первая из них получена *последовательным соединением* схем S_1 и S_2 (она обозначается $S_1 \wedge S_2$), а вторая – *параллельным соединением* схем S_1 и S_2

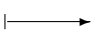

(она обозначается $S_1 \vee S_2$); схема $S_1 \wedge S_2$, по определению, замкнута, если замкнуты обе схемы S_1, S_2 , а схема $S_1 \vee S_2$ замкнута, если замкнута хотя бы одна из схем S_1, S_2 .

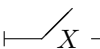
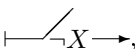
(3) любая контактная схема S получается одним из указанных способов (0), (1), (2); она имеет вход и выход:



Из определения вытекает, что схема S может находиться в одном из двух состояний – замкнутом или разомкнутом, зависящем от состояний ее контактов в данный момент. Из соображений чисто технического характера ясно, что релейно-контактная схема замкнута тогда и только тогда, когда она проводит электрический ток.

По каждой контактной схеме S можно построить ФЛВ F_S следующим образом:

(0) если S имеет вид  или , то соответственно $F_S = \mathbf{1}$ или $F_S = \mathbf{0}$;

(1) если S имеет вид  или , то соответственно $F_S = X$ или $F_S = \neg X$;

(2) если $S = S_1 \wedge S_2$ или $S = S_1 \vee S_2$, то соответственно $F_S = F_{S_1} \wedge F_{S_2}$ или $F_S = F_{S_1} \vee F_{S_2}$.

Например, схеме S , изображенной на рис.1, соответствует формула $F_S = (X \wedge (Z \vee \neg Y)) \vee (\neg X \wedge Z) \vee ((X \vee \neg Y) \wedge \neg Z)$. Обратно, если F – ФЛВ такая, что в нее входят только логические связки \neg, \wedge, \vee , причем связка \neg используется только в паре с логической переменной, то по формуле F легко восстановить контактную схему S , для которой $F_S = F$.

Для произвольной контактной схемы S между множеством состояний ее контактов и множеством интерпретаций формулы F_S естественным способом устанавливается взаимно однозначное соответствие, при котором переменной X в F_S присваивается значение $\mathbf{1}$ или $\mathbf{0}$ в зависимости от того, замкнут контакт X в схеме S или нет.

Из определения схемы S и алгоритма построения по ней ФЛВ F_S непосредственно вытекает важное предложение 1.

ПРЕДЛОЖЕНИЕ 1. Контактная схема S замкнута тогда и только тогда, когда формула F_S истинна при интерпретации, соответствующей данному состоянию контактов в S .

Две контактные схемы называются *эквивалентными*, если при одинаковых состояниях контактов они одновременно либо замкнуты, либо разомкнуты. Имеет место следующее утверждение.

ПРЕДЛОЖЕНИЕ 2. Контактные схемы S_1 и S_2 эквивалентны в том и только в том случае, если соответствующие им ФЛВ F_{S_1} и F_{S_2} равносильны.

Действительно, ввиду предложения 1 схема S_i ($i = 1, 2$) замкнута тогда и только тогда, когда формула F_{S_i} истинна при надлежащей интерпретации. Это означает, что схемы S_1 и S_2 эквивалентны тогда и только тогда, когда истинностные значения формул F_{S_1} и F_{S_2} совпадают при одинаковых интерпретациях, т.е. F_{S_1} и F_{S_2} равносильны.

Задача упрощения контактной схемы S заключается в построении схемы S' , эквивалентной S , и содержащей возможно меньшее число контактов. Предложение 2 позволяет свести ее к задаче упрощения ФЛВ F_S .

ПРИМЕР 1. Упростить контактную схему, изображенную на рис.1.

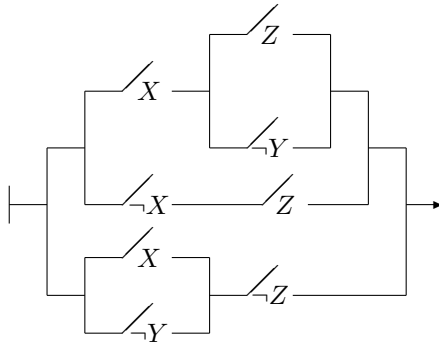


Рис.1

Имеем $F_S = (X \wedge (Z \vee \neg Y)) \vee (\neg X \wedge Z) \vee ((X \vee \neg Y) \wedge \neg Z) \equiv (X \wedge Z) \vee (X \wedge \neg Y) \vee (\neg X \wedge Z) \vee ((X \vee \neg Y) \wedge \neg Z) \equiv Z \vee (X \wedge \neg Y) \vee ((X \vee \neg Y) \wedge \neg Z) \equiv ((Z \vee X \vee \neg Y) \wedge (Z \vee \neg Z) \vee (X \wedge \neg Y)) \equiv Z \vee X \vee \neg Y \vee (X \wedge \neg Y) \equiv Z \vee X \vee \neg Y$.

Искомая схема, представляющая собой параллельное соединение трех контактов, изображена на рис.2.

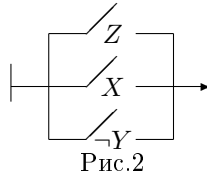


Рис.2

Предложение 1 позволяет также *строить контактные схемы по заданным условиям*.

ПРИМЕР 2. Построить схему, проводящую ток тогда и только тогда, когда большинство из трех ее контактов X , Y , Z замкнуто.

Учитывая предложение 1, сначала выпишем ФЛВ F , принимающую значение **1** тогда и только тогда, когда большинство из ее переменных X , Y , Z истинно (ср. с примером из §1.5):

$$F = (X \wedge Y \wedge Z) \vee (X \wedge Y \wedge \neg Z) \vee (X \wedge \neg Y \wedge Z) \vee (\neg X \wedge Y \wedge Z).$$

Приведем F к равносильной ей ФЛВ с меньшим числом вхождений переменных:

$$F = X \wedge Y \wedge (Z \vee \neg Z) \vee ((X \wedge \neg Y) \vee (\neg X \wedge Y)) \wedge Z \equiv \\ X \wedge Y \vee ((X \wedge \neg Y) \vee (\neg X \wedge Y)) \wedge Z.$$

Соответствующая этой формуле контактная схема изображена на рис.3.

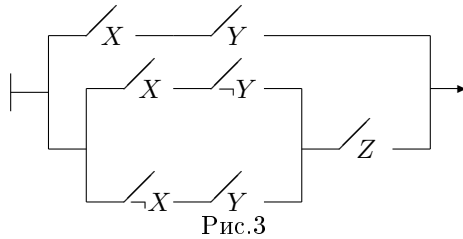


Рис.3

Глава 2

Логика предикатов

§ 2.1. Предикаты

Рассматривая различные высказывания, мы интересовались в основном их истинностными значениями. При этом о структуре каждого более или менее сложного высказывания требовалось знать не так уж и много, а именно, как это высказывание получается из некоторых простых (неделимых) высказываний с помощью известных логических связок. Структура простого высказывания нас уже не интересовала; в частности, мы не выделяли в нем подлежащее и сказуемое. Логика предикатов, в отличие от логики высказываний, позволяет проводить как раз более тонкий анализ простого высказывания. Само слово “предикат” в переводе с латинского языка означает “сказуемое”, т.е. группу слов, характеризующих подлежащее.

Выпишем предложения: “2 – простое число”, “3 – простое число”, “4 – простое число”. Все они являются высказываниями, причем первые два из них истинны, а последнее ложно. Рассмотрим предложение $P(x) = “x – простое число”$, где x пробегает множество \mathbf{N} натуральных чисел. Очевидно, $P(x)$ высказыванием уже не является, но становится таковым при подстановке вместо переменной x любого натурального числа. В этом случае говорим, что на множестве \mathbf{N} задан *одноместный предикат* $P(x)$ “быть простым числом”. На \mathbf{N} можно определить и другие одноместные предикаты: “ x меньше 10”, “ x – четное число”, “ x больше 2015 и делится на 13”.

Предложение $Q(x, y) = “x$ меньше $y”$, где x и y также принима-

ют значения в множестве \mathbf{N} , дает уже пример *двухместного предиката*, определенного на \mathbf{N} . Если вместо переменных x, y подставлять в $Q(x, y)$ различные натуральные числа, то будут получаться соответствующие высказывания, например, “3 меньше 5” или “5 меньше 3”. К двухместным предикатам, заданным на множестве \mathbf{N} , относятся и такие предложения: “ x делится на y ”, “ $x + y = 10$ ”, “НОД(x, y) = 5”, “ $x < y$ или y делится на 3”. Приведенных примеров достаточно, чтобы дать следующее общее определение:

n -местным предикатом, заданным на множестве M , называется предложение, содержащее n переменных и обращающееся в высказывание при подстановке вместо этих переменных элементов множества M . Пусть теперь $P(x_1, \dots, x_n)$ – произвольный n -местный предикат от переменных x_1, \dots, x_n , заданный на M . Множество M принято называть *предметной областью* предиката P , а переменные x_1, \dots, x_n , принимающие свои значения в M , – его *предметными переменными*. Число n предметных переменных называется *арностью* или *местностью* предиката. В связи с этим наряду с термином “ n -местный предикат” мы часто будем пользоваться и термином “ *n -арный предикат*”. Арность n предиката P может принимать значения $n = 0, 1, 2, \dots$. Если P – нульместный предикат (т.е. $n = 0$), то, очевидно, P является некоторым высказыванием об элементах множества M . Обратное, *на всякое высказывание мы можем смотреть как на нульместный предикат*. Исходя из этого, логика высказываний в ее содержательном смысле должна восприниматься как часть (причем наиболее простая) логики предикатов.

С каждым n -местным предикатом $P(x_1, \dots, x_n)$, заданным на множестве M , ассоциируется вполне определенная n -местная функция, которая любому кортежу $(a_1, \dots, a_n) \in M^n$ ставит в соответствие константу $\mathbf{1}$ или $\mathbf{0}$ в зависимости от того, истинно или ложно высказывание $P(a_1, \dots, a_n)$. Для простоты эту функцию, так же как и предикат, будем обозначать $P(x_1, \dots, x_n)$. Рассмотренный выше предикат $P(x) = “x$ – простое число” определяет функцию $P : N \rightarrow \{0, 1\}$ такую, что, например, $P(2) = \mathbf{1}$, а $P(4) = \mathbf{0}$. Аналогично, заданный на множестве \mathbf{N} натуральных чисел предикат $Q(x, y) = “x$ меньше $y”$ определяет функцию $Q : N^2 \rightarrow \{0, 1\}$ такую, что $Q(3, 5) = \mathbf{1}$, а $Q(5, 3) = \mathbf{0}$. Таким образом, мы приходим ко второму определению понятия предиката:

n -местным (n -арным) предикатом, заданным на множестве M , называется отображение n -й декартовой степени множества M

в множество логических констант.

Данное определение предиката $P(x_1, \dots, x_n)$ как функции $P : M^n \rightarrow \{0, 1\}$ мы будем считать основным, поскольку, будучи формальным, оно является более строгим, нежели первое определение. В этом случае нульместный предикат – это просто 0 или 1 .

ПРИМЕР 1. Пусть V – множество прямых в трехмерном пространстве. Определим двухместный предикат $P : V^2 \rightarrow \{0, 1\}$ следующим образом:

$$P(\pi_1, \pi_2) = \begin{cases} 1, & \text{если } \pi_1 \parallel \pi_2, \\ 0, & \text{если } \pi_1 \not\parallel \pi_2. \end{cases}$$

ПРИМЕР 2. Пусть R – множество действительных чисел. Определим трехместный предикат $S : R^3 \rightarrow \{0, 1\}$ следующим образом:

$$S(\alpha, \beta, \gamma) = \begin{cases} 1, & \text{если } \alpha + \beta = \gamma, \\ 0, & \text{если } \alpha + \beta \neq \gamma. \end{cases}$$

Предикат $P : M^n \rightarrow \{0, 1\}$ называется *тождественно истинным* (тождественно ложным) на множестве M , если для любой n -и $(a_1, \dots, a_n) \in M^n$ выполнено $P(a_1, \dots, a_n) = 1$ (соответственно $P(a_1, \dots, a_n) = 0$). Рассмотрим в M^n подмножество $T_P = \{(a_1, \dots, a_n) \in M^n \mid P(a_1, \dots, a_n) = 1\}$. Множество T_P называется *областью истинности* предиката P . Ясно, что каждый предикат P однозначно определяется своей областью истинности T_P , причем $T_P = M^n$ ($T_P = \emptyset$) тогда и только тогда, когда P – тождественно истинный (соответственно тождественно ложный) предикат.

Подмножества из M^n обычно называют n -местными отношениями на M . Отображение $f : P \rightarrow T_P$ устанавливает *взаимно однозначное соответствие между множеством n -местных предикатов и множеством n -местных отношений, заданных на M* . Последнее вытекает из того, что для любого отношения $U \subseteq M^n$ существует предикат $P : M^n \rightarrow \{0, 1\}$ такой, что $T_P = U$ и, следовательно, $f(P) = U$; этот предикат P определяется по U очевидным образом: $P(a_1, \dots, a_n) = 1$ тогда и только тогда, когда $(a_1, \dots, a_n) \in U$. Более глубокая связь между предикатами и отношениями на множествах устанавливается ниже в связи с рассмотрением на предикатах логических операций.

Пусть $P(x_1, \dots, x_r, y_1, \dots, y_{n-r})$ и $Q(x_1, \dots, x_r, z_1, \dots, z_{m-r})$ – предикаты арности n и m соответственно, заданные на множестве M ; здесь x_1, \dots, x_r – общие предметные переменные, участвующие в записи этих предикатов. Тогда предикат $\neg P(x_1, \dots, x_r, y_1, \dots, y_{n-r})$ арности n и предикаты $P \wedge Q$, $P \vee Q$, $P \longrightarrow Q$, $P \longleftrightarrow Q$ арности $n + m - r$ от переменных $x_1, \dots, x_r, y_1, \dots, y_{n-r}, z_1, \dots, z_{m-r}$ определяются следующим естественным способом:

- (1) $\neg P(a_1, \dots, a_r, b_1, \dots, b_{n-r}) = \mathbf{1} \iff P(a_1, \dots, a_r, b_1, \dots, b_{n-r}) = \mathbf{0}$;
- (2) $P \wedge Q(a_1, \dots, a_r, b_1, \dots, b_{n-r}, c_1, \dots, c_{m-r}) = \mathbf{1} \iff P(a_1, \dots, a_r, b_1, \dots, b_{n-r}) = \mathbf{1}$ и $Q(a_1, \dots, a_r, c_1, \dots, c_{m-r}) = \mathbf{1}$;
- (3) $P \vee Q(a_1, \dots, a_r, b_1, \dots, b_{n-r}, c_1, \dots, c_{m-r}) = \mathbf{1} \iff P(a_1, \dots, a_r, b_1, \dots, b_{n-r}) = \mathbf{1}$ или $Q(a_1, \dots, a_r, c_1, \dots, c_{m-r}) = \mathbf{1}$;
- (4) $P \longrightarrow Q(a_1, \dots, a_r, b_1, \dots, b_{n-r}, c_1, \dots, c_{m-r}) = \mathbf{1} \iff P(a_1, \dots, a_r, b_1, \dots, b_{n-r}) = \mathbf{0}$ или $Q(a_1, \dots, a_r, c_1, \dots, c_{m-r}) = \mathbf{1}$;
- (5) $P \longleftrightarrow Q(a_1, \dots, a_r, b_1, \dots, b_{n-r}, c_1, \dots, c_{m-r}) = \mathbf{1} \iff P(a_1, \dots, a_r, b_1, \dots, b_{n-r}) = Q(a_1, \dots, a_r, c_1, \dots, c_{m-r})$; здесь a_i, b_j, c_k ($1 \leq i \leq r, 1 \leq j \leq n - r, 1 \leq k \leq m - r$) – произвольные элементы из M .

Таким образом, в предикатах $\neg P, P \wedge Q, P \vee Q, P \longrightarrow Q, P \longleftrightarrow Q$ роль логических связок полностью адекватна той роли, которую они играли в логике высказываний. Между логическими операциями на предикатах и теоретико-множественными операциями на отношениях существует тесная связь, а именно, справедливо следующее утверждение.

ПРЕДЛОЖЕНИЕ. Если P и Q – предикаты арности n от одного и того же набора предметных переменных, заданные на множестве M , то

- (1) $T_{\neg P} = \bar{T}_P$, где $\bar{T}_P = M^n \setminus T_P$;
- (2) $T_{P \wedge Q} = T_P \cap T_Q$;
- (3) $T_{P \vee Q} = T_P \cup T_Q$;
- (4) $T_{P \longrightarrow Q} = \bar{T}_P \cup T_Q$;
- (5) $T_{P \longleftrightarrow Q} = (\bar{T}_P \cup T_Q) \cap (\bar{T}_Q \cup T_P)$.

Доказательство. (1) Для любой n -и $(a_1, \dots, a_n) \in M^n$ имеем $(a_1, \dots, a_n) \in T_{\neg P} \iff \neg P(a_1, \dots, a_n) = \mathbf{1} \iff P(a_1, \dots, a_n) = \mathbf{0} \iff (a_1, \dots, a_n) \in M^n \setminus T_P = \bar{T}_P$.

(2) Для любой n -и $(a_1, \dots, a_n) \in M^n$ имеем $(a_1, \dots, a_n) \in T_{P \wedge Q} \iff P \wedge Q(a_1, \dots, a_n) = \mathbf{1} \iff P(a_1, \dots, a_n) = \mathbf{1}$ и $Q(a_1, \dots, a_n) = \mathbf{1}$

$$\iff (a_1, \dots, a_n) \in T_P \text{ и } (a_1, \dots, a_n) \in T_Q \iff (a_1, \dots, a_n) \in T_P \cap T_Q.$$

Равенство (3) проверяется аналогично.

(4) Очевидно, предикаты $P \rightarrow Q$ и $\neg P \vee Q$ совпадают как функции, отображающие M^n в $\{\mathbf{0}, \mathbf{1}\}$. Поэтому равны их области истинности, откуда $T_{P \rightarrow Q} = T_{\neg P \vee Q} = T_{\neg P} \cup T_Q = \overline{T_P} \cup T_Q$ ввиду (1) и (3).

Равенство (5) вытекает из (2) и (4). При этом надо лишь заметить, что предикат $P \iff Q$ совпадает с предикатом $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

Учитывая доказанное предложение, *под n -арным предикатом P иногда понимают не функцию $M^n \rightarrow \{\mathbf{0}, \mathbf{1}\}$, а n -местное отношение на множестве M , соответствующее области истинности T_P* . В этом случае логические операции отрицания \neg , конъюнкции \wedge и дизъюнкции \vee удобно интерпретируются теоретико-множественными операциями дополнения $\bar{}$, пересечения \cap и объединения \cup .

При решении задач на нахождение области истинности предикатов, заданных на множестве \mathbf{R} действительных чисел и имеющих арности $n = 2$ или $n = 3$, удобно для наглядности использовать геометрический подход. Если предикат P есть функция из \mathbf{R}^2 в $\{\mathbf{0}, \mathbf{1}\}$, то его область истинности T_P является множеством упорядоченных пар действительных чисел, и потому может интерпретироваться как некоторое множество точек координатной плоскости, которые предикат P отображает в $\mathbf{1}$. Если же P есть функция из \mathbf{R}^3 в $\{\mathbf{0}, \mathbf{1}\}$, то на T_P удобно смотреть как на соответствующее геометрическое место точек трехмерного координатного пространства.

ПРИМЕР 3. Построить область истинности T_P предиката $P(x, y)$, определенного на \mathbf{R} следующим образом: $P(x, y) = \mathbf{1} \iff x^2 + y^2 > 2x$.

T_P есть геометрическое место точек на координатной плоскости ОХУ, задаваемое неравенством $x^2 + y^2 > 2x$. Преобразовывая последнее к неравенству $(x - 1)^2 + y^2 > 1$, получаем, что T_P состоит из точек плоскости, расположенных вне круга единичного радиуса с центром в точке $(1, 0)$ (см. рис.4).

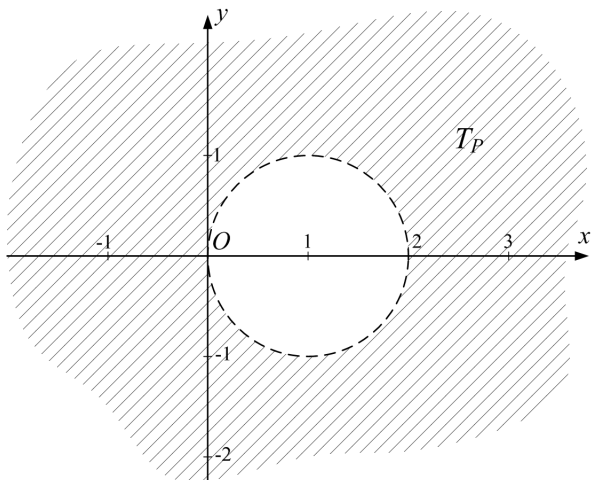


Рис.4

§ 2.2. Кванторы и их геометрическая интерпретация

Когда говорят, что логика предикатов имеет больший запас средств, позволяющих исследовать внутреннюю структуру высказывания, нежели логика высказываний, то обычно подразумевают под этим наличие в логике предикатов большего числа операций, с помощью которых можно строить различные высказывания и предикаты. К известным уже операциям – логическим связкам – добавляются две принципиально новые – *квантор общности* $\forall x$ (читается “для любого x ”) и *квантор существования* $\exists x$ (читается “для некоторого x ” или “существует x такой, что”, здесь x – предметная переменная). Дадим их определение.

Квантором общности (существования) называется функция, сопоставляющая каждому n -местному предикату $P(x_1, x_2, \dots, x_n)$ на множестве M , где $n \geq 1$, $(n - 1)$ -местный предикат $Q(x_2, \dots, x_n) = \forall x_1 P(x_1, x_2, \dots, x_n)$ (соответственно обозначаемый $\exists x_1 P(x_1, x_2, \dots, x_n)$) на этом же множестве, такой, что $Q(a_2, \dots, a_n) = 1$ для $a_2, \dots, a_n \in M$ в том и только в том случае, если для любого (соответственно для некоторого) $a_1 \in M$ выполнено $P(a_1, a_2, \dots, a_n) = 1$.

Из данного определения следует, в частности, что если $P(x)$ – одноместный предикат, то предикаты $\forall xP(x)$ и $\exists xP(x)$ нульместны, т.е. являются высказываниями об элементах множества M .

ПРИМЕР 1. Рассмотрим на множестве \mathbf{R} действительных чисел двухместный предикат $P : P(x, y) = \mathbf{1} \iff x^2 + y > 10$, и положим $Q(y) = \forall xP(x, y)$ и $S(y) = \exists xP(x, y)$. Тогда по определению $Q(y)$ и $S(y)$ – одноместные предикаты, причем $Q(b) = \mathbf{1} \iff$ для любого $a \in \mathbf{R} : a^2 + b > 10$, а $S(b) = \mathbf{1} \iff$ для некоторого $a \in \mathbf{R} : a^2 + b > 10$. Поэтому, очевидно, $Q(b) = \mathbf{1} \iff b > 10$, т.е. $T_Q =]10, +\infty[$, а $S(b) = \mathbf{1}$ при любом $b \in \mathbf{R}$, т.е. $T_S =]-\infty, +\infty[$.

ПРИМЕР 2. Рассмотрим одноместный предикат P на множестве \mathbf{N} натуральных чисел: $P(x) = \mathbf{1} \iff x$ – простое число. Тогда предикату $\forall xP(x)$ соответствует ложное высказывание “всякое натуральное число является простым”, а предикату $\exists xP(x)$ – истинное высказывание “существует простое натуральное число”.

ПРИМЕР 3. На множестве $M = \{a, b, c\}$ заданы предикаты P и Q :

$P(x, y):$	<table style="border-collapse: collapse; text-align: center;"> <tr> <td style="border: 1px solid black; padding: 2px 5px;">$x \backslash y$</td> <td style="border: 1px solid black; padding: 2px 5px;">a</td> <td style="border: 1px solid black; padding: 2px 5px;">b</td> <td style="border: 1px solid black; padding: 2px 5px;">c</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px 5px;">a</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px 5px;">b</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px 5px;">c</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> </tr> </table>	$x \backslash y$	a	b	c	a	0	1	0	b	0	1	0	c	1	1	0
$x \backslash y$	a	b	c														
a	0	1	0														
b	0	1	0														
c	1	1	0														

$Q(x, y):$	<table style="border-collapse: collapse; text-align: center;"> <tr> <td style="border: 1px solid black; padding: 2px 5px;">$x \backslash y$</td> <td style="border: 1px solid black; padding: 2px 5px;">a</td> <td style="border: 1px solid black; padding: 2px 5px;">b</td> <td style="border: 1px solid black; padding: 2px 5px;">c</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px 5px;">a</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px 5px;">b</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px 5px;">c</td> <td style="border: 1px solid black; padding: 2px 5px;">1</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> <td style="border: 1px solid black; padding: 2px 5px;">0</td> </tr> </table>	$x \backslash y$	a	b	c	a	1	0	1	b	1	0	0	c	1	0	0
$x \backslash y$	a	b	c														
a	1	0	1														
b	1	0	0														
c	1	0	0														

Найти область истинности предиката

$$S(y) = \forall x(P(x, y) \vee Q(x, y)).$$

Из определения P и Q следует, что $T_P = \{(a, b), (b, b), (c, a), (c, b)\}$ и $T_Q = \{(a, a), (a, c), (b, a), (c, a)\}$. Поэтому область истинности T_K предиката $K(x, y) = P(x, y) \vee Q(x, y)$ совпадает с множеством пар $T_P \cup T_Q = \{(a, a), (a, b), (a, c), (b, a), (b, b), (c, a), (c, b)\}$. Отсюда получаем: $y \in T_S = T_{\forall xK(x, y)} \iff S(y) = \mathbf{1} \iff$ для любого $x \in M : K(x, y) = \mathbf{1} \iff$ для любого $x \in M : (x, y) \in T_K$, а это, очевидно, истинно при $y = a$ или $y = b$ и ложно при $y = c$, т.е. $T_S = \{a, b\}$.

Если $P(x, y)$ – предикат арности два, заданный на множестве \mathbf{R} , то, как отмечалось в предыдущем параграфе, мы можем наглядно изобразить его область истинности T_P на координатной плоскости.

Поставим следующий вопрос: как, зная T_P , построить области истинности предикатов $\forall xP(x, y)$ и $\exists xP(x, y)$?

Пусть область истинности предиката P представлена на рис.5. Одноместный предикат $Q(y) = \forall xP(x, y)$ есть функция $Q : \mathbf{R} \rightarrow \{\mathbf{0}, \mathbf{1}\}$, при этом на \mathbf{R} удобно смотреть как на координатную ось OY и считать, что $y \in OY$. По определению, имеем: $a \in T_Q \iff Q(a) = \mathbf{1} \iff$ для любого $b \in \mathbf{R} : P(b, a) = \mathbf{1} \iff$ для любого $b \in \mathbf{R} : (b, a) \in T_P \iff l_a \subseteq T_P$, где l_a – прямая, проходящая через точку a на оси OY параллельно оси OX . Таким образом, $T_{\forall xP(x, y)}$ геометрически интерпретируется как множество точек a на оси OY , для которых прямые l_a , определяемые уравнениями $y = a$, целиком лежат в области истинности T_P .

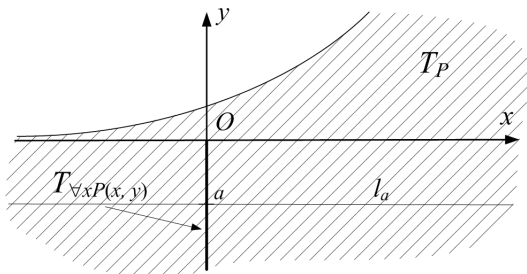


Рис.5

Рассмотрим теперь для предиката $P(x, y)$, область истинности которого изображена на рис.6, предикат $S(y) = \exists xP(x, y)$. $S(y)$ как функция отображает множество \mathbf{R} в $\{\mathbf{0}, \mathbf{1}\}$. отождествим, как и выше, \mathbf{R} с множеством точек оси OY , а T_S – с некоторым его подмножеством. Тогда имеем: $a \in T_S \iff S(a) = \mathbf{1} \iff$ для некоторого $b \in \mathbf{R} : P(b, a) = \mathbf{1} \iff$ для некоторого $b \in \mathbf{R} : (b, a) \in T_P \iff$ точка a принадлежит проекции T_P на ось OY . Таким образом, $T_{\exists xP(x, y)}$ геометрически интерпретируется как проекция области истинности T_P на ось OY .

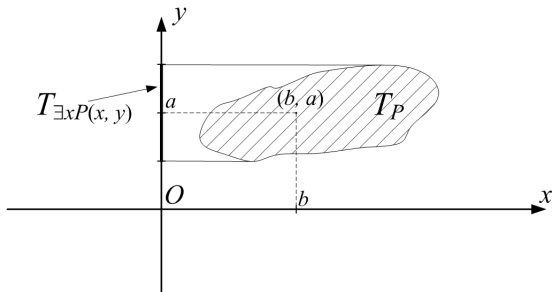


Рис.6

Проведенные рассуждения легко обобщаются на случай трехместного предиката $P(x, y, z)$, действующего как функция $P : \mathbf{R}^3 \rightarrow \{0, 1\}$. В этом случае $T_{\forall x P(x, y, z)}$ состоит из всех таких точек плоскости OYZ , что прямые, проходящие через них параллельно оси OX , целиком расположены в области истинности T_P , а $T_{\exists x P(x, y, z)}$ интерпретируется как проекция T_P на плоскость OYZ .

ПРИМЕР 4. На множестве \mathbf{R} заданы двухместные предикаты P и Q : $P(x, y) = 1 \iff x^2 + y^2 = 4$, $Q(x, y) = 1 \iff x + y > 2$. Найти область истинности предиката $S(y) = \exists x(P(x, y) \wedge Q(x, y))$.

Обозначим через $K(x, y)$ предикат $P(x, y) \wedge Q(x, y)$. Тогда $T_K = T_{P \wedge Q} = T_P \cap T_Q$. Построим области истинности T_P и T_Q и найдем T_K как их пересечение (см. рис. 7).

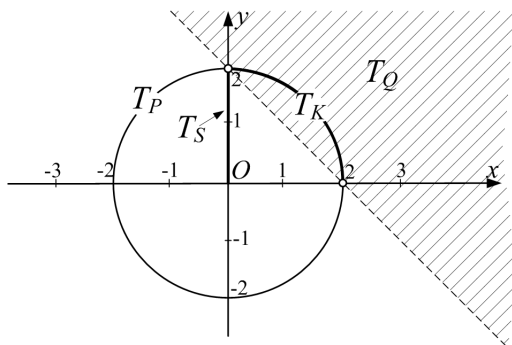


Рис.7

Область истинности T_K геометрически представляет собой дугу окружности радиуса два с центром в начале координат, лежащую в первой четверти. Взяв теперь проекцию T_K на ось OY , получим область истинности T_S предиката $S = \exists x K(x, y) = \exists x (P(x, y) \wedge Q(x, y))$. На рис.4 хорошо видно, что $T_S =]0, 2[$, т.е. $S(y) = \mathbf{1} \iff 0 < y < 2$.

ПРИМЕР 5. Определить, верно или нет следующее утверждение о действительных числах: “существует такое число $z \in \mathbf{R}$, что для любого числа $x \in \mathbf{R}$ найдется число $y \in \mathbf{R}$, для которого выполнялось бы неравенство: $x^2 + y^2 \leq z$ ”.

Обозначим через $P(x, y, z)$ трехместный предикат, заданный на множестве \mathbf{R} действительных чисел следующим образом: $P(x, y, z) = \mathbf{1} \iff x^2 + y^2 \leq z$. Требуется определить истинностное значение высказывания (или, что то же самое, нульместного предиката) $\exists z \forall x \exists y P(x, y, z)$. С этой целью заметим вначале, что области истинности предиката $P(x, y, z)$ соответствует в трехмерном координатном пространстве $OXYZ$ тело, ограниченное поверхностью, задаваемой уравнением $x^2 + y^2 = z$ и являющейся, как хорошо известно, параболоидом вращения (см. рис.8).

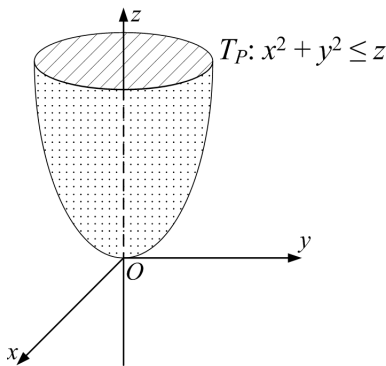


Рис.8

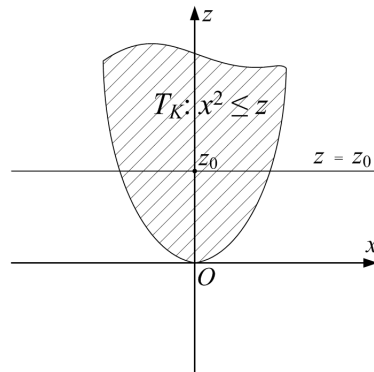


Рис.9

Тогда область истинности двухместного предиката $K(x, z) = \exists y P(x, y, z)$ находится геометрически как проекция указанного тела на координатную плоскость Oxz (см. рис.9). Далее, область истинности предиката $S(z) = \forall x K(x, z)$ составляют все те числа $z_0 \in \mathbf{R}$, для которых прямые с уравнением $z = z_0$ целиком принадлежат T_K . Поскольку таких чисел нет, получаем $T_S = \emptyset$, т.е. для любого

$z \in \mathbf{R}$ имеем $S(z) = \mathbf{0}$, а потому $S(z)$ – тождественно ложный предикат. Это означает, что высказывание $\exists zS(z) = \exists z\forall x\exists yP(x, y, z)$ ложно, т.е. сформулированное выше утверждение неверно.

Заметим, что в разобранном примере о правильном ответе несложно догадаться на интуитивном уровне. Конечно, сделать это было бы гораздо труднее, если бы в рассматриваемом высказывании участвовало не три, а большее число кванторов. Данный пример показывает, как можно в ряде случаев формально, не слишком вдумываясь в смысл высказывания, правильно отвечать на вопрос о его истинностном значении.

§ 2.3. Формулы логики предикатов. Модели и интерпретации

Как и высказывания, предикаты в логике записываются в виде *формул логики предикатов* (сокращенно ФЛП). Зафиксируем некоторый набор предикатных символов $P^{(n)}, Q^{(n)}, R^{(n)}, \dots$ (здесь n – арность соответствующего символа, принимающая значения $n = 0, 1, 2, \dots$), а также некоторый набор x, y, z, \dots символов предметных переменных, возможно, индексированных натуральными числами. Определим ФЛП индукцией по длине:

- (0) логические константы $\mathbf{0}, \mathbf{1}$ являются ФЛП;
- (1) если $P^{(n)}$ – предикатный символ и x_1, \dots, x_n – предметные переменные ($n \geq 0$), то выражения вида $P^{(0)}$ и $P^{(n)}(x_1, \dots, x_n)$ являются ФЛП; такие формулы называются *атомарными*;
- (2) если F и G – ФЛП и x – предметная переменная, то выражения вида $\neg F, (F \wedge G), (F \vee G), (F \longrightarrow G), (F \longleftrightarrow G), \forall xF, \exists xF$ также суть ФЛП; в двух последних случаях формула F называется *областью действия квантора по переменной x* ;
- (3) других формул нет.

Так же как и в случае ФЛВ, договоримся опускать в ФЛП внешние скобки и будем считать, что по убыванию “силы” логические операции располагаются в следующем порядке: $\neg, \forall, \exists, \wedge, \vee, \longrightarrow, \longleftrightarrow$.

При интерпретациях ФЛП (определение см. ниже) n -арные предикатные символы будут отображаться в конкретные n -арные предикаты на множествах; в частности, нульарным символам будут

соответствовать нульарные предикаты, т.е. **0** или **1**. Поэтому нульарные предикатные символы в ФЛП играют ту же роль, что и логические переменные в ФЛВ. Ввиду данного замечания *на всякую ФЛВ мы можем смотреть как на ФЛП, не содержащую кванторов и предикатных символов арности больше нуля.*

Вхождение предметной переменной в ФЛП называется *связанным*, если оно находится сразу за некоторым кванторным символом или входит в область действия квантора по этой переменной. В противном случае вхождение переменной в ФЛП называется *свободным*. *Предметная переменная* называется *свободной (связанной)* в ФЛП, если она имеет по крайней мере одно свободное (соответственно связанное) вхождение в эту формулу. Например, в ФЛП $\forall x(P^{(2)}(x, y) \vee Q^{(1)}(y)) \rightarrow Q^{(1)}(x)$ связанными являются первое и второе вхождения переменной x , а свободными – третье ее вхождение и оба вхождения переменной y . Поэтому в этой формуле переменная x является одновременно и свободной, и связанной, а y только свободной. Если переменные x_1, \dots, x_k свободны в ФЛП F , то часто вместо F пишут $F(x_1, \dots, x_k)$.

Сигнатурой называется произвольное фиксированное множество предикатных символов. Говорят, что ФЛП F является *формулой сигнатуры* Σ , если каждый предикатный символ, используемый в записи F , принадлежит Σ .

Пусть M – некоторое непустое множество, на котором определена совокупность предикатов \mathcal{P} и задано отображение $\mu : \Sigma \rightarrow \mathcal{P}$, ставящее в соответствие каждому n -арному предикатному символу из Σ некоторый n -арный предикат из \mathcal{P} . Тогда трехэлементное множество $\mathfrak{M} = \langle M, \mathcal{P}, \mu \rangle$ называется *моделью* сигнатуры Σ ; при этом M называется *основным множеством* модели \mathfrak{M} .

Пусть $F(x_1, \dots, x_n)$ – ФЛП сигнатуры Σ , где x_1, \dots, x_n – все ее свободные предметные переменные, и $\mathfrak{M} = \langle M, \mathcal{P}, \mu \rangle$ – произвольная модель этой же сигнатуры. *Интерпретацией формулы* F в модели \mathfrak{M} называется отображение $\tilde{\mu} : \{x_1, \dots, x_n\} \cup \Sigma \rightarrow M \cup \mathcal{P}$, переводящее переменные x_1, \dots, x_n в элементы основного множества M модели и совпадающее с μ на Σ (аналогично определяется понятие интерпретации совокупности формул в модели). По каждой интерпретации $\tilde{\mu}$ ФЛП F в модели \mathfrak{M} можно вычислить *истинностное значение* $\tilde{\mu}(F) \in \{\mathbf{0}, \mathbf{1}\}$ следующим образом:

(0) если $F = \mathbf{0}$ или $F = \mathbf{1}$, то соответственно $\tilde{\mu}(F) = \mathbf{0}$ или $\tilde{\mu}(F) = \mathbf{1}$;

(1) если F – атомарная формула, т.е. F имеет вид $P^{(0)}$ или

$P^{(n)}(x_1, \dots, x_n)$, то соответственно $\tilde{\mu}(F) = \tilde{\mu}(P^{(0)})$ или $\tilde{\mu}(F) = P(a_1, \dots, a_n)$, где $P = \tilde{\mu}(P^{(n)})$ и $a_i = \tilde{\mu}(x_i)$, $i = 1, \dots, n$;

(2) если $F = \neg G$ или $F = G \wedge H$, или $F = G \vee H$, или $F = G \longrightarrow H$, или $F = G \longleftrightarrow H$ и значения $\tilde{\mu}(G)$, $\tilde{\mu}(H)$ уже вычислены, то соответственно $\tilde{\mu}(F) = \neg\tilde{\mu}(G)$ или $\tilde{\mu}(F) = \tilde{\mu}(G) \wedge \tilde{\mu}(H)$, или $\tilde{\mu}(F) = \tilde{\mu}(G) \vee \tilde{\mu}(H)$, или $\tilde{\mu}(F) = \tilde{\mu}(G) \longrightarrow \tilde{\mu}(H)$, или $\tilde{\mu}(F) = \tilde{\mu}(G) \longleftrightarrow \tilde{\mu}(H)$;

(3) если $F = \forall xG$ (соответственно $F = \exists xG$), то $\tilde{\mu}(F) = \mathbf{1}$ тогда и только тогда, когда для *любой* (соответственно для *некоторой*) интерпретации η формулы G в \mathfrak{M} , совпадающей с $\tilde{\mu}$ на Σ и на всех отличных от x свободных переменных из G , выполнено $\eta(G) = \mathbf{1}$.

Легко видеть, что понятия интерпретации и истинностного значения ФЛП являются обобщениями аналогичных понятий для ФЛВ.

ПРИМЕР 1. Вычислить истинностное значение ФЛП

$$F(x, y) = \exists x(P^{(1)}(x) \wedge Q^{(2)}(x, y)) \longrightarrow Q^{(2)}(y, x) \vee \neg P^{(1)}(y)$$

в модели $\mathfrak{M} = \langle M, \mathcal{P}, \mu \rangle$ при интерпретации $\tilde{\mu}$, если известно, что $M = \{a, b, c\}$, $\mathcal{P} = \{P, Q\}$, $\mu(P^{(1)}) = P$, $\mu(Q^{(2)}) = Q$ и $\tilde{\mu}(x) = \tilde{\mu}(y) = b$, где

x	$P(x)$
a	1
b	1
c	0

и

$x \setminus y$	a	b	c
a	1	1	0
b	0	1	0
c	1	0	1

По определению, $\tilde{\mu}(F) = \tilde{\mu}(\exists x(P^{(1)}(x) \wedge Q^{(2)}(x, y)) \longrightarrow \tilde{\mu}(Q^{(2)}(y, x) \vee \neg P^{(1)}(y))$. Далее, $\tilde{\mu}(\exists x(P^{(1)}(x) \wedge Q^{(2)}(x, y))) = \mathbf{1} \iff$ для некоторой интерпретации η формулы $P^{(1)}(x) \wedge Q^{(2)}(x, y)$ в \mathfrak{M} такой, что $\eta(y) = \tilde{\mu}(y) = b$, $\eta(P^{(1)}) = \tilde{\mu}(P^{(1)}) = P$ и $\eta(Q^{(2)}) = \tilde{\mu}(Q^{(2)}) = Q$, имеем $\eta(P^{(1)}(x) \wedge Q^{(2)}(x, y)) = \mathbf{1}$. Интерпретация η с таким свойством существует, а именно для $\eta(x) = a$ выполнено $\eta(P^{(1)}(x) \wedge Q^{(2)}(x, y)) = \eta(P^{(1)}(x)) \wedge \eta(Q^{(2)}(x, y)) = P(a) \wedge Q(a, b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. Следовательно, $\tilde{\mu}(\exists x(P^{(1)}(x) \wedge Q^{(2)}(x, y))) = \mathbf{1}$. К тому же $\tilde{\mu}(Q^{(2)}(y, x) \vee \neg P^{(1)}(y)) = \tilde{\mu}(Q^{(2)}(y, x)) \vee \neg\tilde{\mu}(P^{(1)}(y)) = Q(b, b) \vee \neg P(b) = \mathbf{1} \vee \mathbf{0} = \mathbf{1}$. Поэтому $\tilde{\mu}(F) = \tilde{\mu}(\exists x(P^{(1)}(x) \wedge Q^{(2)}(x, y)) \longrightarrow \tilde{\mu}(Q^{(2)}(y, x) \vee \neg P^{(1)}(y))) = \mathbf{1} \longrightarrow \mathbf{1} = \mathbf{1}$.

Иногда для нахождения истинностного значения ФЛП $F(x_1, \dots, x_n)$ в модели $\mathfrak{M} = \langle M, \mathcal{P}, \mu \rangle$ при интерпретации $\tilde{\mu}$

удобно пользоваться не формальным его определением, а следующими соображениями. Если в формулу $F(x_1, \dots, x_n)$ вместо предикатных символов подставить соответствующие им при интерпретации $\tilde{\mu}$ предикаты из \mathcal{P} , а вместо всех свободных вхождений переменных x_1, \dots, x_n — соответствующие им элементы $\tilde{\mu}(x_1), \dots, \tilde{\mu}(x_n)$ основного множества M модели, то формула $F(x_1, \dots, x_n)$ перейдет в некоторое высказывание об элементах множества M . В зависимости от того, истинно или ложно это высказывание, будет истинно или ложно значение F при данной интерпретации.

ПРИМЕР 2. Вычислить истинностное значение ФЛП

$$F(y, z) = \forall x(P^{(2)}(x, y) \longrightarrow Q^{(2)}(x, y) \vee Q^{(2)}(x, z))$$

в модели $\mathfrak{M} = \langle \mathbf{N}, \mathcal{P}, \mu \rangle$ при интерпретации $\tilde{\mu}$, если известно, что \mathbf{N} — множество натуральных чисел, $\mathcal{P} = \{P, Q\}$, $\mu : P^{(2)} \mapsto P : P(m, n) = \mathbf{1} \iff m \mid n$, $Q^{(2)} \mapsto Q : Q(m, n) = \mathbf{1} \iff n = m$, $\tilde{\mu} : y \mapsto 5, z \mapsto 1$.

При интерпретации $\tilde{\mu}$ формула F переходит в следующее высказывание о натуральных числах: “для любого натурального числа x из того, что x делит 5, вытекает, что $x = 5$ или $x = 1$ ”. Так как в силу простоты числа 5 это высказывание истинно, получаем $\tilde{\mu}(F) = \mathbf{1}$.

На языке ФЛП могут быть выражены свойства многих математических объектов, что выгодно отличает этот язык от более бедного языка ФЛВ. Приведем поясняющие примеры.

ПРИМЕР 3. Записать с помощью ФЛП свойство числа быть наибольшим общим делителем двух натуральных чисел.

Напомним, что $d = \text{НОД}(a, b)$, если, во-первых, d — общий делитель чисел a и b и, во-вторых, d делится на любой общий делитель a и b . В данном определении НОД встречается двухместный предикат $P(n, m)$ “деления нацело числа n на число m ”, заданный на множестве \mathbf{N} натуральных чисел: $P(n, m) = \mathbf{1} \iff m \mid n$. Следовательно, нам понадобится один двухместный предикатный символ $P^{(2)}$. Рассмотрим формулу

$$F(a, b, d) = P^{(2)}(a, d) \wedge P^{(2)}(b, d) \wedge \forall x(P^{(2)}(a, x) \wedge P^{(2)}(b, x) \longrightarrow P^{(2)}(d, x))$$

сигнатуры $\{P^{(2)}\}$. Эта формула является, очевидно, искомой в том смысле, что для произвольной ее интерпретации $\tilde{\mu}$ в множестве \mathbf{N}

натуральных чисел, замещающей предикатный символ $P^{(2)}$ предикатом P делимости нацело, выполнено $\check{\mu}(F(a, b, d)) = \mathbf{1}$ тогда и только тогда, когда $d = \text{НОД}(a, b)$.

ПРИМЕР 4. Записать с помощью ФЛП свойство натурального числа быть простым числом.

Число $a \in \mathbf{N}$ простое, если высказывание “для любого $x \in \mathbf{N}$ условие $x \mid a$ влечет за собой $x = a$ или $x = 1$ ” истинно. В данном высказывании фигурируют два двухместных предиката, заданных на \mathbf{N} : $P(n, m) = \mathbf{1} \iff m \mid n$ и $Q(n, m) = \mathbf{1} \iff n = m$ (предикат равенства). В искомой формуле им будут соответствовать предикатные символы $P^{(2)}$ и $Q^{(2)}$. Поскольку в формулу символ числа один не может входить (это не предметная переменная), нам необходимо выразить еще на языке ФЛП свойство натурального числа быть единицей. Это легко сделать, например, используя тот факт, что число y из \mathbf{N} равно единице в том и только в том случае, если высказывание “всякое натуральное число x делится на y ” истинно. Учитывая сказанное, получаем, что формула

$$F(a) = \exists y(\forall x P^{(2)}(x, y) \wedge \forall x(P^{(2)}(a, x) \longrightarrow Q^{(2)}(x, a) \vee Q^{(2)}(x, y)))$$

является искомой.

При различных интерпретациях ФЛП F может принимать различные истинностные значения даже в одной и той же модели \mathfrak{M} . F называется *выполнимой* (*истинной*) на модели \mathfrak{M} , если для *некоторой* (соответственно для *любой*) интерпретации ϕ формулы F в \mathfrak{M} имеет место равенство $\phi(F) = \mathbf{1}$. F называется просто *выполнимой*, если она выполнима на некоторой модели, и *логически общезначимой*, если она истинна на любой модели соответствующей сигнатуры. F называется *логически противоречивой*, если формула $\neg F$ логически общезначима, т.е. $\phi(F) = \mathbf{0}$ для любой интерпретации ϕ формулы F (в произвольную модель). Данные понятия обобщают понятия выполнимой формулы, тавтологии и противоречия, которые встречались в логике высказываний.

Говорят, что *модель конечна* или *бесконечна* в зависимости от того, конечно или бесконечно ее основное множество. Следующий пример показывает, что язык логики предикатов позволяет различать понятия конечного и бесконечного, на что “не способен” язык логики высказываний.

ПРИМЕР 5. Убедиться, что ФЛП $F = \forall x \forall y \forall z (\neg P^{(2)}(x, x) \wedge (P^{(2)}(x, y) \wedge P^{(2)}(y, z) \longrightarrow P^{(2)}(x, z))) \wedge \forall x \exists y P^{(2)}(x, y)$ выполнима

в некоторой бесконечной модели и не выполнима ни в какой конечной модели.

Рассмотрим модель $\mathfrak{M} = \langle \mathbf{N}, \{P\}, \mu \rangle$ сигнатуры $\{P^{(2)}\}$, где P – обычный предикат строгого частичного порядка на множестве \mathbf{N} натуральных чисел, т.е. $P(x, y) = \mathbf{1} \iff x < y$, и $\mu(P^{(2)}) = P$. Поскольку F не содержит свободных предметных переменных, отображение μ является единственной интерпретацией формулы F в модели \mathfrak{M} , причем $\mu(F) = \mathbf{1}$, т.к. отношение $<$ антирефлексивно (для любого $x \in \mathbf{N} : x \not< x$), транзитивно (для любых $x, y, z \in \mathbf{N} : x < y \wedge y < z \longrightarrow x < z$), и для любого $x \in \mathbf{N}$ существует $y \in \mathbf{N}$ такой, что $x < y$.

Вместе с тем формула F не выполняется ни в какой конечной модели $\mathfrak{M}' = \langle M, \{P'\}, \mu' \rangle$. Действительно, в противном случае в M существовала бы сколь угодно длинная цепочка элементов $x_1, x_2, \dots, x_n, \dots$ такая, что $P'(x_i, x_{i+1}) = \mathbf{1}$ для $i = 1, 2, \dots$, и ввиду транзитивности P' имели бы $P'(x_i, x_j) = \mathbf{1}$ для всех $i < j$. Отсюда и из свойства антирефлексивности ($\forall x \neg P'(x, x) = \mathbf{1}$) получаем $x_i \neq x_j$, если $i \neq j$, т.е. все элементы $x_1, x_2, \dots, x_n, \dots$ попарно различны, а это противоречит конечности \mathfrak{M}' .

§ 2.4. Законы логики предикатов

Понятие равносильности ФЛВ естественным образом переносится на ФЛП. Две ФЛП F и G называются *равносильными*, если для любой модели [соответствующей сигнатуры] и для любой интерпретации ϕ формул F и G в эту модель $\phi(F) = \phi(G)$. Другими словами, формулы равносильны, если они не различимы на моделях. Ясно, что отношение равносильности является эквивалентностью, разбивающей множество ФЛП на классы равносильных формул. Примерами таких классов являются классы логически общезначимых и логически противоречивых формул. Как обычно, пишем $F \equiv G$, если F и G равносильны.

Укажем на языке равносильности формул наиболее важные законы логики предикатов.

0. Все законы логики высказываний справедливы и в логике предикатов (см. § 1.2).

1. *Законы отрицания:*

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

$$\neg\exists xF(x) \equiv \forall x\neg F(x).$$

2. Законы перестановочности однопипных кванторов:

$$\forall x\forall yF(x, y) \equiv \forall y\forall xF(x, y),$$

$$\exists x\exists yF(x, y) \equiv \exists y\exists xF(x, y).$$

3. Законы дистрибутивности \forall относительно \wedge и \exists относительно \vee :

$$\forall x(F(x) \wedge G(x)) \equiv \forall xF(x) \wedge \forall xG(x),$$

$$\exists x(F(x) \vee G(x)) \equiv \exists xF(x) \vee \exists xG(x).$$

4. Если переменная x не встречается в формуле G или всякое вхождение x в G является связанным, то имеют место законы:

$$\forall x(F(x) \wedge G) \equiv \forall xF(x) \wedge G,$$

$$\forall x(F(x) \vee G) \equiv \forall xF(x) \vee G,$$

$$\exists x(F(x) \wedge G) \equiv \exists xF(x) \wedge G,$$

$$\exists x(F(x) \vee G) \equiv \exists xF(x) \vee G.$$

5. Если переменная y не встречается в формуле $F(x)$, то допустима подстановка y вместо переменной x в формулах $\forall xF(x)$ и $\exists xF(x)$, а именно:

$$\forall xF(x) \equiv \forall yF(y),$$

$$\exists xF(x) \equiv \exists yF(y).$$

Приведенные законы логики предикатов нуждаются в проверке. Проверим, например, один из законов отрицания: $\neg\forall xF(x) \equiv \exists x\neg F(x)$. Для этого выпишем наряду с x все свободные предметные переменные, входящие в формулу F : x, x_1, \dots, x_n , и рассмотрим интерпретацию ϕ формул $\neg\forall xF(x)$ и $\exists x\neg F(x)$ в произвольной модели \mathfrak{M} соответствующей сигнатуры. Тогда, по определению, имеем: $\phi(\neg\forall xF(x)) = \mathbf{1} \iff \phi(\forall xF(x)) = \mathbf{0} \iff$ неверно, что для любой интерпретации ϕ' формулы F такой, что $\phi'(x_1) = \phi(x_1), \dots, \phi'(x_n) = \phi(x_n)$, выполнено $\phi'(F) = \mathbf{1} \iff$ для некоторой интерпретации ϕ' формулы F в \mathfrak{M} такой, что $\phi'(x_1) = \phi(x_1), \dots, \phi'(x_n) = \phi(x_n)$, выполнено $\phi'(F) = \mathbf{0}$, т.е. $\phi'(\neg F) = \mathbf{1} \iff \phi(\exists x\neg F(x)) = \mathbf{1}$. Таким образом, $\phi(\neg\forall F(x)) = \phi(\exists x\neg F(x))$ для любой интерпретации ϕ этих формул, а значит, $\neg\forall xF(x) \equiv \exists x\neg F(x)$.

Аналогично проверяются и остальные законы логики предикатов. При этом первый и четвертый законы пункта 4 являются простыми следствиями законов дистрибутивности \forall относительно \wedge и \exists относительно \vee . Действительно, если переменная x не входит в формулу G или всякое вхождение x в G связано, то легко понять, что формулы $\forall xG$ и $\exists xG$ равносильны формуле G , и потому $\forall x(F(x) \wedge G) \equiv \forall xF(x) \wedge \forall xG \equiv \forall xF(x) \wedge G$ и $\exists x(F(x) \vee G) \equiv \exists xF(x) \vee \exists xG \equiv \exists xF(x) \vee G$. В этом случае имеет место также дистрибутивность \forall относительно \vee и \exists относительно \wedge (см. пункт 4). Однако в общем случае $\forall x(F(x) \vee G(x)) \not\equiv \forall xF(x) \vee \forall xG(x)$ и $\exists x(F(x) \wedge G(x)) \not\equiv \exists xF(x) \wedge \exists xG(x)$.

Покажем, например, что $\forall x(F(x) \vee G(x)) \not\equiv \forall xF(x) \vee \forall xG(x)$ для некоторых атомарных формул $F(x)$ и $G(x)$ (считаем, что F и G – одноместные предикатные символы). Для этого рассмотрим модель $\mathfrak{M} = \langle \mathbf{N}, \{P, Q\}, \mu \rangle$, где одноместные предикаты P и Q определяются на множестве \mathbf{N} натуральных чисел следующим образом: $P(x) = \mathbf{1} \iff x \leq 2$ и $Q(x) = \mathbf{1} \iff x > 2$, а $\mu(F) = P$ и $\mu(G) = Q$.

Тогда, очевидно, $\mu(\forall x(F(x) \vee G(x))) = \mathbf{1}$, в то время как $\mu(\forall xF(x) \vee \forall xG(x)) = \mu(\forall xF(x)) \vee \mu(\forall xG(x)) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$. Следовательно, формулы $\forall x(F(x) \vee G(x))$ и $\forall xF(x) \vee \forall xG(x)$ не равносильны.

Отметим некоторые важные следствия из выписанных законов логики предикатов:

$$1'. \quad \exists x(F(x) \longrightarrow G(x)) \equiv \forall xF(x) \longrightarrow \exists xG(x).$$

2'. Если переменная x не встречается в формуле G или всякое вхождение x в G является связанным, то

$$\exists x(F(x) \longrightarrow G) \equiv \forall xF(x) \longrightarrow G,$$

$$\forall x(F(x) \longrightarrow G) \equiv \exists xF(x) \longrightarrow G,$$

$$\exists x(G \longrightarrow F(x)) \equiv G \longrightarrow \exists xF(x),$$

$$\forall x(G \longrightarrow F(x)) \equiv G \longrightarrow \forall xF(x).$$

Докажем равносильность 1'. В самом деле, $\exists x(F(x) \longrightarrow G(x)) \equiv \exists x(\neg F(x) \vee G(x)) \equiv \exists x\neg F(x) \vee \exists xG(x) \equiv \neg \forall xF(x) \vee \exists xG(x) \equiv \forall xF(x) \longrightarrow \exists xG(x)$.

Первая и третья равносильности пункта 2' вытекают из 1', а остальные получаются аналогично 1' применением законов логики предикатов из пункта 4.

ПРИМЕР 1. Доказать, что ФЛП

$$F = \exists xP^{(2)}(x, t) \longrightarrow \exists uQ^{(3)}(y, t, u) \wedge \forall xR^{(1)}(x)$$

и

$$G = \forall x\forall z\exists u(P^{(2)}(x, t) \longrightarrow Q^{(3)}(y, t, u) \wedge R^{(1)}(z))$$

равносильны.

$$\begin{aligned} & \text{Действительно, } F = \exists xP^{(2)}(x, t) \longrightarrow \exists uQ^{(3)}(y, t, u) \wedge \forall xR^{(1)}(x) \\ \equiv^4 & \exists xP^{(2)}(x, t) \longrightarrow \forall x(\exists uQ^{(3)}(y, t, u) \wedge R^{(1)}(x)) \\ \equiv^4 & \exists xP^{(2)}(x, t) \longrightarrow \forall x\exists u(Q^{(3)}(y, t, u) \wedge R^{(1)}(x)) \\ \equiv^5 & \exists xP^{(2)}(x, t) \longrightarrow \forall z\exists u(Q^{(3)}(y, t, u) \wedge R^{(1)}(z)) \\ \equiv^{2'} & \forall x(P^{(2)}(x, t) \longrightarrow \forall z\exists u(Q^{(3)}(y, t, u) \wedge R^{(1)}(z))) \\ \equiv^{2'} & \forall x\forall z(P^{(2)}(x, t) \longrightarrow \exists u(Q^{(3)}(y, t, u) \wedge R^{(1)}(z))) \\ \equiv^{2'} & \forall x\forall z\exists u(P^{(2)}(x, t) \longrightarrow Q^{(3)}(y, t, u) \wedge R^{(1)}(z)) = G. \end{aligned}$$

ПРИМЕР 2. Доказать, что ФЛП

$$F = \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (\exists xP^{(1)}(x) \longrightarrow \exists xQ^{(2)}(x, y))$$

логически общезначима.

Проверять логическую общезначимость формулы F , используя непосредственно определение (см. §2.3), довольно сложно. Поэтому мы сначала упростим F с помощью равносильных преобразований:

$$\begin{aligned} F &= \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (\exists xP^{(1)}(x) \longrightarrow \exists xQ^{(2)}(x, y)) \\ \equiv^5 & \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (\exists zP^{(1)}(z) \longrightarrow \exists xQ^{(2)}(x, y)) \\ \equiv^{2'} & \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow \exists x(\exists zP^{(1)}(z) \longrightarrow Q^{(2)}(x, y)) \\ \equiv^{2'} & \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow \exists x\forall z(P^{(1)}(z) \longrightarrow Q^{(2)}(x, y)) \\ \equiv^{1'} & \exists x((P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow \forall z(P^{(1)}(z) \longrightarrow Q^{(2)}(x, y))) \\ \equiv^{2'} & \exists x\forall z((P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (P^{(1)}(z) \longrightarrow Q^{(2)}(x, y))) \\ \equiv^0 & \exists x\forall z(\neg(\neg P^{(1)}(x) \vee Q^{(2)}(x, y)) \vee (\neg P^{(1)}(z) \vee Q^{(2)}(x, y))) \\ \equiv^0 & \exists x\forall z(P^{(1)}(x) \vee \neg P^{(1)}(z) \vee Q^{(2)}(x, y)). \end{aligned}$$

Итак, $F \equiv G(y)$, где $G(y) = \exists x\forall z(P^{(1)}(x) \vee \neg P^{(1)}(z) \vee Q^{(2)}(x, y))$. Покажем теперь, что формула $G(y)$ логически общезначима. Зафиксируем произвольную модель $\mathfrak{M} = \langle M, \{P, Q\}, \mu \rangle$, где P и Q — соответственно одноместный и двухместный предикаты на основном множестве M модели и $\mu(P^{(1)}) = P$, $\mu(Q^{(2)}) = Q$. Пусть $\tilde{\mu}$ — произвольная интерпретация формулы $G(y)$ в модели \mathfrak{M} , отображающая свободную предметную переменную y в некоторый элемент b из M . Тогда $G(y)$ перейдет при интерпретации $\tilde{\mu}$ в следующее высказывание об элементах множества M : “существует $x \in M$ такой, что для любого $z \in M$ справедливо $P(x) = \mathbf{1}$ или $\neg P(z) = \mathbf{1}$,

или $Q(x, b) = \mathbf{1}$ ". Если найдется элемент $x \in M$ такой, что $P(x) = \mathbf{1}$, то данное высказывание, очевидно, истинно. В противном случае P – тождественно ложный предикат и, следовательно, для любого элемента $z \in M$ имеем $\neg P(z) = \mathbf{1}$, что, в свою очередь, опять влечет за собой истинность рассматриваемого высказывания. Таким образом, $\tilde{\mu}(G) = \mathbf{1}$ для произвольной интерпретации $\tilde{\mu}$, т.е. G – логически общезначимая формула. Отсюда следует общезначимость исходной формулы F .

Законы логики предикатов позволяют правильно строить отрицания различных предложений.

ПРИМЕР 3. Записать условие для действительного числа a , означающее, что a не является пределом функции $f(x)$ в точке x_0 .

Приведем сначала определение предела функции действительного аргумента: *число a называется пределом функции $f(x)$ в точке x_0 , если для любого положительного ϵ существует положительное δ такое, что для любого числа x неравенство $|x - x_0| < \delta$ влечет за собой $|f(x) - a| < \epsilon$.*

Запишем данное определение на языке ФЛП:

$$F(a, x_0) = \forall \epsilon (\epsilon > 0 \longrightarrow \exists \delta (\delta > 0 \wedge \forall x (|x - x_0| < \delta \longrightarrow |f(x) - a| < \epsilon));$$

здесь мы отождествляем для простоты предметные переменные с действительными числами, а вместо символов предикатов пишем сами предикаты “ $\epsilon > 0$ ”, “ $\delta > 0$ ”, “ $|x - x_0| < \delta$ ” и “ $|f(x) - a| < \epsilon$ ”.

Тогда имеем: $\neg F(a, x_0)$

$$\begin{aligned} &\equiv \exists \epsilon \neg (\epsilon > 0 \longrightarrow \exists \delta (\delta > 0 \wedge \forall x (|x - x_0| < \delta \longrightarrow |f(x) - a| < \epsilon))) \\ &\equiv \exists \epsilon \neg (\neg (\epsilon > 0) \vee \exists \delta (\delta > 0 \wedge \forall x (\neg (|x - x_0| < \delta) \vee |f(x) - a| < \epsilon))) \\ &\equiv \exists \epsilon (\epsilon > 0 \wedge \forall \delta (\delta > 0 \wedge \forall x (\neg (|x - x_0| < \delta) \vee |f(x) - a| < \epsilon))) \\ &\equiv \exists \epsilon (\epsilon > 0 \wedge \forall \delta (\neg (\delta > 0) \vee \neg \forall x (\neg (|x - x_0| < \delta) \vee |f(x) - a| < \epsilon))) \\ &\equiv \exists \epsilon (\epsilon > 0 \wedge \forall \delta (\neg (\delta > 0) \vee \exists x (\neg \neg (|x - x_0| < \delta) \wedge \neg (|f(x) - a| < \epsilon)))) \\ &\equiv \exists \epsilon (\epsilon > 0 \wedge \forall \delta (\delta > 0 \longrightarrow \exists x (|x - x_0| < \delta \wedge |f(x) - a| \geq \epsilon))). \end{aligned}$$

Таким образом, *число a не является пределом функции $f(x)$ в точке x_0 , если (и только если) существует положительное ϵ такое, что для любого положительного δ найдется число x , для которого $|x - x_0| < \delta$ и тем не менее $|f(x) - a| \geq \epsilon$.*

§ 2.5. Предваренные нормальные формы

ФЛП называется *предваренной нормальной формой* (сокращенно ПНФ), если она имеет вид

$$\mathbf{q}_1 x_1 \mathbf{q}_2 x_2 \cdots \mathbf{q}_n x_n F(x_1, x_2, \dots, x_n),$$

где $\mathbf{q}_i \in \{\forall, \exists\}$ для $i = 1, 2, \dots, n$ и формула F не содержит кванторов. Таким образом, в ПНФ все кванторы (если они есть) “вынесены вперед”. При этом последовательность кванторов $\mathbf{q}_1 x_1 \mathbf{q}_2 x_2 \cdots \mathbf{q}_n x_n$ называется *кванторной приставкой*, а формула $F(x_1, x_2, \dots, x_n)$ – бескванторной частью ПНФ. Справедлива следующая

ТЕОРЕМА. *Всякая ФЛП равносильна некоторой ПНФ.*

Доказательство. Пусть G – произвольная ФЛП. Поскольку все логические связки могут быть выражены через связки \neg и \wedge (см. §1.5), а квантор $\exists x$ – через квантор $\forall x$ и отрицание \neg (т.к. $\exists x H(x) \equiv \neg \forall \neg H(x)$), считаем без ограничения общности, что в формулу G входят лишь символы логических операций \neg , \wedge и \forall . Далее доказательство будем проводить индукцией по длине формулы G .

Случай 1: G равна $\mathbf{0}$, $\mathbf{1}$ или атомарной формуле. Тогда G сама является ПНФ.

Случай 2: $G = \neg H$. По предположению индукции, формула H равносильна ПНФ вида $\mathbf{q}_1 x_1 \cdots \mathbf{q}_n x_n H'(x_1, \dots, x_n)$. Тогда $G \equiv \neg H \equiv \neg \mathbf{q}_1 x_1 \cdots \mathbf{q}_n x_n H'(x_1, \dots, x_n) \equiv \bar{\mathbf{q}}_1 x_1 \cdots \bar{\mathbf{q}}_n x_n \neg H'(x_1, \dots, x_n)$, где

$$\bar{\mathbf{q}}_i = \begin{cases} \forall, & \text{если } \mathbf{q}_i = \exists, \\ \exists, & \text{если } \mathbf{q}_i = \forall. \end{cases}$$

Случай 3: $G = H_1 \wedge H_2$. Применяя индуктивное предположение к формулам H_1 и H_2 , имеющим меньшую длину, чем G , получаем, что они равносильны соответственно ПНФ вида $\mathbf{q}_1 x_1 \cdots \mathbf{q}_n x_n H'_1(x_1, \dots, x_n)$ и $\mathbf{q}'_1 y_1 \cdots \mathbf{q}'_m y_m H'_2(y_1, \dots, y_m)$. Ввиду законов 5 логики предикатов (см. §2.4) мы имеем право при необходимости переименовывать связанные вхождения переменных в ФЛП, а значит, можем считать, что переменные x_1, \dots, x_n не встречаются в записи формулы $\mathbf{q}'_1 y_1 \cdots \mathbf{q}'_m y_m H'_2(y_1, \dots, y_m)$, а переменные y_1, \dots, y_m – в записи формулы $\mathbf{q}_1 x_1 \cdots \mathbf{q}_n x_n H'_1(x_1, \dots, x_n)$. Тогда, учитывая законы 4 логики предикатов, получаем $G = H_1 \wedge H_2 \equiv \mathbf{q}_1 x_1 \cdots \mathbf{q}_n x_n H'_1(x_1, \dots, x_n) \wedge \mathbf{q}'_1 y_1 \cdots \mathbf{q}'_m y_m H'_2(y_1, \dots, y_m) \equiv \mathbf{q}_1 x_1 \cdots \mathbf{q}_n x_n \mathbf{q}'_1 y_1 \cdots \mathbf{q}'_m y_m (H'_1(x_1, \dots, x_n) \wedge H'_2(y_1, \dots, y_m))$. Последняя формула является ПНФ, равносильной G .

Случай 4: $G = \forall xH(x)$. По предположению индукции, $H(x)$ равносильна некоторой ПНФ вида $\mathbf{q}_1x_1 \cdots \mathbf{q}_nx_nH'(x, x_1, \dots, x_n)$, причем из соображений, приведенных выше, также можно считать, что переменные x_1, \dots, x_n отличны от x . Тогда, очевидно, формула $G = \forall xH(x)$ равносильна ПНФ вида $\forall x\mathbf{q}_1x_1 \cdots \mathbf{q}_nx_nH'(x, x_1, \dots, x_n)$. Теорема доказана.

В доказательстве этой теоремы указан, по существу, алгоритм приведения любой ФЛП к равносильной ей ПНФ. При этом, конечно, не обязательно приводить сначала данную ФЛП к формуле, содержащей лишь символы логических операций \neg , \wedge , \vee ; законы логики предикатов 3,4 и 5, а также следствия 1' и 2' из этих законов позволяют легко выносить вперед все кванторы в любом конкретном случае.

ПРИМЕР 1. Построить ПНФ, равносильные следующим ФЛП:
 $F_1 = \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (\forall yP^{(1)}(y) \vee \exists zQ^{(2)}(y, z));$
 $F_2 = \exists xQ^{(2)}(x, y) \longrightarrow (P^{(1)}(x) \longrightarrow \neg\exists zQ^{(2)}(x, z)).$

Имеем:

$$\begin{aligned} F_1 &\equiv \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (\forall uP^{(1)}(u) \vee \exists zQ^{(2)}(y, z)) \\ &\equiv \forall x(P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow \forall u\exists z(P^{(1)}(u) \vee Q^{(2)}(y, z)) \\ &\equiv \exists x((P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow \forall u\exists z(P^{(1)}(u) \vee Q^{(2)}(y, z))) \\ &\equiv \exists x\forall u\exists z((P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (P^{(1)}(u) \vee Q^{(2)}(y, z))); \end{aligned}$$

$$\begin{aligned} F_2 &\equiv \exists tQ^{(2)}(t, y) \longrightarrow (P^{(1)}(x) \longrightarrow \forall z\neg Q^{(2)}(x, z)) \\ &\equiv \exists tQ^{(2)}(t, y) \longrightarrow \forall z(P^{(1)}(x) \longrightarrow \neg Q^{(2)}(x, z)) \\ &\equiv \forall t(Q^{(2)}(t, y) \longrightarrow \forall z(P^{(1)}(x) \longrightarrow \neg Q^{(2)}(x, z))) \\ &\equiv \forall t\forall z(Q^{(2)}(t, y) \longrightarrow (P^{(1)}(x) \longrightarrow \neg Q^{(2)}(x, z))). \end{aligned}$$

ЗАМЕЧАНИЕ. Приведение к ПНФ формул логики предикатов не является однозначным. Действительно, легко видеть, например, что формула F_1 в разобранным примере может быть приведена и к ПНФ вида

$$\forall u\exists z\exists x((P^{(1)}(x) \longrightarrow Q^{(2)}(x, y)) \longrightarrow (P^{(1)}(u) \vee Q^{(2)}(y, z)))$$

с существенно другой кванторной приставкой. Удивительно, что данная формула равносильна ПНФ, полученной в примере 1, несмотря на то, что разнотипные кванторы, как нетрудно понять, переставлять в общем случае нельзя.

ПРИМЕР 2. Доказать равносильность ФЛП приведением их к ПНФ:

$$F_1 = \exists x(\forall yP^{(2)}(x, y) \longrightarrow Q^{(1)}(x) \vee R^{(1)}(y));$$

$$F_2 = \exists z(\exists x\neg P^{(2)}(x, z) \vee \exists xQ^{(1)}(x) \vee R^{(1)}(y)).$$

$$\text{Имеем } F_1 \equiv \exists x(\forall zP^{(2)}(x, z) \longrightarrow Q^{(1)}(x) \vee R^{(1)}(y))$$

$$\equiv \exists x\exists z(P^{(2)}(x, z) \longrightarrow Q^{(1)}(x) \vee R^{(1)}(y));$$

$$F_2 \equiv \exists z(\exists x(\neg P^{(2)}(x, z) \vee Q^{(1)}(x)) \vee R^{(1)}(y))$$

$$\equiv \exists z\exists x(\neg P^{(2)}(x, z) \vee Q^{(1)}(x) \vee R^{(1)}(y))$$

$$\equiv \exists z\exists x(P^{(2)}(x, z) \longrightarrow Q^{(1)}(x) \vee R^{(1)}(y))$$

$$\equiv \exists x\exists z(P^{(2)}(x, z) \longrightarrow Q^{(1)}(x) \vee R^{(1)}(y)).$$

Так как полученные ПНФ для формул F_1 и F_2 совпадают, заключаем, что $F_1 \equiv F_2$.

§ 2.6. Проблема разрешения для общезначимости и выполнимости ФЛП

В логике высказываний вопрос о том, будет ли данная формула тавтологией или выполнимой формулой, решается очень просто — методом построения ее таблицы истинности (или, что то же самое, методом интерпретаций). К сожалению, распространить этот метод на все ФЛП невозможно по той простой причине, что тогда пришлось бы интерпретировать ту или иную формулу в *бесконечном* множестве моделей для доказательства ее общезначимости или выполнимости. Поэтому в логике предикатов естественна постановка следующей задачи, носящей название *проблемы разрешения*: *указать единый эффективный способ, т.е. алгоритм, для определения по произвольной ФЛП, выполнима она (соответственно логически общезначима) или нет.*

Заметим, что вопрос об общезначимости ФЛП полностью сводится к вопросу о выполнимости соответствующих формул. В самом деле, формула F логически общезначима тогда и только тогда, когда формула $\neg F$ логически противоречива, т.е. невыполнима. Поэтому, проверяя, выполнима или нет формула $\neg F$, мы тем самым отвечаем на вопрос об общезначимости формулы F , и наоборот. К сожалению, в отличие от логики высказываний, проблема разрешения в логике предикатов оказалась связанной с большими трудностями. Причины этих затруднений были выяснены лишь в 30-е годы XX века, когда в математике было дано строгое определение понятия алгоритма. Это помогло американскому логик Алонзо Чёрчу впервые установить, что *проблема разрешения для*

логики предикатов неразрешима, т.е. искомый в этой проблеме алгоритм невозможен.

ЗАМЕЧАНИЕ. В переводе на компьютерный язык последнее означает, что нельзя написать программу, которая бы позволяла по произвольной ФЛП выдавать за конечное время ответ (положительный или отрицательный) о выполнимости или общезначимости этой формулы. Вместе с тем, в логике имеется ряд мощных методов, помогающих в ряде весьма общих случаев решать данную задачу. С одним из таких методов – *правилом резолюций* – читатель может познакомиться, например, в книгах [6], [22]. Отметим, что указанный метод, в отличие от того, на что “способен” универсальный алгоритм, позволяет лишь для любой ФЛП, которая невыполнима (что, разумеется, заранее не известно), через конечное число шагов подтвердить этот факт. Если же формула, подаваемая на входе в компьютер, выполнима, то программа, написанная по методу резолюций, может бесконечно долго работать (“циклить”), при этом пользователь априори не будет знать о том, происходит “заикливание” или все же через какое-то конечное время работы компьютер остановится и выдаст ответ. В математической теории алгоритмов обсуждаемый в данном контексте вопрос тесным образом связан с такими понятиями как *рекурсивное* и *рекурсивно-перечислимое множества*, с их сходством и различием (см. например, [15]). Строго говоря, множество всех невыполнимых формул (как и множество логически общезначимых формул) является всего лишь рекурсивно-перечислимым, но не рекурсивным. Множество же всех выполнимых ФЛП не только не рекурсивно, но даже не рекурсивно-перечислимо.

Неразрешимость в общем случае указанной проблемы для логики предикатов не означает, что мы не сможем в каких-то конкретных случаях определить, является данная ФЛП выполнимой (логически общезначимой) или нет (см., в частности, примеры 5 из §2.3 и 2 из §2.4). Более того, для некоторых не слишком широких, но важных классов ФЛП решение данной проблемы может быть осуществлено. К числу таких формул относятся, например, ФЛП, содержащие только предикатные символы, арности которых равны единице (т.е. они содержат в своей записи лишь атомарные формулы от одной переменной). Часть логики, в которой употребляются только такие выражения, связана с именем Аристотеля, который впервые ее исследовал. Известные виды умозаключений этой логи-

ки, так называемые “модусы силлогизмов”, полностью выражаются на языке формул от одной предметной переменной (вспомним хотя бы умозаключение: “Все люди смертны. Сократ – человек. Следовательно, Сократ смертен”). В связи с этим сформулируем следующее принципиальное утверждение.

ТЕОРЕМА. *Если ФЛП, содержащая только предикатные символы арности один, выполнима на некоторой модели, то она выполнима и на модели, основное множество которой содержит не более чем 2^n элементов, где n – число различных предикатных символов в записи этой формулы.*

Не приводя полное доказательство этой теоремы, укажем его идею. Пусть формула $F(x_1, x_2, \dots, x_m)$ удовлетворяет условию теоремы, где x_1, x_2, \dots, x_m – все свободные предметные переменные в ее записи. Тогда формула $\exists x_1 \exists x_2 \dots \exists x_m F(x_1, x_2, \dots, x_m)$ так же будет удовлетворять этому условию, поскольку, очевидно, $F(x_1, x_2, \dots, x_m)$ выполнима на какой-то модели в том и только в том случае, когда $\exists x_1 \exists x_2 \dots \exists x_m F(x_1, x_2, \dots, x_m)$ выполнима на этой модели. Поэтому далее без ограничения общности можно считать, что все вхождения предметных переменных в исходной формуле F связаны. Запишем F в предваренной нормальной форме:

$$\mathbf{q}_1 x_1 \cdots \mathbf{q}_k x_k H(P_1^{(1)}(x_1), \dots, P_1^{(1)}(x_k); \dots; P_n^{(1)}(x_1), \dots, P_n^{(1)}(x_k)),$$

где $H(P_1^{(1)}(x_1), \dots, P_1^{(1)}(x_k); \dots; P_n^{(1)}(x_1), \dots, P_n^{(1)}(x_k))$ – бескванторная часть формулы F ; здесь H – ФЛВ $H(A_{11}, \dots, A_{1k}; \dots; A_{n1}, \dots, A_{nk})$, в которую вместо каждой логической переменной A_{ij} ($1 \leq i \leq n, 1 \leq j \leq k$) подставлена атомарная формула $P_i^{(1)}(x_j)$ от одной предметной переменной. Так как F выполнима, найдется модель с основным множеством M и конкретными предикатами $P_i(x_j)$ ($1 \leq i \leq n, 1 \leq j \leq k$) на нем, для которых

$$\phi(F) = \mathbf{q}_1 x_1 \cdots \mathbf{q}_k x_k H(P_1(x_1), \dots, P_1(x_k); \dots; P_n(x_1), \dots, P_n(x_k)) = \mathbf{1};$$

здесь ϕ – такая интерпретация формулы F в эту модель, что $\phi(P_i^{(1)}) = P_i$, $i = 1, 2, \dots, n$.

Для каждого кортежа $\alpha = (\xi_1, \xi_2, \dots, \xi_n) \in \{\mathbf{0}, \mathbf{1}\}^n$ выберем теперь в M такие элементы a , для которых выполнены равенства

$$P_1(a) = \xi_1, P_2(a) = \xi_2, \dots, P_n(a) = \xi_n,$$

и подмножество всех этих элементов в M обозначим через M_α . Ясно, что $M_\alpha \cap M_\beta = \emptyset$ при $\alpha \neq \beta$ и $M = \bigcup_\alpha M_\alpha$; при этом для каждого $\alpha \in \{\mathbf{0}, \mathbf{1}\}^n$ возможно $M_\alpha = \emptyset$. Таким образом, мы имеем дело с разбиением множества M на классы, соответствующие непустым множествам M_α . Рассмотрим фактор-множество \overline{M} множества M по этому разбиению, т.е. $\overline{M} = \{M_\alpha \mid M_\alpha \neq \emptyset, \alpha \in \{\mathbf{0}, \mathbf{1}\}^n\}$. По построению, $|\overline{M}| \leq |\{\mathbf{0}, \mathbf{1}\}^n| = 2^n$.

Определим теперь на множестве \overline{M} одноместные предикаты $P'_i(x_j)$, ($1 \leq i \leq n, 1 \leq j \leq k$) следующим образом:

$$\text{для любого } M_\alpha \in \overline{M}, P'_i(M_\alpha) = P_i(a), \text{ где } a \in M_\alpha;$$

очевидно, что значение $P'_i(M_\alpha)$ определено корректно, поскольку оно не зависит от выбора элемента a из M_α .

Рассмотрим в модели с основным множеством \overline{M} и предикатами $P'_i(x_j)$ интерпретацию ϕ' формулы F , такую, что $\phi'(P_i^{(1)}) = P'_i$, $i = 1, 2, \dots, n$. Нетрудно доказать, что тогда

$$\begin{aligned} & \mathbf{q}_1 x_1 \cdots \mathbf{q}_k x_k H(P'_1(x_1), \dots, P'_1(x_k); \dots; P'_n(x_1), \dots, P'_n(x_k)) = \\ & \mathbf{q}_1 x_1 \cdots \mathbf{q}_k x_k H(P_1(x_1), \dots, P_1(x_k); \dots; P_n(x_1), \dots, P_n(x_k)), \end{aligned}$$

т.е. $\phi'(F) = \phi(F) = \mathbf{1}$, и значит формула F выполнима на модели, основное множество \overline{M} которой содержит не более чем 2^n элементов.

СЛЕДСТВИЕ. Пусть формула F содержит только предикатные символы арности один и является истинной на всякой модели с основным множеством, не превышающем 2^n элементов, где n — число различных предикатных символов в F . Тогда формула F логически общезначима.

Доказательство. В самом деле, допустим, что F не является логически общезначимой формулой. В таком случае ее отрицание $\neg F$ выполнимо на некоторой модели. Так как $\neg F$ также удовлетворяет условиям теоремы, найдется модель с основным множеством, содержащим не более чем 2^n элементов, на которой формула $\neg F$ выполнима. Следовательно, F не может быть истинной на данной модели, а это противоречит условию следствия. Итак, предположение, что формула F не является логически общезначимой, приводит к противоречию, что и требовалось доказать.

Приведенная теорема и следствие из нее позволяют сделать вывод о разрешимости проблемы разрешения в классе формул, включающих только предикатные символы арности один. Из следствия

видно, что для того, чтобы выяснить, является ли формула F из указанного класса логически общезначимой или нет, достаточно проверить, является ли она истинной на всякой модели, основное множество которой содержит не более чем 2^n элементов. Последняя задача вполне осуществима, т.к. число таких моделей конечно и их можно перебрать за конечное время (при этом предполагается, что мы не различаем изоморфные модели). Заметим к тому же, что достаточно проверять истинность формулы F на моделях с основным множеством, состоящим в точности из 2^n элементов. Это вытекает из того, что, как нетрудно понять, всякая модель с числом элементов меньше 2^n , на которой формула F не истинна, вложима в подходящую модель мощности 2^n с таким же свойством.

В данном контексте полезно также принять во внимание следующее замечание. Пусть F содержит свободные предметные переменные x_1, x_2, \dots, x_k и мы хотим проверить ее истинность на некоторой конечной модели $\mathfrak{M} = \langle M, \mathcal{P}, \mu \rangle$ той же сигнатуры, что и F , где $M = \{a_1, a_2, \dots, a_m\}$. Для этого, очевидно, достаточно проверить истинность на \mathfrak{M} формулы $\bar{F} = \forall x_1 \forall x_2 \dots \forall x_k F(x_1, x_2, \dots, x_k)$, которая называется *замыканием* формулы F (очевидно, в \bar{F} все вхождения переменных являются связанными). Так как в запись формулы \bar{F} входят атомарные формулы только от одной переменной, \bar{F} несложными равносильными преобразованиями приводится к ФЛП, в которой логические связки соединяют лишь формулы вида $\forall xG(x)$ и $\exists xG(x)$, причем $G(x)$ не содержит переменных, отличных от x . Таким образом, нам нужно научиться вычислять истинностные значения формул $\forall xG(x)$ и $\exists xG(x)$ при их произвольной интерпретации μ в модели \mathfrak{M} , а это легко осуществляется ввиду конечности \mathfrak{M} и следующих очевидных равенств:

$$\mu(\forall xG(x)) = P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_m),$$

$$\mu(\exists xG(x)) = P(a_1) \vee P(a_2) \vee \dots \vee P(a_m);$$

здесь $P(x)$ – одноместный предикат на множестве M , соответствующий формуле $G(x)$ при интерпретации μ .

ПРИМЕР. Выяснить, являются ли ФЛП

$$F_1 = (\exists xP^{(1)}(x) \vee Q^{(1)}(y) \vee (\forall xP^{(1)}(x) \longrightarrow R^{(1)}(z)),$$

$$F_2 = P^{(1)}(x) \wedge Q^{(1)}(y) \longrightarrow (Q^{(1)}(x) \longrightarrow \forall zP^{(1)}(z))$$

логически общезначимыми или нет.

Рассмотрим замыкание

$$\bar{F}_1 = \forall y \forall z ((\exists x P^{(1)}(x)) \vee Q^{(1)}(y) \vee (\forall x P^{(1)}(x) \longrightarrow R^{(1)}(z)))$$

формулы F_1 . Имеем:

$$\begin{aligned} \bar{F}_1 &\equiv (\exists x P^{(1)}(x)) \vee \forall y \forall z (Q^{(1)}(y) \vee (\forall x P^{(1)}(x) \longrightarrow R^{(1)}(z))) \\ &\equiv (\exists x P^{(1)}(x)) \vee \forall y (Q^{(1)}(y) \vee (\forall x P^{(1)}(x) \longrightarrow \forall z R^{(1)}(z))) \\ &\equiv (\exists x P^{(1)}(x)) \vee (\forall y Q^{(1)}(y)) \vee (\forall x P^{(1)}(x) \longrightarrow \forall z R^{(1)}(z)) \\ &\equiv (\exists x P^{(1)}(x)) \vee (\forall y Q^{(1)}(y)) \vee \neg(\forall x P^{(1)}(x)) \vee \forall z R^{(1)}(z) \\ &\equiv (\exists x P^{(1)}(x)) \vee (\exists x \neg P^{(1)}(x)) \vee (\forall y Q^{(1)}(y)) \vee \forall z R^{(1)}(z) \\ &\equiv \exists x (P^{(1)}(x) \vee \neg P^{(1)}(x)) \vee \forall y Q^{(1)}(y) \vee \forall z R^{(1)}(z). \end{aligned}$$

При интерпретации μ в произвольной модели формуле $P^{(1)}(x) \vee \neg P^{(1)}(x)$ соответствует тождественно истинный предикат от переменной x , и потому $\mu(\exists x (P^{(1)}(x) \vee \neg P^{(1)}(x))) = \mathbf{1}$. Отсюда следует, что при любом μ выполнено $\mu(\bar{F}_1) = \mathbf{1}$, т.е. формула \bar{F}_1 логически общезначима. Поэтому логически общезначима и формула F_1 .

Преобразуем теперь замыкание

$$\bar{F}_2 = \forall x \forall y (P^{(1)}(x) \wedge Q^{(1)}(y) \longrightarrow (Q^{(1)}(x) \longrightarrow \forall z P^{(1)}(z)))$$

формулы F_2 :

$$\begin{aligned} \bar{F}_2 &\equiv \forall x \forall y (\neg P^{(1)}(x) \vee \neg Q^{(1)}(y) \vee \neg Q^{(1)}(x) \vee \forall z P^{(1)}(z)) \\ &\equiv \forall x (\neg P^{(1)}(x) \vee \forall y \neg Q^{(1)}(y) \vee \neg Q^{(1)}(x) \vee \forall z P^{(1)}(z)) \\ &\equiv \forall x (\neg P^{(1)}(x) \vee \neg Q^{(1)}(x)) \vee \forall y \neg Q^{(1)}(y) \vee \forall z P^{(1)}(z) \\ &\equiv \neg \exists x (P^{(1)}(x) \wedge Q^{(1)}(x)) \vee \neg \exists y Q^{(1)}(y) \vee \forall z P^{(1)}(z) = H. \end{aligned}$$

Покажем, что формула H не является логически общезначимой. Для этого ввиду доказанного выше следствия из теоремы и сделанного затем замечания мы должны найти опровергающую для H модель $\mathfrak{M} = \langle M, \{P, Q\}, \mu \rangle$, основное множество M которой содержит всего четыре элемента (т.к. $2^2 = 4$). Положим $M = \{a, b, c, d\}$ и определим одноместные предикаты P и Q на M таким образом, чтобы $\mu(\exists x (P^{(1)}(x) \wedge Q^{(1)}(x))) = \mu(\exists y Q^{(1)}(y)) = \mathbf{1}$, а $\mu(\forall z P^{(1)}(z)) = \mathbf{0}$, где $\mu(P^{(1)}) = P$ и $\mu(Q^{(1)}) = Q$. Поскольку $\mu(\exists x (P^{(1)}(x) \wedge Q^{(1)}(x))) = (P(a) \wedge Q(a)) \vee (P(b) \wedge Q(b)) \vee (P(c) \wedge Q(c)) \vee (P(d) \wedge Q(d))$, $\mu(\exists y Q^{(1)}(y)) = Q(a) \vee Q(b) \vee Q(c) \vee Q(d)$ и $\mu(\forall z P^{(1)}(z)) = P(a) \wedge P(b) \wedge P(c) \wedge P(d)$, ясно, что P и Q можно задать, например, так:

x	$P(x)$
a	1
b	0
c	1
d	1

и

x	$Q(x)$
a	1
b	1
c	1
d	1

Тогда $\mu(H) = \neg\mu(\exists x(P^{(1)}(x) \wedge Q^{(1)}(x))) \vee \neg\mu(\exists yQ^{(1)}(y)) \vee \mu(\forall zP^{(1)}(z)) = \neg \mathbf{1} \vee \neg \mathbf{1} \vee \mathbf{0} = \mathbf{0}$. Отсюда следует, что формула H и равносильная ей формула \bar{F}_2 не выполняются на данной модели $\mathfrak{M} = \langle M, \{P, Q\}, \mu \rangle$, а значит, формула F_2 не является истинной на \mathfrak{M} , т.е. F_2 не логически общезначима.

В заключение параграфа обратим внимание на то, что проблема разрешения тесным образом связана со следующей задачей: *указать универсальный алгоритм для определения по двум произвольным ФЛП, равносильны они или нет*. Как мы знаем, в логике высказываний такой алгоритм существует: это способ сравнения истинностных таблиц. В логике предикатов подобный алгоритм невозможен, поскольку вопрос о равносильности ФЛП F и G сводится, очевидно, к вопросу об общезначимости формулы $F \leftrightarrow G$, а эта задача в общем случае неразрешима. Однако при определенных ограничениях на F и G такой алгоритм существует; например, если формулы F и G содержат в своей записи только атомарные формулы от одной переменной. Последнее замечание вытекает из установленной в данном параграфе разрешимости проблемы разрешения в классе ФЛП, содержащих лишь предикатные символы арности один.

§ 2.7. Приложение логики предикатов к анализу рассуждений

В первой главе для ФЛВ было введено понятие логического следования, которое, как отмечалось, можно использовать при анализе различного рода рассуждений. Однако существует целый ряд рассуждений, правильность которых нельзя проверить, не выходя за рамки языка логики высказываний (соответствующие примеры таких рассуждений см. ниже). В связи с этим возникает необходимость в обобщении понятия логического следования на ФЛП.

Пусть Γ – некоторое множество ФЛП и F – произвольная ФЛП. Говорим, что F логически следует из Γ , если для любой модели \mathfrak{M}

формула F истинна на \mathfrak{M} как только все формулы из Γ истинны на \mathfrak{M} . При этом, как и в случае ФЛВ, будем писать $\Gamma \models F$. ФЛП называется *замкнутой*, если она не содержит свободных переменных. Так, все ФЛВ являются замкнутыми.

Заметим, что если формулы логики предикатов F и G обе замкнуты, то их равносильность эквивалентна тому, что $F \models G$ и $G \models F$. Это в общем случае не так, если какая-то из указанных формул не является замкнутой. В самом деле, для любой атомарной формулы $P^{(1)}(x)$ по нашему определению имеем $P^{(1)}(x) \models \forall x P^{(1)}(x)$ и $\forall x P^{(1)}(x) \models P^{(1)}(x)$, однако $P^{(1)}(x) \not\models \forall x P^{(1)}(x)$. Введенное нами для ФЛП понятие логического следования будет полностью адекватно (даже в случае незамкнутых формул) понятию синтаксической выводимости в теории исчисления предикатов, которое мы рассмотрим в третьей главе.

Следующее полезное утверждение обобщает теорему из §1.3. Его доказательство мы опускаем, т.к. оно незначительно отличается от соответствующего доказательства в логике высказываний.

ТЕОРЕМА. Пусть F_1, \dots, F_n, G – ФЛП, причем формулы F_1, \dots, F_n замкнуты. Тогда справедливо:

а) $F_1, \dots, F_n \models G$ в том и только в том случае, если формула $F_1 \wedge \dots \wedge F_n \longrightarrow G$ логически общезначима;

б) $F_1, \dots, F_n \models G$ в том и только в том случае, если формула $F_1 \wedge \dots \wedge F_n \wedge \neg G$ логически противоречива.

В качестве примеров установим корректность нескольких рассуждений, которые могут быть записаны на языке ФЛП.

ПРИМЕР 1. Все люди смертны. Сократ – человек. Следовательно, Сократ смертен.

Используем определение логического следования. Для этого рассмотрим произвольную модель \mathfrak{M} , на основном множестве которой заданы предикаты:

$$P(x) = \mathbf{1} \iff x \text{ – человек,}$$

$$Q(x) = \mathbf{1} \iff x \text{ – Сократ,}$$

$$S(x) = \mathbf{1} \iff x \text{ – смертен.}$$

Мы хотим проверить, что из истинности на \mathfrak{M} формул $\forall x(P(x) \longrightarrow S(x))$ и $Q(x) \longrightarrow P(x)$ вытекает истинность на \mathfrak{M} формулы $Q(x) \longrightarrow S(x)$; здесь и в других примерах для простоты вместо предикатных символов пишем в ФЛП сами предикаты. Допустим от противного, что формула $Q(x) \longrightarrow S(x)$ не истинна на

\mathfrak{M} , т.е. для некоторой ее интерпретации ϕ в данной модели имеем $\phi(Q(x) \rightarrow S(x)) = \mathbf{0}$. Это означает, что $Q(a) = \mathbf{1}$ и $S(a) = \mathbf{0}$, где $a = \phi(x)$. Из истинности на \mathfrak{M} формулы $Q(x) \rightarrow P(x)$ и равенства $Q(a) = \mathbf{1}$ получаем $P(a) = \mathbf{1}$, откуда $\phi((P(x) \rightarrow S(x)) = P(a) \rightarrow S(a) = \mathbf{1} \rightarrow \mathbf{0} = \mathbf{0}$. Но это противоречит истинности на \mathfrak{M} формулы $\forall x(P(x) \rightarrow S(x))$. Итак, мы доказали по определению, что $\forall x(P(x) \rightarrow S(x)), Q(x) \rightarrow P(x) \models Q(x) \rightarrow S(x)$, т.е. данное рассуждение правильно.

ПРИМЕР 2. Некоторые студенты любят учиться. Ни один студент не любит нравоучений. Следовательно, никакое учение не является нравоучением.

В данное рассуждение входят такие предикаты:

$$P(x) = \mathbf{1} \iff x - \text{студент,}$$

$$B(x) = \mathbf{1} \iff x - \text{учение,}$$

$$D(x) = \mathbf{1} \iff x - \text{нравоучение,}$$

$$L(x, y) = \mathbf{1} \iff x \text{ любит } y.$$

Приводимые высказывания можно записать с помощью следующих ФЛП:

$$F_1 = \exists x(P(x) \wedge \forall y(B(y) \rightarrow L(x, y))),$$

$$F_2 = \forall x(P(x) \rightarrow \forall y(D(y) \rightarrow \neg L(x, y))),$$

$$G = \forall x(B(x) \rightarrow \neg D(x)).$$

Покажем, также исходя непосредственно из определения логического следования, что $F_1, F_2 \models G$. Пусть формулы F_1 и F_2 истинны на некоторой модели. Из истинности формулы F_1 вытекает, что найдется элемент a в основном множестве модели такой, что $P(a) = \mathbf{1}$ и $\forall y(B(y) \rightarrow L(a, y)) = \mathbf{1}$. Из истинности F_2 следует, в частности, что $P(a) \rightarrow \forall y(D(y) \rightarrow \neg L(a, y)) = \mathbf{1}$ и, поскольку $P(a) = \mathbf{1}$, справедливо равенство $\forall y(D(y) \rightarrow \neg L(a, y)) = \mathbf{1}$. Отсюда и из равенства $\forall y(B(y) \rightarrow L(a, y)) = \mathbf{1}$ выводим, что предикаты $D(y) \rightarrow \neg L(a, y)$ и $B(y) \rightarrow L(a, y)$ тождественно истинны, а потому тождественно истинным является и предикат

$$\begin{aligned} & ((D(y) \rightarrow \neg L(a, y)) \wedge (B(y) \rightarrow L(a, y))) \vee \neg B(y) \vee \neg D(y) \\ & \equiv ((\neg D(y) \vee \neg L(a, y)) \wedge (\neg B(y) \vee L(a, y))) \vee \neg B(y) \vee \neg D(y) \\ & \equiv (\neg D(y) \wedge \neg B(y)) \vee (\neg L(a, y) \wedge \neg B(y)) \vee (\neg D(y) \wedge L(a, y)) \\ & \quad \vee (\neg L(a, y) \wedge L(a, y)) \vee \neg B(y) \vee \neg D(y) \\ & \equiv (\neg L(a, y) \wedge L(a, y)) \vee \neg B(y) \vee \neg D(y) \equiv \mathbf{0} \vee \neg B(y) \vee \neg D(y) \\ & \equiv \neg B(y) \vee \neg D(y) \equiv B(y) \rightarrow \neg D(y). \end{aligned}$$

Следовательно, предикат $B(x) \rightarrow \neg D(x)$ так же тождественно истинен, т.е. на данной модели истинна формула $G = \forall x(B(x) \rightarrow$

$\neg D(x)$).

Таким образом, мы доказали, что $F_1, F_2 \models G$, и значит, как это ни покажется странным, рассуждение логично.

ПРИМЕР 3. Некоторые студенты приходят на лекции всегда вовремя. Все студенты, которые поздно ложатся спать, опаздывают на лекции. Следовательно, есть студенты, которые никогда не ложатся поздно спать.

В этом рассуждении встречаются предикаты:

$P(x) = \mathbf{1} \iff x$ – студент,

$Q(x) = \mathbf{1} \iff x$ приходит на лекции всегда вовремя,

$R(x) = \mathbf{1} \iff x$ поздно ложится спать.

Соответствующие высказывания записываются в виде следующих ФЛП:

$F_1 = \exists x(P(x) \wedge Q(x))$,

$F_2 = \forall x(P(x) \longrightarrow (R(x) \longrightarrow \neg Q(x)))$,

$G = \exists x(P(x) \wedge \neg R(x))$.

Мы хотим проверить, верно ли, что $F_1, F_2 \models G$. Для этого ввиду замкнутости формул F_1 и F_2 мы можем применить приведенную выше теорему. Рассмотрим формулу $F_1 \wedge F_2 \wedge \neg G$ и докажем, что она логически противоречива. В самом деле, имеем:

$$\begin{aligned} F_1 \wedge F_2 \wedge \neg G &\equiv F_1 \wedge \forall x(P(x) \longrightarrow (R(x) \longrightarrow \neg Q(x))) \wedge \neg G \\ &\equiv F_1 \wedge \forall x(\neg P(x) \vee \neg R(x) \vee \neg Q(x)) \wedge \neg G \\ &\equiv F_1 \wedge \forall x\neg(P(x) \wedge R(x) \wedge Q(x)) \wedge \neg G \\ &\equiv F_1 \wedge \neg\exists x(P(x) \wedge R(x) \wedge Q(x)) \wedge \neg G \\ &\equiv F_1 \wedge \neg\exists x(P(x) \wedge R(x) \wedge Q(x)) \wedge \neg\exists x(P(x) \wedge \neg R(x)) \\ &\equiv F_1 \wedge \neg(\exists x(P(x) \wedge R(x) \wedge Q(x)) \vee \exists x(P(x) \wedge \neg R(x))) \\ &\equiv F_1 \wedge \neg\exists x((P(x) \wedge Q(x) \wedge R(x)) \vee (P(x) \wedge \neg R(x))) \\ &\equiv F_1 \wedge \neg\exists x((P(x) \wedge Q(x)) \vee (P(x) \wedge \neg R(x))) \\ &\equiv F_1 \wedge \neg\exists x(P(x) \wedge Q(x)) \wedge \neg\exists x(P(x) \wedge \neg R(x)) \\ &\equiv F_1 \wedge \neg F_1 \wedge \neg\exists x(P(x) \wedge \neg R(x)) \\ &\equiv \mathbf{0} \wedge \neg\exists x(P(x) \wedge \neg R(x)) \equiv \mathbf{0}. \end{aligned}$$

Отсюда в силу пункта (б) теоремы заключаем $F_1, F_2 \models G$, т.е. исследуемое рассуждение корректно.

Глава 3

Аксиоматический метод

Метод интерпретаций, основанный на понятии истинностного значения формулы, позволяет достаточно глубоко исследовать свойства логических операций – связок и кванторов. Так, с помощью этого метода мы могли выяснить, является ли та или иная ФЛП общезначимой, противоречивой или выполнимой, следует ли она логически из других заданных формул, а также являются ли две формулы равносильными, т.е. логически неразличимыми. Вместе с тем мы отмечали, что даже для решения указанных задач метод интерпретаций нельзя считать универсальным (см. §2.6). В настоящей главе будет рассмотрен еще один метод – *аксиоматический*. Он принципиально отличается от предыдущего подходом к понятию истинности формулы (точнее истинности утверждения, записанного с помощью этой формулы) и основан на естественном стремлении считать формулу истинной, если она выводима из заданного списка аксиом, т.е. является *теоремой*. В нашем случае выводимость будет означать определенное оперирование символами и выражениями некоторого формального языка. В связи с этим аксиоматический метод еще называют *синтаксическим* в отличие от метода интерпретаций, являющегося по сути своей *семантическим* (семантика – значение, смысл). Одной из основных задач данной главы будет установление тесной взаимосвязи этих методов, а в ряде важных случаев – и их полной адекватности. Мы также рассмотрим ряд проблем, естественным образом возникающих внутри аксиоматического метода, таких как проблемы полноты и непротиворечивости формальных теорий, независимости их аксиом и т.п.

§ 3.1. Формальные теории

Исходным понятием аксиоматического метода является понятие формальной теории. Полагаем, что *формальная теория* \mathcal{S} определена, если выполнены следующие условия:

(1) Задано некоторое счетное множество символов, называемое *алфавитом* теории \mathcal{S} . *Выражение* теории – это любая конечная последовательность элементов ее алфавита. Выражения в совокупности образуют *формальный язык* теории \mathcal{S} .

(2) Имеется подмножество выражений, называемых *формулами* теории \mathcal{S} .

(3) В множестве формул выделены выражения, которые называются *аксиомами* теории \mathcal{S} .

(4) Зафиксировано конечное множество R_1, \dots, R_n отношений между формулами, именуемых *правилами вывода*. При этом говорят, что формула F является *непосредственным следствием* формул $F_1, \dots, F_{k(i)}$ по правилу вывода R_i ($i = 1, 2, \dots, n$) и пишут

$$\frac{F_1, \dots, F_{k(i)}}{F},$$

если F находится в отношении R_i с $F_1, \dots, F_{k(i)}$.

Обычно подразумевается, что существуют алгоритмы, т.е. эффективные процедуры, позволяющие определить по любому выражению теории \mathcal{S} , будет ли оно формулой этой теории, а по любым формулам $F, F_1, \dots, F_{k(i)}$ и правилу R_i ($i = 1, 2, \dots, n$), будет ли F непосредственным следствием $F_1, \dots, F_{k(i)}$ по этому правилу вывода. Если к тому же существует алгоритм, распознающий среди формул данной теории аксиомы, то такая теория называется *эффективно аксиоматизированной*.

Приведем примеры формальных теорий.

ПРИМЕР 1. На обычную геометрию Евклида, изучаемую в школе, можно смотреть как на формальную теорию. В самом деле, полагаем, что алфавит этой теории включает в себя русский, греческий и латинский алфавиты, знаки препинания, знак пробела, а также общепринятые в математике символы, служащие для обозначения ряда ее понятий. Под формулами в данной теории будем понимать некоторые осмысленные выражения русского языка, а именно высказывания о свойствах тех или иных геометрических объектов (например, “*треугольник ABC – равнобедренный*”). Аксиомами теории являются обычные постулаты евклидовой геометрии.

рии, а ее правилами вывода – общеупотребительные в математике правила умозаключений (например, из формул “*треугольники ABC и DEF конгруэнтны*” и “*треугольник ABC – равнобедренный*” непосредственно следует формула “*треугольник DEF – равнобедренный*”).

ПРИМЕР 2. Определим формальную теорию \mathcal{T} , которую мы будем называть *теорией исчисления высказываний*. В самом названии этой теории угадывается связь с логикой высказываний. Позднее мы увидим, что теория \mathcal{T} является своего рода синтаксическим аналогом семантической логики высказываний.

(1) Алфавит теории \mathcal{T} состоит из логических связок \neg , \longrightarrow , скобок $(,)$ и букв A, B, C, \dots (этими же буквами в логике высказываний обозначались логические переменные).

(2) Конечную последовательность элементов данного алфавита будем называть формулой теории \mathcal{T} , если она является ФЛВ. Например, выражения $(\neg A \longrightarrow B) \longrightarrow \neg\neg B$ и $\neg(A \longrightarrow \neg B)$ суть формулы теории \mathcal{T} , в то время как выражения $\neg(A \vee B) \vee \neg\neg B$ и $A \wedge B$ формулами этой теории, вообще говоря, не являются, так как символы \vee и \wedge не входят в ее алфавит. Это ничуть не противоречит высказанному выше тезису об адекватности теории \mathcal{T} логике высказываний, поскольку, как известно, всякая ФЛВ равносильна формуле, содержащей лишь связки \neg и \longrightarrow (см. §1.5); в целях сокращения записи формул теории \mathcal{T} мы по определению можем считать, что $A \wedge B$ означает $\neg(A \longrightarrow \neg B)$, а $A \vee B$ означает $\neg A \longrightarrow B$.

(3) Для произвольных формул F, G и H теории \mathcal{T} следующие формулы суть аксиомы:

$$(A1) \quad F \longrightarrow (G \longrightarrow F);$$

$$(A2) \quad (F \longrightarrow (G \longrightarrow H)) \longrightarrow ((F \longrightarrow G) \longrightarrow (F \longrightarrow H));$$

$$(A3) \quad (\neg G \longrightarrow \neg F) \longrightarrow ((\neg G \longrightarrow F) \longrightarrow G).$$

Таким образом, в теории \mathcal{T} имеется бесконечное множество аксиом, каждая из которых получается подстановкой в одну из схем аксиом (A1), (A2), (A3) вместо F, G и H некоторых формул. Легко проверить, что все аксиомы теории \mathcal{T} являются тавтологиями. Это одно из необходимых условий, которыми мы руководствуемся при их выборе. Другое необходимое условие – это полнота данной системы аксиом; более подробно об этом будет сказано ниже.

(4) Единственным правилом вывода теории \mathcal{T} служит правило *modus ponens* (сокращенно MP):

$$\frac{F, F \rightarrow G}{G},$$

которое утверждает, что формула G есть непосредственное следствие формул F и $F \rightarrow G$. Например, подставляя $\neg A$ вместо F и $B \rightarrow \neg C$ вместо G , получаем, что

$$\frac{\neg A, \neg A \rightarrow (B \rightarrow \neg C)}{B \rightarrow \neg C} \text{ (MP)}.$$

Итак, теория \mathcal{T} исчисления высказываний определена. Отметим, что \mathcal{T} эффективно аксиоматизирована, поскольку для любой ее формулы легко проверить, будет ли она аксиомой.

Одним из основных понятий аксиоматического метода является понятие [синтаксической] выводимости. Пусть задана произвольная формальная теория \mathcal{S} . Говорим, что формула F есть *следствие в \mathcal{S} множества формул Γ* (или *F выводится в \mathcal{S} из Γ*), если существует последовательность F_1, \dots, F_n формул такая, что $F_n = F$ и для любого i формула F_i есть либо аксиома теории \mathcal{S} , либо элемент Γ , либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода. В этом случае последовательность F_1, \dots, F_n формул называется *выводом F из Γ* . Формулы множества Γ называются *гипотезами* или *посылками* вывода. Если F выводится в \mathcal{S} из Γ , то мы употребляем запись $\Gamma \vdash_{\mathcal{S}} F$; при этом мы будем также писать $\Gamma \vdash F$, если ясно, о какой теории идет речь.

ПРИМЕР 3. Проверить, что $A \rightarrow (B \rightarrow C)$, $A \rightarrow B \vdash_{\mathcal{T}} A \rightarrow C$.

Построим вывод в теории \mathcal{T} формулы $A \rightarrow C$ из формул $A \rightarrow (B \rightarrow C)$ и $A \rightarrow B$:

- (1) $A \rightarrow (B \rightarrow C)$ (гипотеза)
- (2) $A \rightarrow (B \rightarrow C) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ (схема аксиом (A2))
- (3) $(A \rightarrow B) \rightarrow (A \rightarrow C)$ (из (1), (2) по MP)
- (4) $A \rightarrow B$ (гипотеза)
- (5) $A \rightarrow C$ (из (3), (4) по MP)

Следующее утверждение включает несколько простых, но очень важных свойств выводимости.

ПРЕДЛОЖЕНИЕ. (1) Если $\Gamma \vdash F$ и $\Gamma \subseteq \Delta$, то $\Delta \vdash F$.

(2) Если $\Gamma \vdash F$ и $\Delta \vdash G$ для любой формулы G из множества Γ , то $\Delta \vdash F$.

(3) $\Gamma \vdash F$ тогда и только тогда, когда в Γ существует конечное подмножество Δ , для которого $\Delta \vdash F$.

Доказательство. (1) Условие $\Gamma \vdash F$ означает, что существует вывод F_1, \dots, F_n формулы F из множества формул Γ . Если $\Gamma \subseteq \Delta$, то эту же последовательность формул F_1, \dots, F_n можно взять в качестве вывода F из Δ и, следовательно, будем иметь $\Delta \vdash F$.

(2) Пусть $\Gamma \vdash F$. Тогда существует последовательность формул F_1, \dots, F_n такая, что $F_n = F$ и для любого i формула F_i есть либо аксиома, либо гипотеза (т.е. элемент Γ), либо получается из предыдущих формул по одному из правил вывода. Пусть к тому же $\Delta \vdash G$, если $G \in \Gamma$, т.е. для каждой формулы множества гипотез Γ найдется ее вывод из Δ . Заменим в выводе F_1, \dots, F_n формулы F из Γ каждую гипотезу ее выводом из Δ . Получим последовательность формул, которая, очевидно, будет выводом F из Δ , а значит, $\Delta \vdash F$.

(3) Пусть $\Gamma \vdash F$. Вывод F из Γ содержит лишь конечное подмножество гипотез, которое мы и обозначим через Δ . Тогда, очевидно, выполнено $\Delta \vdash F$. Обратно, если $\Delta \vdash F$ и $\Delta \subseteq \Gamma$, то в силу доказанного свойства (1) имеем $\Gamma \vdash F$.

Формула F теории \mathcal{S} называется *теоремой*, если она выводится в \mathcal{S} из пустого множества гипотез, т.е. $\emptyset \vdash_{\mathcal{S}} F$. Другими словами, F – теорема теории \mathcal{S} , если существует последовательность формул F_1, \dots, F_n такая, что $F_n = F$ и для любого i формула F_i есть либо аксиома теории \mathcal{S} , либо непосредственное следствие каких-то предыдущих формул по одному из правил вывода. В этом случае цепочка формул F_1, \dots, F_n называется *выводом* или *доказательством* теоремы F . В целях экономии места принято опускать в записи $\emptyset \vdash_{\mathcal{S}} F$ знак пустого множества и писать $\vdash_{\mathcal{S}} F$ или $\vdash F$, если ясно, теоремой какой теории является формула F .

ПРИМЕР 4. Показать, что $\vdash_{\mathcal{T}} F \longrightarrow F$ для любой формулы F теории \mathcal{T} .

Построим доказательство теоремы $F \longrightarrow F$ в \mathcal{T} :

(1) $F \longrightarrow ((F \longrightarrow F) \longrightarrow F)$ (подстановка в схему аксиом (A1))

(2) $(F \rightarrow ((F \rightarrow F) \rightarrow F)) \rightarrow ((F \rightarrow (F \rightarrow F)) \rightarrow (F \rightarrow F))$ (подстановка в схему аксиом (A2))

(3) $(F \rightarrow (F \rightarrow F)) \rightarrow (F \rightarrow F)$ (из (1), (2) по МР)

(4) $(F \rightarrow (F \rightarrow F))$ (схема аксиом (A1))

(5) $F \rightarrow F$ (из (3), (4) по МР)

ПРИМЕР 5. Доказать, что в теории \mathcal{T} всякая теорема является тавтологией.

Действительно, заметим сначала, что для любых формул F и G теории \mathcal{T} из того, что F и $F \rightarrow G$ суть тавтологии, вытекает, что и G – тавтология. Поэтому свойство формул теории \mathcal{T} “*быть тавтологией*” сохраняется при применении к ним правила вывода МР. Отсюда, поскольку каждая теорема теории \mathcal{T} получается из аксиом с помощью правила МР, а все аксиомы в \mathcal{T} суть тавтологии, заключаем, что и все теоремы в \mathcal{T} являются тавтологиями.

Естественна постановка вопроса о справедливости обратного утверждения: *будет ли всякая тавтология теоремой теории \mathcal{T} ?* Как мы увидим, ответ на этот вопрос оказывается положительным. Иначе говоря, список аксиом теории \mathcal{T} является “достаточно полным” для того, чтобы из него выводилась любая тавтология. В этом состоит смысл так называемой *теоремы о полноте* для теории \mathcal{T} исчисления высказываний. Эта теорема будет доказана нами в гораздо более общем случае, охватывающем широкий класс формальных теорий. Их мы начинаем изучать в следующем параграфе.

§ 3.2. Теории первого порядка. Теорема о непротиворечивости

Определим произвольную *теорию первого порядка \mathcal{K}* .

(1) Алфавит теории \mathcal{K} включает логические связки \neg, \rightarrow ; знак квантора общности \forall ; скобки $(,)$; запятую $,$ (вводимую нами для облегчения чтения формул); счетное множество предметных переменных x, y, z, \dots (возможно, индексированных); непустое конечное или счетное множество предикатных символов $P^{(n)}, Q^{(n)}, S^{(n)}, \dots (n \geq 0)$; а также конечное (возможно и пустое) или счетное множество *функциональных символов* $f^{(n)}, g^{(n)}, h^{(n)}, \dots (n \geq 0)$. Как мы знаем из содержания второй главы, предикатным символам при интерпретациях формул соответствуют конкретные предикаты на множествах. Но

на множествах помимо предикатов можно рассматривать и различные операции*; они и будут соответствовать функциональным символам при интерпретациях. Предикатные и функциональные символы в совокупности образуют *сигнатуру* $\Sigma(\mathcal{K}) = \{P^{(n)}, Q^{(n)}, S^{(n)}, \dots; f^{(n)}, g^{(n)}, h^{(n)}, \dots\}$ теории \mathcal{K} .

(2) Прежде чем дать определение формулы теории \mathcal{K} , введем понятие ее *терма*.

(1') предметные переменные x, y, z, \dots , а также нульарные функциональные символы $f^{(0)}, g^{(0)}, h^{(0)}, \dots$ из $\Sigma(\mathcal{K})$ (если они есть) суть термы теории \mathcal{K} ;

(2') для произвольного функционального символа $f^{(n)} \in \Sigma(\mathcal{K})$ ($n \geq 1$) и термов t_1, \dots, t_n теории \mathcal{K} выражение вида $f^{(n)}(t_1, \dots, t_n)$ тоже есть терм этой теории;

(3') других термов нет.

Теперь мы можем определить формулы теории \mathcal{K} :

(1'') выражения вида $P^{(0)}$ и $P^{(n)}(t_1, \dots, t_n)$ суть формулы; здесь $P^{(0)}$ и $P^{(n)}$ – предикатные символы из $\Sigma(\mathcal{K})$, а t_1, \dots, t_n – произвольные термы теории \mathcal{K} ; такие формулы называются *атомарными*;

(2'') если F и G – формулы, то выражения вида $\neg F$, $(F \rightarrow G), \forall x F$ также являются формулами;

(3'') других формул нет.

Как обычно, мы будем опускать некоторые скобки для сокращения записи формул. При этом будем писать $F \wedge G$ вместо $\neg(F \rightarrow \neg G)$, $F \vee G$ вместо $\neg F \rightarrow G$ и $\exists x F$ вместо $\neg \forall x \neg F$. Так же как и в случае ФЛП, определим понятия свободной и связанной переменной и свободного и связанного вхождения переменной в формуле (см. §2.3).

(3) Аксиомы теории \mathcal{K} разбиваются на два класса: *логические аксиомы* и *собственные аксиомы*.

Логические аксиомы подразделяются на пять схем (A1)–(A5), которые справедливы для любой теории первого порядка. Первые три из них аналогичны схемам аксиом теории \mathcal{T} исчисления высказываний:

$$(A1) F \rightarrow (G \rightarrow F);$$

$$(A2) (F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H));$$

$$(A3) (\neg G \rightarrow \neg F) \rightarrow ((\neg G \rightarrow F) \rightarrow G);$$

* Напомним, что n -арной операцией на множестве M называется любое отображение $M^n \rightarrow M$. Нульарные операции – это выделенные элементы из M .

здесь F, G и H – произвольные формулы теории \mathcal{K} .

Следующая схема аксиом имеет вид:

$$(A4) \quad \forall x(F \longrightarrow G) \longrightarrow (F \longrightarrow \forall xG),$$

где формула F не содержит свободных вхождений x .

Для определения схемы (A5) нам понадобится понятие термина, свободного для данной переменной в формуле. Пусть $F(x)$ – формула теории \mathcal{K} , где x – какая-то свободная в F переменная и t – некоторый терм теории \mathcal{K} . Обозначим через $F(t)$ формулу, получающуюся из $F(x)$ заменой каждого свободного вхождения переменной x термом t . Терм t называется *свободным для переменной x в формуле $F(x)$* , если в формуле $F(t)$ никакое вхождение термина t (полученное указанным выше способом) не содержит связанных вхождений переменных. Так например, для переменной x в формуле $F(x, z) = \forall yP^{(3)}(x, y, z) \longrightarrow \forall x\forall zQ^{(2)}(x, z)$ терм $t_1 = f^{(2)}(x, z)$ свободен, а терм $t_2 = f^{(2)}(x, y)$ нет, поскольку $F(t_1, z) = \forall yP^{(3)}(f^{(2)}(x, z), y, z) \longrightarrow \forall x\forall zQ^{(2)}(x, z)$, а $F(t_2, z) = \forall yP^{(3)}(f^{(2)}(x, y), y, z) \longrightarrow \forall x\forall zQ^{(2)}(x, z)$, и в последнем случае вхождение термина t_2 в формуле $F(t_2, z)$ содержит связанную переменную y .

Приведем теперь последнюю схему логических аксиом:

$$(A5) \quad \forall xF(x) \longrightarrow F(t),$$

где $F(x)$ – произвольная формула теории \mathcal{K} и t – терм теории \mathcal{K} , свободный для x в $F(x)$. При $t = x$ мы получаем одну из логических аксиом $\forall xF(x) \longrightarrow F(x)$. Мы также включаем в указанную схему логических аксиом формулы вида $\forall xF \longrightarrow F$, где переменная x не встречается в записи формулы F или все ее вхождения в F связаны.

Логические аксиомы должны подчиняться необходимому условию: быть истинными при любой интерпретации. Ограничения, наложенные на формулы в схемах (A4), (A5), объясняются именно этим требованием.

Собственные аксиомы сформулировать в общем случае нельзя, так как они индивидуальны для каждой теории первого порядка.

(4) В теории \mathcal{K} имеются два правила вывода: знакомое нам уже *modus ponens* $\frac{F, F \longrightarrow G}{G}$ (MP) и, новое, *правило обобщения* $\frac{F}{\forall xF}$ (ПО).

Как видно из определения, две теории первого порядка могут отличаться друг от друга лишь множеством предикатных и функциональных символов, т.е. сигнатурой, и множеством собственных аксиом. Поэтому для того, чтобы задать конкретную теорию первого порядка, достаточно указать ее сигнатуру и собственные аксиомы.

Как и в логике предикатов, формулу теории \mathcal{K} будем называть замкнутой, если она не содержит свободных переменных. Для каждой формулы $F = F(x_1, \dots, x_k)$ теории \mathcal{K} , где x_1, \dots, x_k – все свободные переменные в F , можно построить ее замыкание $\bar{F} = \forall x_1 \cdots \forall x_k F(x_1, \dots, x_k)$. Ясно, что формула F замкнута тогда и только тогда, когда $F = \bar{F}$.

Следующий пример демонстрирует одно полезное свойство выводимости в теориях первого порядка, позволяющее во многих рассуждениях ограничиваться рассмотрением замкнутых формул.

ПРИМЕР 1. Пусть Γ – некоторое множество формул теории первого порядка и F – произвольная формула. Показать, что $\Gamma \vdash F$ тогда и только тогда, когда $\Gamma \vdash \bar{F}$; в частности, выполнено $F \vdash \bar{F}$ и $\bar{F} \vdash F$.

Действительно, для любой свободной в F переменной x имеем по правилу обобщения $F \vdash \forall x F$. С другой стороны, последовательность формул $F_1 = \forall x F$, $F_2 = \forall x F \rightarrow F$, $F_3 = F$ является выводом F из формулы $\forall x F$, и значит, $\forall x F \vdash F$; здесь F_1 – гипотеза, F_2 – аксиома из схемы (A5), F_3 – непосредственное следствие формул F_1 и F_2 по правилу МР. Теперь остается выписать цепочку эквивалентностей: $\Gamma \vdash F(x_1, \dots, x_k) \iff \Gamma \vdash \forall x_k F(x_1, \dots, x_k) \iff \Gamma \vdash \forall x_{k-1} \forall x_k F(x_1, \dots, x_k) \iff \dots \iff \Gamma \vdash \forall x_1 \cdots \forall x_{k-1} \forall x_k F(x_1, \dots, x_k)$, т.е. $\Gamma \vdash F \iff \Gamma \vdash \bar{F}$.

Пусть Σ – произвольная сигнатура и M – непустое множество, на котором определены некоторые предикаты и операции, образующие соответственно множества \mathcal{P} и \mathcal{F} . Пусть к тому же задано отображение $\mu : \Sigma \rightarrow \mathcal{P} \cup \mathcal{F}$, ставящее в соответствие каждому n -арному предикатному символу из Σ какой-либо предикат из \mathcal{P} , а n -арному функциональному символу – какую-либо n -арную операцию из \mathcal{F} . Тогда четырехэлементное множество $\mathfrak{M} = \langle M, \mathcal{P}, \mathcal{F}, \mu \rangle$ называется *алгебраической системой* сигнатуры Σ ; при этом M называется *основным множеством* системы \mathfrak{M} . Например, множество натуральных чисел \mathbb{N} с естественным предикатом (отношением) линейного порядка \leq и операциями сложения $+$ и умноже-

ния \cdot образует алгебраическую систему $\langle \mathbf{N}, \leq, \{+, \cdot\}, \mu \rangle$ сигнатуры $\Sigma = \{P^{(2)}, f^{(2)}, g^{(2)}\}$, где $\mu(P^{(2)}) = “\leq”$, $\mu(f^{(2)}) = “+”$, $\mu(g^{(2)}) = “\cdot”$. Две алгебраические системы мы не различаем, если они *изоморфны*, т.е. если существует взаимно однозначное отображение основного множества одной из них на основное множество другой, сохраняющее операции и предикаты.

Рассмотрим произвольную теорию первого порядка \mathcal{K} . Пусть $F(x_1, \dots, x_k)$ – некоторая формула этой теории, где x_1, \dots, x_k – все свободные предметные переменные в F , и $\mathfrak{M} = \langle M, \mathcal{P}, \mathcal{F}, \mu \rangle$ – некоторая алгебраическая система сигнатуры $\Sigma(\mathcal{K})$. *Интерпретацией формулы F в системе \mathfrak{M}* называется отображение $\tilde{\mu} : \{x_1, \dots, x_k\} \cup \Sigma(\mathcal{K}) \rightarrow M \cup \mathcal{P} \cup \mathcal{F}$, переводящее переменные x_1, \dots, x_k в элементы основного множества M и совпадающее с μ на $\Sigma(\mathcal{K})$. Подобно тому как вычислялись истинностные значения ФЛП (см. §2.3), для каждой интерпретации $\tilde{\mu}$ формулы F в системе \mathfrak{M} находится значение $\tilde{\mu}(F) \in \{\mathbf{0}, \mathbf{1}\}$. Новое для нас заключается лишь в том, что надо научиться сначала вычислять *значения термов* при интерпретации. Для любого термина t теории \mathcal{K} индукцией по его длине определим $\tilde{\mu}(t) \in M$:

(1') если t – предметная переменная или нульарный функциональный символ, то $\tilde{\mu}(t)$ уже известно;

(2') если $t = f^{(n)}(t_1, \dots, t_n)$, то $\tilde{\mu}(t) = f(a_1, \dots, a_n)$, где $f = \tilde{\mu}(f^{(n)})$ и $a_i = \tilde{\mu}(t_i)$, $i = 1, \dots, n$.

Теперь индукцией по длине формулы F определим $\tilde{\mu}(F) \in \{\mathbf{0}, \mathbf{1}\}$:

(1'') пусть F – атомарная формула; тогда если F – нульарный предикатный символ, то $\tilde{\mu}(F)$ уже известно и совпадает с $\mu(F)$; если же $F = P^{(n)}(t_1, \dots, t_n)$, то $\tilde{\mu}(F) = P(a_1, \dots, a_n)$, где $P = \tilde{\mu}(P^{(n)})$ и $a_i = \tilde{\mu}(t_i)$, $i = 1, \dots, n$;

(2'') если $F = \neg G$ или $F = G \rightarrow H$, то соответственно $\tilde{\mu}(F) = \neg \tilde{\mu}(G)$ или $\tilde{\mu}(F) = \tilde{\mu}(G) \rightarrow \tilde{\mu}(H)$;

(3'') если $F = \forall x G$, то $\tilde{\mu}(F) = \mathbf{1}$ тогда и только тогда, когда для любой интерпретации η формулы G в \mathfrak{M} , совпадающей с $\tilde{\mu}$ на $\Sigma(\mathcal{K})$ и на всех отличных от x свободных переменных из G , выполнено $\eta(G) = \mathbf{1}$.

Формула F называется *истинной на системе \mathfrak{M}* , если она истинна при любой интерпретации в этой системе.

Моделью теории первого порядка \mathcal{K} называется всякая алгебраическая система сигнатуры $\Sigma(\mathcal{K})$, на которой истинны все собствен-

ные аксиомы теории \mathcal{K} . Заметим, что в данном определении слово “собственные” можно опустить, поскольку логические аксиомы теории \mathcal{K} “по своей природе” истинны на любой системе сигнатуры $\Sigma(\mathcal{K})^\dagger$, а значит, и на любой модели теории \mathcal{K} .

ПРИМЕР 2. Для теории \mathcal{K} первого порядка, заданной своей сигнатурой $\Sigma(\mathcal{K})$ и собственными аксиомами A_1, A_2 , выяснить, будет ли моделью этой теории алгебраическая система \mathfrak{M} :

(1) $\Sigma(\mathcal{K}) = \{P^{(2)}, f^{(1)}\}$, $A_1 = \forall x P^{(2)}(x, x)$, $A_2 = \forall x P^{(2)}(x, f^{(1)}(x))$; $\mathfrak{M} = \langle \mathbf{R}, P, f, \mu \rangle$, где \mathbf{R} – множество действительных чисел, $P(x, y) = \mathbf{1} \iff x \leq y$, $f(x) = x + 1$ и $\mu(P^{(2)}) = P$, $\mu(f^{(1)}) = f$.

(2) $\Sigma(\mathcal{K}) = \{P^{(2)}, f^{(2)}\}$, $A_1 = \forall x \forall y \forall z (P^{(2)}(x, y) \longrightarrow P^{(2)}(f^{(2)}(x, z), f^{(2)}(y, z)))$, $A_2 = \exists x \forall y P^{(2)}(x, y)$; $\mathfrak{M} = \langle \mathbf{Z}, P, f, \mu \rangle$, где \mathbf{Z} – множество целых чисел, $P(x, y) = \mathbf{1} \iff x \leq y$, $f(x, y) = x + y$ и $\mu(P^{(2)}) = P$, $\mu(f^{(2)}) = f$.

Надо проверить истинность аксиом A_1 и A_2 на системе \mathfrak{M} . Для этого проще применить не формальное определение истинностного значения формулы, приведенное выше, а правило, аналогичное тому, которым мы пользовались при вычислении значений ФЛП (см. пример 2 из §2.3). Так как указанные аксиомы не содержат свободных предметных переменных, для каждой из них имеется единственная интерпретация в системе \mathfrak{M} , совпадающая с отображением $\mu : \Sigma(\mathcal{K}) \longrightarrow \{P, f\}$. При данной интерпретации в случае (1) аксиомам A_1 и A_2 соответствуют истинные высказывания: “для любого $x \in \mathbf{R} : x \leq x$ ” и “для любого $x \in \mathbf{R} : x \leq x + 1$ ”. Поэтому $\mu(A_1) = \mathbf{1}$ и $\mu(A_2) = \mathbf{1}$, а значит, система \mathfrak{M} является моделью теории \mathcal{K} .

В случае (2) аксиомы A_1 и A_2 заданной интерпретацией переводятся соответственно в высказывания “для любых $x, y, z \in \mathbf{Z}$ условие $x \leq y$ влечет за собой $x + z \leq y + z$ ” и “существует $x \in \mathbf{Z}$ такой, что для любого $y \in \mathbf{Z} : x \leq y$ ”. Второе высказывание о наличии наименьшего целого числа неверно. Поэтому $\mu(A_2) = \mathbf{0}$ и, несмотря на то, что $\mu(A_1) = \mathbf{1}$, данная система моделью теории \mathcal{K} не является.

Приведем теперь ряд важных примеров теорий первого порядка, а также укажем, какие системы будут для них моделями.

[†]Попытайтесь сами проверить этот не совсем очевидный тезис.

ПРИМЕР 3. Теория \mathcal{T} исчисления высказываний может быть задана как теория первого порядка. Ее сигнатура – это счетное множество нульарных предикатных символов, которые мы раньше называли логическими переменными. Собственных аксиом \mathcal{T} не имеет. Так как формулы этой теории не содержат предметных переменных, отпадает необходимость в кванторах, и потому в определении \mathcal{T} достаточно было ограничиться тремя схемами (A1)–(A3) логических аксиом. Моделью теории \mathcal{T} является любое непустое множество с заданными на нем нульместными предикатами $\mathbf{0}$ и $\mathbf{1}$.

ПРИМЕР 4. Теория исчисления предикатов – это теория первого порядка без собственных аксиом, сигнатура которой содержит счетные наборы символов предикатов любой арности и не содержит функциональных символов. Ее модели – это модели логики предикатов данной сигнатуры, а формулы суть ФЛП.

ПРИМЕР 5. Теория [строго] частично упорядоченных множеств. Ее сигнатура состоит из единственного предикатного символа $P^{(2)}$. Вместо $P^{(2)}(x, y)$ и $\neg P^{(2)}(x, y)$ будем использовать более привычные обозначения $x < y$ и $x \not< y$ соответственно. Данная теория имеет две собственные аксиомы:

- (а) $\forall x(x \not< x)$ (аксиома антирефлексивности);
- (б) $\forall x\forall y\forall z(x < y \wedge y < z \longrightarrow x < z)$ (аксиома транзитивности).

Моделями для нее являются [строго] частично упорядоченные множества.

ПРИМЕР 6. Теория групп. Ее сигнатура имеет один предикатный символ $P^{(2)}$ и два функциональных символа $f^{(0)}$, $f^{(2)}$. В соответствии с обычными обозначениями, мы будем писать $t = s$ вместо $P^{(2)}(t, s)$, $t \cdot s$ вместо $f^{(2)}(t, s)$ и символ единичного элемента e вместо $f^{(0)}$. Тогда собственные аксиомы этой теории примут вид:

- (а) $\forall x\forall y\forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$ (аксиома ассоциативности);
- (б) $\forall x(e \cdot x = x \cdot e = x)$ (свойство единичного элемента);
- (в) $\forall x\exists y(y \cdot x = x \cdot y = e)$ (существование обратного элемента);
- (г) $\forall x(x = x)$ (рефлексивность равенства);
- (д) $\forall x\forall y\forall z(x = y \wedge y = z \longrightarrow x = z)$ (транзитивность равенства);
- (е) $\forall x\forall y(x = y \longrightarrow y = x)$ (симметричность равенства);
- (ж) $\forall x\forall y\forall z(x = y \longrightarrow z \cdot x = z \cdot y \wedge x \cdot z = y \cdot z)$ (подстановочность равенства).

Моделями данной теории являются группы.

В дальнейшем через \mathcal{K} мы всегда будем обозначать некоторую теорию первого порядка.

Обобщим теперь понятие логического следования, введенное для ФЛП, на формулы произвольной теории \mathcal{K} . Будем говорить, что формула F *логически следует в \mathcal{K}* из множества формул Γ , если для любой модели \mathfrak{M} теории \mathcal{K} из того, что все формулы из Γ истинны на \mathfrak{M} , вытекает, что и F истинна на \mathfrak{M} . В этом случае так же будем писать $\Gamma \models F$ (или $\Gamma \models_{\mathcal{K}} F$, если мы хотим подчеркнуть, что речь идет о теории \mathcal{K}). Формула F называется *логически общезначимой в \mathcal{K}* , если она истинна на любой модели теории \mathcal{K} . Это равносильно тому, что F логически следует в \mathcal{K} из пустого множества формул, т.е. выполнено $\models_{\mathcal{K}} F$. Данное понятие обобщает понятие логической общезначимости, которое мы вводили для ФЛП. Из определения модели теории \mathcal{K} непосредственно видно, что *все аксиомы теории \mathcal{K} логически общезначимы в ней*.

Заметим, что из пункта (3) определения истинностного значения формулы следует, что формула F истинна на системе \mathfrak{M} тогда и только тогда, когда формула вида $\forall xF$ истинна на \mathfrak{M} . Отсюда, навешивая последовательно кванторы общности на свободные переменные из F , получаем, что F истинна на \mathfrak{M} тогда и только тогда, когда ее замыкание \bar{F} истинно на \mathfrak{M} . Поэтому *логическая общезначимость формулы F в теории \mathcal{K} равносильна логической общезначимости в \mathcal{K} формулы \bar{F}* .

Следующее утверждение указывает на прямую связь между синтаксическим понятием выводимости и семантическим понятием логического следования.

ПРЕДЛОЖЕНИЕ. Пусть Γ – некоторое множество формул теории \mathcal{K} и F – произвольная формула. Тогда условие $\Gamma \vdash_{\mathcal{K}} F$ влечет за собой $\Gamma \models_{\mathcal{K}} F$.

Доказательство. Пусть $\Gamma \vdash_{\mathcal{K}} F$, т.е. существует последовательность формул F_1, \dots, F_n такая, что $F_n = F$ и каждая формула F_i есть либо аксиома теории \mathcal{K} , либо гипотеза, либо непосредственное следствие формул с меньшими номерами по одному из правил вывода – МР или ПО. Надо установить, что для любой модели \mathfrak{M} теории \mathcal{K} формула F истинна на \mathfrak{M} , как только все гипотезы из Γ истинны на \mathfrak{M} . Докажем это индукцией по длине n вывода F из Γ . Поскольку F_1 является либо аксиомой (и потому логически общезначимой в \mathcal{K} формулой), либо гипотезой, формула F_1 истинна на \mathfrak{M} . Предположим, что утверждение доказано для всех $i < n$

и проверим истинность на \mathfrak{M} формулы F_n . При этом достаточно разобрать случай, когда F_n получается из предыдущих формул по МР или ПО. Пусть, например, $\frac{F_i, F_j}{F_n}$ (МР), где $i, j < n$ и формула F_j имеет вид $F_i \rightarrow F_n$. Тогда, по предположению индукции, для любой интерпретации ϕ формул F_i и $F_i \rightarrow F_n$ в модели \mathfrak{M} выполнено $\phi(F_i) = \mathbf{1}$ и $\phi(F_i \rightarrow F_n) = \mathbf{1}$, а значит, выполнено и $\phi(F_n) = \mathbf{1}$, т.е. формула F_n истинна на \mathfrak{M} . Если же $\frac{F_i}{F_n}$ (ПО), где $i < n$ и $F_n = \forall x F_i$, то из истинности F_i на \mathfrak{M} следует истинность на \mathfrak{M} и формулы F_n . Предложение доказано.

Полагая в условии предложения $\Gamma = \emptyset$, получим

СЛЕДСТВИЕ. *Любая теорема теории первого порядка логически общезначима: если $\vdash F$, то $\models F$.*

Говорят, что множество Γ формул теории \mathcal{K} имеет модель в \mathcal{K} , если все формулы из Γ истинны на некоторой модели теории \mathcal{K} .

Множество Γ формул теории \mathcal{K} называется *противоречивым* в \mathcal{K} , если существует замкнутая формула F этой теории такая, что $\Gamma \vdash_{\mathcal{K}} F$ и, одновременно, $\Gamma \vdash_{\mathcal{K}} \neg F$. В противном случае говорят, что Γ *непротиворечиво* в \mathcal{K} .

Следующая теорема дает важное достаточное условие непротиворечивости.

ТЕОРЕМА О НЕПРОТИВОРЕЧИВОСТИ. *Если множество формул теории первого порядка имеет модель, то оно непротиворечиво.*

Доказательство. Пусть множество формул Γ имеет модель \mathfrak{M} в теории \mathcal{K} . Если бы Γ было противоречивым, то нашлась бы замкнутая формула F в \mathcal{K} такая, что $\Gamma \vdash_{\mathcal{K}} F$ и $\Gamma \vdash_{\mathcal{K}} \neg F$. Отсюда, в силу доказанного выше предложения, выполнялось бы $\Gamma \models_{\mathcal{K}} F$ и $\Gamma \models_{\mathcal{K}} \neg F$. Тогда, поскольку формулы из Γ истинны на модели \mathfrak{M} , истинными на \mathfrak{M} должны быть обе формулы F и $\neg F$. Получили противоречие, доказывающее теорему.

Установленная в этом параграфе зависимость между понятиями выводимости и логического следования и, в частности, между понятиями теоремы и логически общезначимой формулы помогает оправдать выбор набора логических аксиом и правил вывода для теорий первого порядка. Мы полностью обоснуем его, если докажем, что в любой теории первого порядка класс теорем совпадает с классом общезначимых формул и, более того, понятие логического

следования совпадает с понятием выводимости. Этому и посвящены следующие три параграфа.

§ 3.3. Теорема о дедукции

Теорема о дедукции, доказанная французским математиком Жаком Эрбраном в 1930 году, является первым существенным шагом, приближающим нас к поставленной цели. Из логики предикатов (см. §2.7) мы знаем, что условие $F \models G$ равносильно общезначимости формулы $F \longrightarrow G$, т.е. условию $\models F \longrightarrow G$; здесь F — замкнутая формула. Очевидно, этим свойством обладают формулы любой теории первого порядка. Оказывается, нечто подобное имеет место и в том случае, если знак \models логического следования заменить на знак \vdash выводимости, а именно, справедлива следующая

ТЕОРЕМА О ДЕДУКЦИИ. Пусть Γ — некоторое множество формул теории первого порядка и F, G — какие-то формулы, причём F замкнута. Тогда $\Gamma \cup \{F\} \vdash G$ в том и только в том случае, если $\Gamma \vdash F \longrightarrow G$.

Доказательство. Довольно легко проверяется, что условие $\Gamma \vdash F \longrightarrow G$ влечет за собой $\Gamma \cup \{F\} \vdash G$. В самом деле, если $\Gamma \vdash F \longrightarrow G$, то существует вывод F_1, \dots, F_n формулы $F \longrightarrow G$ из Γ . Добавив к нему две новые формулы $F_{n+1} = F$ и $F_{n+2} = G$, получим вывод $F_1, \dots, F_n = F \longrightarrow G, F_{n+1} = F, F_{n+2} = G$ формулы G из множества формул $\Gamma \cup \{F\}$; здесь F_{n+1} — гипотеза, а F_{n+2} — непосредственное следствие формул F_n, F_{n+1} по правилу МР.

Обратное утверждение менее тривиально. Пусть $\Gamma \cup \{F\} \vdash G$, т.е. существует последовательность формул F_1, \dots, F_n такая, что $F_n = G$ и для любого i формула F_i есть либо аксиома, либо гипотеза (т.е. $F_i \in \Gamma$ или $F_i = F$), либо непосредственное следствие каких-то предыдущих формул по одному из правил вывода. Докажем индукцией по i ($i = 1, 2, \dots, n$), что $\Gamma \vdash F \longrightarrow F_i$.

БАЗА ИНДУКЦИИ: $\Gamma \vdash F \longrightarrow F_1$. Действительно, имеем одну из трех возможностей F_1 — аксиома или $F_1 \in \Gamma$, или $F_1 = F$. В первых двух случаях последовательность формул $F_1, F_1 \longrightarrow (F \longrightarrow F_1), F \longrightarrow F_1$ является выводом $F \longrightarrow F_1$ из Γ ; здесь $F_1 \longrightarrow (F \longrightarrow F_1)$ есть аксиома из схемы (А1) и $F \longrightarrow F_1$ получается из формул $F_1, F_1 \longrightarrow (F \longrightarrow F_1)$ по МР. Пусть $F_1 = F$. Тогда

заметим, что формула $F \longrightarrow F$ будет теоремой (ее вывод аналогичен выводу в теории \mathcal{T} ; см. пример 4 из §3.1), и потому $\Gamma \vdash F \longrightarrow F$.

ШАГ ИНДУКЦИИ: пусть для всех $i < k$ уже доказано $\Gamma \vdash F \longrightarrow F_i$; проверим, что $\Gamma \vdash F \longrightarrow F_k$. Если F_k – аксиома или $F_k \in \Gamma$, или $F_k = F$, то выводимость $F \longrightarrow F_k$ из Γ устанавливается так же как и в базе индукции. Поэтому остается разобрать два случая: $\frac{F_i, F_j}{F_k}$ (MP) и $\frac{F_i}{F_k}$ (ПО), где $i, j < k$.

Пусть $\frac{F_i, F_j}{F_k}$ (MP) и $F_j = F_i \longrightarrow F_k$. Тогда $F \longrightarrow F_i$, $F \longrightarrow F_j \vdash F \longrightarrow F_k$. В самом деле, ниже указан искомый вывод:

- (1) $F \longrightarrow F_i$ (гипотеза)
- (2) $F \longrightarrow (F_i \longrightarrow F_k)$ (гипотеза)
- (3) $(F \longrightarrow (F_i \longrightarrow F_k)) \longrightarrow ((F \longrightarrow F_i) \longrightarrow (F \longrightarrow F_k))$ (схема аксиом (A2))
- (4) $(F \longrightarrow F_i) \longrightarrow (F \longrightarrow F_k)$ (из (2), (3) по MP)
- (5) $F \longrightarrow F_k$ (из (1), (4) по MP)

По предположению индукции имеем $\Gamma \vdash F \longrightarrow F_i$ и $\Gamma \vdash F \longrightarrow F_j$, а поскольку $F \longrightarrow F_i$, $F \longrightarrow F_j \vdash F \longrightarrow F_k$, получаем $\Gamma \vdash F \longrightarrow F_k$ (см. предложение из §3.1 о свойствах выводимости).

Пусть $\frac{F_i}{F_k}$ (ПО) и $F_k = \forall x F_i$. Тогда построим сначала вывод $F \longrightarrow F_k$ из $F \longrightarrow F_i$:

- (1) $F \longrightarrow F_i$ (гипотеза)
- (2) $\forall x (F \longrightarrow F_i)$ (из (1) по ПО)
- (3) $\forall x (F \longrightarrow F_i) \longrightarrow (F \longrightarrow \forall x F_i)$ (схема аксиом (A4))
- (4) $F \longrightarrow \forall x F_i$, т.е. $F \longrightarrow F_k$ (из (2), (3) по MP)

Заметим, что формула (3) этого вывода действительно является аксиомой, т.к. переменная x не входит свободно в F ; это единственное место в доказательстве, где используется замкнутость формулы F .

По предположению индукции имеем $\Gamma \vdash F \longrightarrow F_i$, и в силу того, что $F \longrightarrow F_i \vdash F \longrightarrow F_k$, получаем $\Gamma \vdash F \longrightarrow F_k$.

Итак, мы установили, что $\Gamma \vdash F \longrightarrow F_i$ для любого индекса i от 1 до n . Полагая теперь $i = n$, заключаем $\Gamma \vdash F \longrightarrow F_n$, т.е. $\Gamma \vdash F \longrightarrow G$. Теорема доказана.

СЛЕДСТВИЕ. Пусть F, G – формулы теории первого порядка, причем F замкнута. Тогда $F \vdash G$ в том и только в том случае, если $\vdash F \longrightarrow G$.

Приведем примеры того, как использование теоремы о дедукции значительно упрощает доказательства некоторых утверждений на выводимость в теориях первого порядка.

ПРИМЕР 1. Если формула F замкнута, то

$$F \longrightarrow (G \longrightarrow H), G \vdash F \longrightarrow H.$$

Покажем сначала, что $F \longrightarrow (G \longrightarrow H)$, $G, F \vdash H$. Для этого построим соответствующий вывод:

- (1) F (гипотеза)
- (2) $F \longrightarrow (G \longrightarrow H)$ (гипотеза)
- (3) $G \longrightarrow H$ (из (1), (2) по МР)
- (4) G (гипотеза)
- (5) H (из (3), (4) по МР)

Применяя теперь к утверждению $F \longrightarrow (G \longrightarrow H)$, $G, F \vdash H$ теорему о дедукции, получаем $F \longrightarrow (G \longrightarrow H)$, $G \vdash F \longrightarrow H$.

ПРИМЕР 2. Если формула F замкнута, то

$$F \longrightarrow G, G \longrightarrow H \vdash F \longrightarrow H.$$

Укажем прежде вывод H из формул $F \longrightarrow G$, $G \longrightarrow H$, F :

- (1) F (гипотеза)
- (2) $F \longrightarrow G$ (гипотеза)
- (3) G (из (1), (2) по МР)
- (4) $G \longrightarrow H$ (гипотеза)
- (5) H (из (3), (4) по МР)

Таким образом, имеем $F \longrightarrow G$, $G \longrightarrow H$, $F \vdash H$ и, по теореме о дедукции, $F \longrightarrow G$, $G \longrightarrow H \vdash F \longrightarrow H$.

ПРИМЕР 3. Для любых замкнутых формул F и G следующие формулы являются теоремами (в произвольной теории первого порядка):

- | | |
|---|---|
| (а) $\neg\neg F \longrightarrow F$; | (г) $(G \longrightarrow F) \longrightarrow (\neg F \longrightarrow \neg G)$; |
| (б) $F \longrightarrow \neg\neg F$; | (д) $G \longrightarrow (\neg F \longrightarrow \neg(G \longrightarrow F))$; |
| (в) $(\neg F \longrightarrow \neg G) \longrightarrow (G \longrightarrow F)$; | (е) $\neg(G \longrightarrow F) \longrightarrow \neg F$. |

(а) Вывод теоремы $\neg\neg F \longrightarrow F$:

- (1) $(\neg F \longrightarrow \neg\neg F) \longrightarrow ((\neg F \longrightarrow \neg F) \longrightarrow F)$ (схема аксиом (А3))

- (2) $\neg F \longrightarrow \neg F$ (это теорема; см. пример 4 из §3.1)
 (3) $(\neg F \longrightarrow \neg\neg F) \longrightarrow F$ (из (1), (2) ввиду примера 1)
 (4) $\neg\neg F \longrightarrow (\neg F \longrightarrow \neg\neg F)$ (схема аксиом (A1))
 (5) $\neg\neg F \longrightarrow F$ (из (3), (4) ввиду примера 2)

(б) Вывод теоремы $F \longrightarrow \neg\neg F$:

(1) $(\neg\neg\neg F \longrightarrow \neg F) \longrightarrow ((\neg\neg\neg F \longrightarrow F) \longrightarrow \neg\neg F)$ (схема аксиом (A3))

(2) $\neg\neg\neg F \longrightarrow \neg F$ (теорема по пункту (а), рассмотренному выше)

(3) $(\neg\neg\neg F \longrightarrow F) \longrightarrow \neg\neg F$ (из (1), (2) по МР)

(4) $F \longrightarrow (\neg\neg\neg F \longrightarrow F)$ (схема аксиом (A1))

(5) $F \longrightarrow \neg\neg F$ (из (3), (4) ввиду примера 2)

(в) Вывод теоремы $(\neg F \longrightarrow \neg G) \longrightarrow (G \longrightarrow F)$.

Сначала установим, что $\neg F \longrightarrow \neg G, G \vdash F$:

(1) $\neg F \longrightarrow \neg G$ (гипотеза)

(2) G (гипотеза)

(3) $(\neg F \longrightarrow \neg G) \longrightarrow ((\neg F \longrightarrow G) \longrightarrow F)$ (схема аксиом (A3))

(4) $(\neg F \longrightarrow G) \longrightarrow F$ (из (1), (3) по МР)

(5) $G \longrightarrow (\neg F \longrightarrow G)$ (схема аксиом (A1))

(6) $G \longrightarrow F$ (из (4), (5) ввиду примера 2)

(7) F (из (2), (6) по МР)

Применив теперь дважды к утверждению $\neg F \longrightarrow \neg G, G \vdash F$ теорему о дедукции, получим окончательно $\vdash (\neg F \longrightarrow \neg G) \longrightarrow (G \longrightarrow F)$.

(г) Вывод теоремы $(G \longrightarrow F) \longrightarrow (\neg F \longrightarrow \neg G)$.

Покажем прежде, что $G \longrightarrow F \vdash \neg F \longrightarrow \neg G$:

(1) $G \longrightarrow F$ (гипотеза)

(2) $\neg\neg G \longrightarrow G$ (теорема по пункту (а))

(3) $\neg\neg G \longrightarrow F$ (из (1), (2) ввиду примера 2)

(4) $F \longrightarrow \neg\neg F$ (теорема по пункту (б))

(5) $\neg\neg G \longrightarrow \neg\neg F$ (из (3), (4) ввиду примера 2)

(6) $(\neg\neg G \longrightarrow \neg\neg F) \longrightarrow (\neg F \longrightarrow \neg G)$ (теорема по пункту (в))

(7) $\neg F \longrightarrow \neg G$ (из (5), (6) по МР)

Применив к утверждению $G \longrightarrow F \vdash \neg F \longrightarrow \neg G$ теорему о дедукции, получим требуемый результат.

(д) Вывод теоремы $G \longrightarrow (\neg F \longrightarrow \neg(G \longrightarrow F))$.

По правилу МР имеем $G, G \longrightarrow F \vdash F$. Дважды пользуясь теоремой о дедукции, получаем $\vdash G \longrightarrow ((G \longrightarrow F) \longrightarrow F)$. В силу пункта (г) выполнено $\vdash ((G \longrightarrow F) \longrightarrow F) \longrightarrow (\neg F \longrightarrow \neg(G \longrightarrow F))$. Отсюда, учитывая пример 2, заключаем, что $\vdash G \longrightarrow (\neg F \longrightarrow \neg(G \longrightarrow F))$.

(е) Вывод теоремы $\neg(G \longrightarrow F) \longrightarrow \neg F$:

(1) $F \longrightarrow (G \longrightarrow F)$ (схема аксиом (А1))

(2) $(F \longrightarrow (G \longrightarrow F)) \longrightarrow (\neg(G \longrightarrow F) \longrightarrow \neg F)$ (теорема по пункту (г))

(3) $\neg(G \longrightarrow F) \longrightarrow \neg F$ (из (1), (2) по МР)

§ 3.4. Обращение теоремы о непротиворечивости

Приводимая в этом параграфе теорема является основным средством в обосновании адекватности выбранной нами аксиоматики в теориях первого порядка. Она представляет собой обращение теоремы о непротиворечивости.

ТЕОРЕМА. *Всякое непротиворечивое множество формул теории первого порядка имеет [счетную] модель.*[‡]

Доказательство этой теоремы мы разобьем на ряд лемм.

ЛЕММА 1. *Если формулы F и G замкнуты, то*

(а) $\neg F \longrightarrow G, \neg F \longrightarrow \neg G \vdash F$;

(б) $G, \neg F \vdash \neg(G \longrightarrow F)$;

(в) $\neg(G \longrightarrow F) \vdash \neg F$;

(г) $\neg(G \longrightarrow F) \vdash G$.

Доказательство пункта (а) состоит в построении соответствующего вывода:

(1) $(\neg F \longrightarrow \neg G) \longrightarrow ((\neg F \longrightarrow G) \longrightarrow F)$ (схема аксиом (А3))

(2) $\neg F \longrightarrow G$ (гипотеза)

(3) $(\neg F \longrightarrow \neg G) \longrightarrow F$ (из (1), (2) ввиду примера 1 параграфа

3.3)

(4) $\neg F \longrightarrow \neg G$ (гипотеза)

(5) F (из (3), (4) по МР)

[‡]Для так называемых *теорий первого порядка с равенством*, которые мы рассмотрим в §3.6, эта теорема будет переформулирована в слегка модифицированном виде.

(б) В силу примера 3(д) из §3.3 имеем $\vdash G \rightarrow (\neg F \rightarrow \neg(G \rightarrow F))$. Применив дважды теорему о дедукции, получим последовательно $G \vdash \neg F \rightarrow \neg(G \rightarrow F)$ и $G, \neg F \vdash \neg(G \rightarrow F)$.

(в) Ввиду пункта (е) того же примера выполнено $\vdash \neg(G \rightarrow F) \rightarrow \neg F$, откуда по теореме о дедукции получаем $\neg(G \rightarrow F) \vdash \neg F$.

(г) Покажем сначала, что $\neg G, G \vdash F$:

- (1) $\neg G$ (гипотеза)
- (2) G (гипотеза)
- (3) $G \rightarrow (\neg F \rightarrow G)$ (схема аксиом (A1))
- (4) $\neg G \rightarrow (\neg F \rightarrow \neg G)$ (схема аксиом (A1))
- (5) $\neg F \rightarrow \neg G$ (из (1), (4) по MP)
- (6) $\neg F \rightarrow G$ (из (2), (3) по MP)
- (7) F (из (5), (6) по пункту (а), рассмотренному выше)

Итак, имеем $\neg G, G \vdash F$. Отсюда по теореме о дедукции выполнено $\neg G \vdash G \rightarrow F$ и, снова по той же теореме, $\vdash \neg G \rightarrow (G \rightarrow F)$. Теперь построим искомый вывод формулы G из $\neg(G \rightarrow F)$:

- (1) $\neg G \rightarrow (G \rightarrow F)$ (теорема)
- (2) $\neg(G \rightarrow F)$ (гипотеза)
- (3) $(\neg G \rightarrow (G \rightarrow F)) \rightarrow (\neg(G \rightarrow F) \rightarrow \neg\neg G)$ (теорема по пункту (г) примера 3 из §3.3)
- (4) $\neg\neg G \rightarrow G$ (теорема по пункту (а) того же примера)
- (5) $\neg(G \rightarrow F) \rightarrow \neg\neg G$ (из (1), (3) по MP)
- (6) $\neg(G \rightarrow F) \rightarrow G$ (из (4), (5) ввиду примера 2 параграфа 3.3)
- (7) G (из (2), (6) по MP)

ЛЕММА 2. Пусть Γ – некоторое множество формул теории первого порядка и F – замкнутая формула этой теории. Тогда если множество формул $\Gamma \cup \{\neg F\}$ противоречиво, то $\Gamma \vdash F$.

Доказательство. Пусть $\Gamma \cup \{\neg F\}$ противоречиво, т.е. существует замкнутая формула G такая, что $\Gamma \cup \{\neg F\} \vdash G$ и $\Gamma \cup \{\neg F\} \vdash \neg G$. Учитывая теорему о дедукции, получаем $\Gamma \vdash \neg F \rightarrow G$ и $\Gamma \vdash \neg F \rightarrow \neg G$. Отсюда и из установленного в пункте (а) леммы 1 следования $\neg F \rightarrow G, \neg F \rightarrow \neg G \vdash F$ заключаем, что $\Gamma \vdash F$.

ЗАМЕЧАНИЕ. Из леммы 2 вытекает следующий полезный факт: если множество формул противоречиво, то из него выводится любая формула (это утверждение есть синтаксический ана-

лог известного нам тезиса о том, что из лжи следует все, что угодно). В самом деле, пусть Γ противоречиво и F – произвольная формула. Тогда противоречиво и множество формул $\Gamma \cup \{\neg\bar{F}\}$, откуда в силу леммы 2 имеем $\Gamma \vdash \bar{F}$, т.к. формула \bar{F} замкнута. Поэтому, принимая во внимание пример 1 из §3.2, получаем $\Gamma \vdash F$.

Множество Γ формул произвольной теории \mathcal{K} называется *полным в \mathcal{K}* , если $\Gamma \vdash_{\mathcal{K}} F$ или $\Gamma \vdash_{\mathcal{K}} \neg F$ для любой замкнутой формулы F теории \mathcal{K} . Следующее вспомогательное утверждение в честь его автора носит название *леммы Линденбаума*.

ЛЕММА 3. *Всякое непротиворечивое множество формул теории первого порядка содержится в некотором полном непротиворечивом множестве формул этой теории.*

Доказательство. Пусть Γ – непротиворечивое множество формул теории \mathcal{K} . Поскольку алфавит теории \mathcal{K} счетен, счетным будет и множество всех ее выражений. Поэтому мы можем перенумеровать все замкнутые формулы в \mathcal{K} ; пусть F_1, F_2, \dots – какой-нибудь их пересчет. Следующим образом определим теперь последовательность $\Gamma_0, \Gamma_1, \Gamma_2, \dots$ множеств, состоящих из формул теории \mathcal{K} . Считаем $\Gamma_0 = \Gamma$. Предположим далее, что множество Γ_n ($n \geq 0$) определено. Тогда полагаем $\Gamma_{n+1} = \Gamma_n \cup \{F_{n+1}\}$, если $\Gamma_n \not\vdash \neg F_{n+1}$, и $\Gamma_{n+1} = \Gamma_n \cup \{\neg F_{n+1}\}$, если $\Gamma_n \not\vdash F_{n+1}$ (заметим, что корректность пошагового построения Γ_{n+1} по множеству формул Γ_n вытекает из непротиворечивости Γ_n , что проверяется ниже; если при этом выполнено одновременно как $\Gamma_n \not\vdash \neg F_{n+1}$, так и $\Gamma_n \not\vdash F_{n+1}$, то выбираем любую из двух возможностей). Положим $\Gamma_\infty = \bigcup_n \Gamma_n$. По построению, $\Gamma_\infty \supseteq \Gamma$ и для любой замкнутой формулы F теории \mathcal{K} имеем $\Gamma_\infty \vdash F$ или $\Gamma_\infty \vdash \neg F$, т.е. множество формул Γ_∞ является полным. Действительно, $F = F_{n+1}$ для некоторого натурального n и либо $\Gamma_\infty \supseteq \Gamma_{n+1} \supseteq \{F_{n+1}\}$, либо $\Gamma_\infty \supseteq \Gamma_{n+1} \supseteq \{\neg F_{n+1}\}$. Для доказательства непротиворечивости Γ_∞ достаточно доказать непротиворечивость каждого из множеств Γ_n , т.к. всякий вывод противоречия из Γ_∞ использует лишь конечное число гипотез и, следовательно, является выводом противоречия уже из некоторого множества Γ_n . Непротиворечивость множества формул Γ_n докажем индукцией по номеру n . По условию, множество $\Gamma_0 = \Gamma$ непротиворечиво. Допустим, что множество Γ_n непротиворечиво и рассмотрим два случая, один из которых обязательно имеет место.

Случай 1: $\Gamma_n \not\vdash F_{n+1}$. Тогда в силу леммы 2 множество формул $\Gamma_{n+1} = \Gamma_n \cup \{\neg F_{n+1}\}$ непротиворечиво.

Случай 2: $\Gamma_n \not\vdash \neg F_{n+1}$. Тогда множество формул $\Gamma_n \cup \{\neg F_{n+1}\}$ непротиворечиво в силу той же леммы. Следовательно, поскольку $\neg F_{n+1} \vdash F_{n+1}$ (см. пример 3(a) из §3.3), непротиворечивым будет и множество формул $\Gamma_{n+1} = \Gamma_n \cup \{F_{n+1}\}$.

Итак, непротиворечивость Γ_n влечет за собой непротиворечивость Γ_{n+1} . Отсюда вытекает непротиворечивость всех формул Γ_n , а потому и множества формул $\Gamma_\infty = \bigcup_n \Gamma_n$. Лемма доказана.

Пусть теория \mathcal{K}' получена из \mathcal{K} добавлением к сигнатуре $\Sigma(\mathcal{K})$ новых символов. В этом случае будем говорить, что \mathcal{K}' является *расширением* теории \mathcal{K} .

Назовем всякий терм *замкнутым*, если он не содержит предметных переменных. Очевидно, нульарные функциональные символы суть замкнутые термы.

ЛЕММА 4. *Для любого непротиворечивого множества Γ формул теории \mathcal{K} существует непротиворечивое множество Γ' формул расширения \mathcal{K}' теории \mathcal{K} , содержащее Γ и такое, что если $\Gamma \vdash_{\mathcal{K}} \neg \forall x F(x)$, где x — единственная свободная переменная в $F(x)$, то в Γ' найдется формула вида $\neg F(t)$, где t — некоторый замкнутый терм теории \mathcal{K}' .*

Доказательство. Пусть $F_1(x_1), F_2(x_2), \dots$ — какой-нибудь пересчет всех формул теории \mathcal{K} , содержащих не более одной свободной переменной и таких, что формулы $\neg \forall x_1 F_1(x_1), \neg \forall x_2 F_2(x_2), \dots$ выводятся из Γ . Выберем последовательность t_1, t_2, \dots нульарных функциональных символов таким образом, чтобы $t_k \notin \Sigma(\mathcal{K}) \cup \{t_1, t_2, \dots, t_{k-1}\}$ ни при каком k . Обозначим через \mathcal{K}' (соответственно \mathcal{K}_n) расширение теории \mathcal{K} , для которого $\Sigma(\mathcal{K}') = \Sigma(\mathcal{K}) \cup \{t_1, t_2, \dots\}$ (соответственно $\Sigma(\mathcal{K}_n) = \Sigma(\mathcal{K}) \cup \{t_1, t_2, \dots, t_n\}$), а через Γ' (соответственно Γ_n) — множество формул $\Gamma \cup \{\neg F_1(t_1), \neg F_2(t_2), \dots\}$ (соответственно $\Gamma \cup \{\neg F_1(t_1), \neg F_2(t_2), \dots, \neg F_n(t_n)\}$); при этом считаем $\mathcal{K}_0 = \mathcal{K}$ и $\Gamma_0 = \Gamma$. Покажем, что Γ' непротиворечиво в \mathcal{K}' . Действительно, ввиду очевидных равенств $\Gamma' = \bigcup_n \Gamma_n$ и $\Sigma(\mathcal{K}') = \bigcup_n \Sigma(\mathcal{K}_n)$ достаточно установить непротиворечивость каждого множества формул Γ_n в расширении \mathcal{K}_n . Проведем индукцию по n . По условию множество $\Gamma_0 = \Gamma$ непротиворечиво в $\mathcal{K}_0 = \mathcal{K}$. Пусть доказана непротиворечивость Γ_n в \mathcal{K}_n и допустим от противного, что множество формул Γ_{n+1} противоречиво в \mathcal{K}_{n+1} . Тогда, поскольку $\Gamma_{n+1} = \Gamma_n \cup \{\neg F_{n+1}(t_{n+1})\}$ и формула $F_{n+1}(t_{n+1})$ замкнута, применение леммы 2 дает $\Gamma_n \vdash_{\mathcal{K}_{n+1}} F_{n+1}(t_{n+1})$. Заменяем теперь в последова-

тельности формул, являющейся выводом $F_{n+1}(t_{n+1})$ из Γ_n в теории \mathcal{K}_{n+1} , каждое вхождение символа t_{n+1} переменной x_{n+1} . Так как $t_{n+1} \notin \Sigma(\mathcal{K}) \cup \{t_1, t_2, \dots, t_n\}$, мы получим, очевидно, последовательность формул, которая будет выводом $F_{n+1}(x_{n+1})$ из Γ_n в теории \mathcal{K}_n . Таким образом, будем иметь $\Gamma_n \vdash_{\mathcal{K}_n} F_{n+1}(x_{n+1})$ и, учитывая правило обобщения, $\Gamma_n \vdash_{\mathcal{K}_n} \forall x_{n+1} F_{n+1}(x_{n+1})$. С другой стороны, имеем $\Gamma_n \vdash_{\mathcal{K}_n} \neg \forall x_{n+1} F_{n+1}(x_{n+1})$, т.к. $\Gamma_n \supseteq \Gamma$ и $\Gamma \vdash_{\mathcal{K}} \neg \forall x_{n+1} F_{n+1}(x_{n+1})$. Но этого не может быть, поскольку множество формул Γ_n непротиворечиво. Итак, мы доказали для любого n непротиворечивость Γ_n в теории \mathcal{K}_n , а следовательно, и непротиворечивость Γ' в теории \mathcal{K}' . Из определения множества формул Γ' непосредственно вытекает, что оно подчиняется указанному в лемме условию.

ЛЕММА 5. *Для любого непротиворечивого множества Γ формул теории \mathcal{K} существует полное непротиворечивое множество Γ' формул расширения \mathcal{K}' теории \mathcal{K} , содержащее Γ и такое, что если $\Gamma' \vdash_{\mathcal{K}'} \neg \forall x F(x)$, где x – единственная свободная переменная в $F(x)$, то в Γ' найдется формула вида $\neg F(t)$, где t – некоторый замкнутый терм теории \mathcal{K}' .*

Доказательство. Применяя поочерёдно леммы 3 и 4, построим возрастающую по включению последовательность $\Gamma = \Gamma_0 \subseteq \Phi_1 \subseteq \Gamma_1 \subseteq \Phi_2 \subseteq \dots$ множеств формул и возрастающую по включению сигнатур последовательность $\mathcal{K} = \mathcal{K}_0, \mathcal{K}_1, \mathcal{K}_2, \dots$ теорий, обладающие следующими свойствами: для всякого $n \geq 1$ множества формул Γ_n и Φ_n непротиворечивы в \mathcal{K}_n , причем Γ_n – полное в \mathcal{K}_n множество, и если $\Gamma_{n-1} \vdash_{\mathcal{K}_{n-1}} \neg \forall x F(x)$, где $F(x)$ содержит не более одной свободной переменной, то в Φ_n существует формула вида $\neg F(t)$ для некоторого замкнутого термина t из \mathcal{K}_n . Положим $\Gamma' = \bigcup_n \Gamma_n = \bigcup_n \Phi_n$, а в качестве \mathcal{K}' возьмем расширение теории \mathcal{K} такое, что $\Sigma(\mathcal{K}') = \bigcup_n \Sigma(\mathcal{K}_n)$. Тогда легко видеть, что множество формул Γ' и теория \mathcal{K}' удовлетворяют приведенным в условии леммы требованиям.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Пусть Γ – непротиворечивое множество формул теории \mathcal{K} . Мы хотим указать модель теории \mathcal{K} , на которой истинны все формулы из Γ . Ясно, что такую модель достаточно построить для множества формул Γ' , существование которого с заданными свойствами в некотором расширении \mathcal{K}' теории \mathcal{K} обеспечивается леммой 5. В качестве основного множества искомой модели мы возьмем множество M всех замкнутых термов теории

\mathcal{K}' . Каждому функциональному символу $f^{(n)} \in \Sigma(\mathcal{K}')$ в M соответствует операция f_n , вычисляющая по любым $t_1, t_2, \dots, t_n \in M$ элемент $f^{(n)}(t_1, t_2, \dots, t_n) \in M$; при $n = 0$ символу $f^{(0)}$ соответствует выделенный элемент $f^{(0)} \in M$. Каждый предикатный символ $P^{(n)} \in \Sigma(\mathcal{K}')$ интерпретируется в M предикатом P_n , который определяется следующим образом: для любых $t_1, t_2, \dots, t_n \in M$ выполнено:

$$P_n(t_1, t_2, \dots, t_n) = \begin{cases} \mathbf{1}, & \text{если } \Gamma' \vdash P^{(n)}(t_1, t_2, \dots, t_n), \\ \mathbf{0}, & \text{если } \Gamma' \not\vdash P^{(n)}(t_1, t_2, \dots, t_n). \end{cases} \quad (*)$$

Множество M с указанными операциями и предикатами образует алгебраическую систему \mathfrak{M} сигнатуры $\Sigma(\mathcal{K}')$. Чтобы доказать, что \mathfrak{M} является моделью \mathcal{K}' , на которой истинна всякая формула из Γ' , докажем сначала, что *произвольная замкнутая формула F теории \mathcal{K}' истинна в \mathfrak{M} тогда и только тогда, когда $\Gamma' \vdash F$ в теории \mathcal{K}'* . Доказательство будем вести индукцией по числу связей и кванторов в F . Если F есть замкнутая атомарная формула, то, согласно определению (*), она истинна в \mathfrak{M} тогда и только тогда, когда $\Gamma' \vdash F$. Допустим далее, что это утверждение верно для всех замкнутых формул с меньшим, чем у F , числом связей и кванторов. Рассмотрим три возможных случая.

Случай 1: $F = \neg G$. Если F истинна в \mathfrak{M} , то G ложна в \mathfrak{M} и, следовательно, в силу предположения индукции $\Gamma' \not\vdash G$. Так как Γ' является полным в \mathcal{K}' множеством формул и G замкнута, имеем $\Gamma' \vdash \neg G$, т.е. $\Gamma' \vdash F$. С другой стороны, если F ложна в \mathfrak{M} , то G истинна в \mathfrak{M} , и тогда $\Gamma' \vdash G$, а поскольку Γ' непротиворечиво, получаем $\Gamma' \not\vdash \neg G$, т.е. $\Gamma' \not\vdash F$.

Случай 2: $F = G \longrightarrow H$. Из замкнутости F вытекает замкнутость формул G и H . Если F ложна в \mathfrak{M} , то G истинна и H ложна в \mathfrak{M} . Тогда согласно индуктивному предположению $\Gamma' \vdash G$ и $\Gamma' \not\vdash H$. Из полноты Γ' имеем $\Gamma' \vdash \neg H$. Поэтому ввиду того, что $G, \neg H \vdash \neg(G \longrightarrow H)$ по лемме 1(б), справедливо $\Gamma' \vdash \neg(G \longrightarrow H)$, т.е. $\Gamma' \vdash \neg F$ и, в силу непротиворечивости Γ' , имеем $\Gamma' \not\vdash F$. Обратное, если $\Gamma' \not\vdash F$, то из полноты Γ' получаем $\Gamma' \vdash \neg F$, т.е. $\Gamma' \vdash \neg(G \longrightarrow H)$. Тогда, поскольку $\neg(G \longrightarrow H) \vdash G$ и $\neg(G \longrightarrow H) \vdash \neg H$ по лемме 1(в,г), имеем $\Gamma' \vdash G$, $\Gamma' \vdash \neg H$ и, ввиду непротиворечивости Γ' , выполнено $\Gamma' \not\vdash H$. Отсюда, учитывая предположение индукции, делаем вывод, что G истинна, а H ложна в \mathfrak{M} , и значит, формула $F = G \longrightarrow H$ также ложна в \mathfrak{M} .

Случай 3: $F = \forall xG$. Если x не входит свободно в G , т.е. G замкнута, то F истинна в \mathfrak{M} тогда и только тогда, когда в \mathfrak{M} истинна G . Принимая во внимание тот факт, что $\Gamma' \vdash F$ тогда и только тогда, когда $\Gamma' \vdash G$, получаем интересное нас утверждение для F из соответствующего утверждения о G . Поэтому далее считаем, что $G = G(x)$, где x – единственная свободная переменная в G .

Предположим, что F истинна в \mathfrak{M} и тем не менее $\Gamma' \not\vdash F$. В силу полноты Γ' имеем $\Gamma' \vdash \neg F$, т.е. $\Gamma' \vdash \neg \forall xG(x)$. Отсюда по известному свойству множества формул Γ' вытекает наличие замкнутого термина t теории \mathcal{K}' , для которого $\neg G(t) \in \Gamma'$ и, в частности, $\Gamma' \vdash \neg G(t)$. Так как формула $F = \forall xG(x)$ истинна в \mathfrak{M} , то истинна в \mathfrak{M} и формула $G(t)$, откуда по индуктивному предположению получаем $\Gamma' \vdash G(t)$. Но этого быть не может, поскольку $\Gamma' \vdash \neg G(t)$, а Γ' непротиворечиво. Итак, из истинности F в \mathfrak{M} следует $\Gamma' \vdash F$.

Обратно, допустим теперь, что $\Gamma' \vdash F$ и вместе с тем F ложна в \mathfrak{M} . Из ложности формулы $\forall xG(x)$ в \mathfrak{M} и из определения основного множества системы \mathfrak{M} как множества M всех замкнутых термов теории \mathcal{K}' вытекает, что для некоторого замкнутого термина t из \mathcal{K}' формула $G(t)$ ложна. С другой стороны, имеем по условию $\Gamma' \vdash \forall xG(x)$. Учитывая аксиому (A5) $\forall xG(x) \rightarrow G(t)$, получаем $\forall xG(x) \vdash G(t)$ и, следовательно, $\Gamma' \vdash G(t)$. Поэтому в силу индуктивного предположения формула $G(t)$ должна быть истинной в \mathfrak{M} , а это не так. Данное противоречие доказывает, что условие $\Gamma' \vdash F$ влечет за собой истинность формулы F в системе \mathfrak{M} .

Таким образом, установлено, что любая замкнутая формула F из \mathcal{K}' истинна в \mathfrak{M} в том и только в том случае, если $\Gamma' \vdash F$. Рассмотрим теперь произвольную формулу G из Γ' . Согласно примеру 1 из §3.2 имеем $\Gamma' \vdash \bar{G}$, где \bar{G} – замыкание G . По доказанному выше формула \bar{G} истинна в \mathfrak{M} , а значит и формула G истинна в \mathfrak{M} . Аналогично проверяется, что всякая аксиома теории \mathcal{K}' истинна в \mathfrak{M} , т.е. система \mathfrak{M} является моделью для \mathcal{K}' . Отсюда, поскольку $\Gamma' \supseteq \Gamma$ и \mathcal{K}' есть расширение теории \mathcal{K} , получаем, что \mathfrak{M} – модель теории \mathcal{K} , на которой истинны все формулы из Γ . Осталось заметить, что \mathfrak{M} счетна, так как счетно множество всех замкнутых термов теории \mathcal{K}' , являющееся по построению основным множеством для \mathfrak{M} . Теорема доказана.

§ 3.5. Теоремы об адекватности, полноте и компактности. Теорема Лёвенгейма-Сколема

Следующая теорема устанавливает равноправность синтаксического понятия выводимости и семантического понятия логического следования.

ТЕОРЕМА ОБ АДЕКВАТНОСТИ. *Пусть Γ – некоторое множество формул теории первого порядка и F – произвольная формула. Тогда $\Gamma \vdash F$ в том и только в том случае, если $\Gamma \models F$.*

Доказательство. В §3.2 было показано, что условие $\Gamma \vdash F$ влечет за собой $\Gamma \models F$. Обратное, пусть $\Gamma \models F$. Это означает, что для любой модели \mathfrak{M} данной теории из того, что все формулы из Γ истинны на \mathfrak{M} , следует истинность на \mathfrak{M} формулы F , а потому и ее замыкания \bar{F} . Тогда формулы из множества $\Gamma \cup \{\bar{F}\}$ не могут быть одновременно истинными ни на какой модели. Отсюда ввиду доказанной нами теоремы, являющейся обращением теоремы о непротиворечивости, получаем, что множество формул $\Gamma \cup \{\bar{F}\}$ противоречиво. Поэтому в силу леммы 2 из §3.4 имеем $\Gamma \vdash \bar{F}$, так как формула \bar{F} замкнута. Осталось вспомнить, что из условия $\Gamma \vdash \bar{F}$ следует $\Gamma \vdash F$. Теорема доказана.

Полагая в теореме об адекватности $\Gamma = \emptyset$, получаем равноправность условий $\vdash F$ и $\models F$. Таким образом, справедлива следующая

ТЕОРЕМА О ПОЛНОТЕ. *Во всякой теории первого порядка теоремами являются все те и только те формулы, которые логически общезначимы.*

Эта теорема впервые была доказана австрийским математиком Куртом Гёделем в 1930 году для классического случая теории исчисления предикатов. Суть ее заключается в том, что указанных пяти схем логических аксиом и двух правил вывода – modus ponens и правила обобщения – вполне достаточно для того, чтобы каждая логически общезначимая формула в теории первого порядка была выводима. В этом смысле *список логических аксиом и правил вывода является полным*. Так как в теории \mathcal{T} исчисления высказываний логически общезначимые формулы – это в точности тавтологии, получаем

СЛЕДСТВИЕ 1. *В теории исчисления высказываний класс теорем совпадает с классом тавтологий.*

В качестве другого следствия развитой нами техники отметим теорему о компактности, доказанную в полной общности в 1936 году советским математиком *Анатолием Ивановичем Мальцевым*.

ТЕОРЕМА О КОМПАКТНОСТИ. *Пусть Γ – некоторое множество формул теории первого порядка и F – произвольная формула. Тогда $\Gamma \models F$ в том и только в том случае, если $\Delta \models F$ для некоторого конечного подмножества Δ множества Γ .*

В самом деле, заменив в данном утверждении знак \models логического следования знаком \vdash выводимости, мы получим ввиду теоремы об адекватности равносильное ему утверждение, которое, как известно, справедливо (см. предложение о свойствах выводимости, доказанное в §3.1).

Заметим, что если F – логически противоречивая формула (т.е. она ложна при любой интерпретации), то условие $\Gamma \models F$ эквивалентно тому, что Γ не имеет [счетной] модели. Отсюда и из теоремы о компактности легко вытекает

СЛЕДСТВИЕ 2. *Множество формул теории первого порядка имеет [счетную] модель тогда и только тогда, когда каждое его конечное подмножество имеет модель.*

В действительности, это утверждение равносильно теореме о компактности и является одной из ее модификаций. Термин “компактность” заимствован из топологии; его использование объясняется следующими соображениями. Пусть \mathcal{E} – множество всех счетных моделей теории \mathcal{K} первого порядка. Подмножество \mathcal{U} множества \mathcal{E} назовем *замкнутым*, если для некоторого множества Δ формул теории \mathcal{K} выполнено $\mathfrak{M} \in \mathcal{U}$ тогда и только тогда, когда все формулы из Δ истинны на \mathfrak{M} . Множество \mathcal{E} вместе с системой всех своих замкнутых подмножеств образует *топологическое пространство*. Напомним, что топологическое пространство называется *компактным*, если оно обладает следующим свойством: пусть $\{\mathcal{U}_\lambda\}_{\lambda \in \Lambda}$ – любая совокупность замкнутых множеств, такая, что $\mathcal{U}_{\lambda_1} \cap \dots \cap \mathcal{U}_{\lambda_k} \neq \emptyset$ для каждого конечного набора $\lambda_1, \dots, \lambda_k \in \Lambda$; тогда $\bigcap_{\lambda \in \Lambda} \mathcal{U}_\lambda \neq \emptyset$. Из теоремы Мальцева о компактности вытекает компактность пространства моделей \mathcal{E} . Действительно, для замкнутого множества \mathcal{U}_λ моделей теории \mathcal{K} обозначим

через Δ_λ множество формул, его определяющее. Тогда условие $\mathcal{U}_{\lambda_1} \cap \dots \cap \mathcal{U}_{\lambda_k} \neq \emptyset$ эквивалентно тому, что множество формул $\Delta_{\lambda_1} \cup \dots \cup \Delta_{\lambda_k}$ имеет модель в \mathcal{K} . Поэтому, если пересечение всякого конечного семейства замкнутых множеств из $\{\mathcal{U}_\lambda\}_{\lambda \in \Lambda}$ непусто, то любое конечное подмножество множества формул $\Gamma = \bigcup_{\lambda \in \Lambda} \Delta_\lambda$ имеет модель в \mathcal{K} . Отсюда в силу следствия 2 получаем, что множество Γ само имеет в \mathcal{K} подходящую счетную модель \mathfrak{M} . Ясно, что тогда $\mathfrak{M} \in \bigcap_{\lambda \in \Lambda} \mathcal{U}_\lambda$ и, следовательно, $\bigcap_{\lambda \in \Lambda} \mathcal{U}_\lambda \neq \emptyset$. Компактность пространства \mathcal{E} моделей теории \mathcal{K} установлена.

В следующем параграфе мы рассмотрим одно из многочисленных приложений теоремы о компактности для теорий первого порядка с равенством. В заключение же данного параграфа в качестве еще одного следствия из теоремы о непротиворечивости и из ее обращения отметим такое полезное утверждение:

ТЕОРЕМА ЛЁВЕНГЕЙМА-СКОЛЕМА (1915, 1919). *Если множество формул теории первого порядка имеет модель, то оно имеет и счетную модель.*

Доказательство. Если множество формул Γ имеет модель в теории \mathcal{K} , то Γ непротиворечиво в \mathcal{K} (см. §3.2). Следовательно, в силу обращения теоремы о непротиворечивости Γ имеет счетную модель.

Оказывается, справедливо и более сильное утверждение, доказательство которого мы опускаем (его также называют иногда теоремой Лёвенгейма-Сколема): *если множество формул теории первого порядка имеет модель, то оно имеет модель любой бесконечной мощности.* Заметим, что здесь требование бесконечности модели существенно ввиду примера 5 из §2.3. Как мы увидим, для теорий первого порядка с равенством формулировка этой теоремы будет выглядеть несколько иначе.

§ 3.6. Теории первого порядка с равенством

Пусть \mathcal{K} – теория первого порядка, сигнатура которой содержит двухместный предикатный символ $E^{(2)}$. Будем сокращенно писать $t = s$ вместо $E^{(2)}(t, s)$ и $t \neq s$ вместо $\neg E^{(2)}(t, s)$. Теория \mathcal{K} называется *теорией первого порядка с равенством*, если следующие формулы являются теоремами \mathcal{K} :

$$(1) \forall x(x = x) \quad (\text{рефлексивность равенства});$$

(2) $\forall x \forall y (x = y \longrightarrow y = x)$ (симметричность равенства);

(3) $\forall x \forall y \forall z (x = y \wedge y = z \longrightarrow x = z)$ (транзитивность равенства);

(4) $\forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n (x_1 = y_1 \wedge \dots \wedge x_n = y_n \wedge F(x_1, \dots, x_n) \longrightarrow F(y_1, \dots, y_n))$ (подстановочность равенства);

здесь $F(x_1, \dots, x_n)$ – произвольная формула в \mathcal{K} .

В качестве примеров теорий первого порядка с равенством можно привести известные нам уже теории групп и полугрупп, а также следующие теории, встречающиеся в курсе общей алгебры.

ПРИМЕР 1. *Теория абелевых групп.* Ее сигнатура имеет один предикатный символ $=$ и два функциональных символа: $+$ (двухместный) и 0 (нульместный). Собственные аксиомы имеют вид:

(а) $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$;

(д) $\forall x (x = x)$;

(б) $\forall x (x + 0 = x)$;

(е) $\forall x \forall y (x = y \longrightarrow y = x)$;

(в) $\forall x \exists y (x + y = 0)$;

(ж) $\forall x \forall y \forall z (x = y \wedge y = z \longrightarrow x = z)$;

(г) $\forall x \forall y (x + y = y + x)$;

(з) $\forall x \forall y \forall z (x = y \longrightarrow x + z = y + z)$.

ПРИМЕР 2. *Теория полей.* Ее сигнатура содержит один предикатный символ $=$ и четыре функциональных символа: двухместные $+$ и \cdot , нульместные 0 и 1 . Собственные аксиомы имеют вид:

(а)–(з) из примера 1;

(л) $\forall x \forall y (x \cdot y = y \cdot x)$;

(и) $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$;

(м) $\forall x (x \cdot 1 = x)$;

(к) $\forall x \forall y \forall z (x \cdot (y + z) = x \cdot y + x \cdot z)$;

(н) $\forall x (x \neq 0 \longrightarrow \exists y (x \cdot y = 1))$.

Заметим, что аксиомы (а)–(м) определяют *теорию коммутативных ассоциативных колец с единицей*.

Для всякой модели теории первого порядка \mathcal{K} с равенством отношение E , соответствующее в этой модели предикатному символу $=$, является отношением эквивалентности. Если на основном множестве некоторой модели это отношение E оказывается отношением тождества, то такая модель называется *нормальной*.

В силу отмеченной выше *теоремы (4) подстановочности равенства* отношение E является стабильным в модели относительно применения операций и предикатов, т.е. является *конгруэнцией* на данной модели. Поэтому всякой модели \mathfrak{M} теории \mathcal{K} можно сопоставить некоторую нормальную модель \mathfrak{M}' теории \mathcal{K} . Для этого в

качестве основного множества M' новой модели \mathfrak{M}' возьмем множество классов эквивалентности, определяемых отношением E на основном множестве M модели \mathfrak{M} . Каждой операции f и каждому предикату P , действующим на M , естественным образом поставим в соответствие операцию f^* и предикат P^* на фактор-множестве M' :

$$f^*(\bar{a}_1, \dots, \bar{a}_n) = \overline{f(a_1, \dots, a_n)} \text{ и } P^*(\bar{a}_1, \dots, \bar{a}_n) = \mathbf{1} \iff \\ P(a_1, \dots, a_n) = \mathbf{1};$$

здесь \bar{a} – класс эквивалентности, содержащий элемент a . Это определение операций и предикатов на M' не зависит от выбора представителей a_1, \dots, a_n соответствующих классов эквивалентности. Множество M' с так заданными на нем операциями и предикатами образует систему \mathfrak{M}' ; она называется *фактор-системой* алгебраической системы \mathfrak{M} по конгруэнции E . Легко понять, что всякая формула, истинная на \mathfrak{M} , будет истинна и на \mathfrak{M}' , а поскольку \mathfrak{M} есть модель \mathcal{K} , моделью теории \mathcal{K} будет и система \mathfrak{M}' . Из построения ясно, что для любых элементов $\bar{a}, \bar{b} \in M'$ выполнено $(a, b) \in E \iff \bar{a} = \bar{b}$ и, следовательно, \mathfrak{M}' – нормальная модель теории \mathcal{K} .

Для теорий первого порядка с равенством формулировки некоторых теорем, доказанных в предыдущих параграфах, можно модифицировать, используя понятие нормальной модели. Так, обращение теоремы о непротиворечивости примет следующий вид:

Всякое непротиворечивое множество формул теории первого порядка с равенством имеет конечную или счетную нормальную модель.

Действительно, мы знаем, что любое такое множество формул имеет счетную модель. Очевидно, что факторизация этой модели по соответствующей конгруэнции приводит к нормальной конечной или счетной модели.

Теорема Лёвенгейма-Сколема будет иметь такой вид:

Если множество формул теории первого порядка с равенством имеет бесконечную нормальную модель, то оно имеет и счетную нормальную модель.

В самом деле, пусть множество формул Γ имеет бесконечную нормальную модель \mathfrak{M} в теории \mathcal{K} с равенством. Обозначим через

\mathcal{K}' теорию, получающуюся из \mathcal{K} добавлением списка (*) собственных аксиом:

$$\exists x_1 \dots \exists x_n (x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge \dots \wedge x_{n-1} \neq x_n),$$

где $n = 2, 3, \dots$. Так как \mathfrak{M} бесконечна, она является моделью и теории \mathcal{K}' . Тогда, как известно, Γ имеет счетную модель \mathfrak{M}' в \mathcal{K}' . Пусть \mathfrak{M}'' – нормальная модель, полученная из модели \mathfrak{M}' описанным выше способом. Поскольку \mathfrak{M}'' удовлетворяет аксиомам (*), она не может быть конечной. Следовательно, \mathfrak{M}'' – искомая счетная нормальная модель, на которой истинны все формулы из Γ .

Усиленная формулировка теоремы Лёвенгейма-Сколема для теорий с равенством примет следующий вид (соответствующее доказательство требует чуть более сложных рассуждений):

Если множество формул теории первого порядка с равенством имеет бесконечную нормальную модель, то оно имеет и нормальную модель любой бесконечной мощности.

Заметим, что в теориях первого порядка с равенством под моделью, как правило, принято понимать то, что мы называем нормальной моделью.

В заключение данного параграфа покажем, как теорема о компактности А. И. Мальцева применяется при доказательстве так называемых *локальных теорем* в алгебре (формулируемых для теорий первого порядка с равенством).

ПРИМЕР. Доказать, что *счетная полугруппа вложима в счетную группу, если любая ее конечно порожденная подполугруппа вложима в подходящую группу.*

В примере 6 из §3.2 мы указали множество (а)–(ж) собственных аксиом теории групп. Обозначим это множество через Φ_1 . Выберем в Φ_1 подмножество Φ_0 , состоящее из аксиомы ассоциативности (а) и аксиом (г)–(ж), описывающих свойства предиката равенства: рефлексивность, симметричность, транзитивность и подстановочность. Тогда Φ_0 является множеством собственных аксиом *теории полугрупп*; класс ее моделей совпадает с классом полугрупп. Пусть S – счетная полугруппа, каждая конечно порожденная подполугруппа которой вложима в какую-либо группу. Расширим теорию полугрупп добавлением к ее сигнатуре счетного множества $\{f_x^{(0)}\}_{x \in S}$ нулевых функциональных символов, индексированных

элементами из S , и рассмотрим в этой теории следующее множество формул:

$$\Delta(S) = \{f_x^{(0)} = f_y^{(0)}, f_u^{(0)} \neq f_v^{(0)}, f_x^{(0)} \cdot f_y^{(0)} = f_z^{(0)}, f_u^{(0)} \cdot f_v^{(0)} \neq f_w^{(0)} \mid x, y, z, u, v, w \in S, \text{ где } x = y, u \neq v, x \cdot y = z, u \cdot v \neq w\}.$$

Покажем, что множество формул $\Phi = \Phi_1 \cup \Delta(S)$ имеет модель. Возьмем любое конечное подмножество Ψ из Φ . Формулы из Ψ содержат лишь конечное число функциональных символов $f_{x_1}^{(0)}, \dots, f_{x_n}^{(0)}$, где $x_1, \dots, x_n \in S$. Породим в S элементами x_1, \dots, x_n подполугруппу. Она, будучи конечно порожденной, вложима по условию в некоторую группу. Очевидно, что все формулы множества Ψ истинны на последней при интерпретации, ставящей в соответствие каждому символу $f_x^{(0)}$ элемент $x \in S$. Таким образом, произвольное конечное подмножество Ψ из Φ имеет модель. Ввиду следствия 2 теоремы о компактности получаем тогда, что и само Φ имеет модель, т.е. все формулы из Φ истинны на какой-то полугруппе S' . По теореме Лёвенгейма-Сколема полугруппу S' можно выбрать счетной. Поскольку $\Phi_1 \subseteq \Phi$, делаем вывод, что S' – группа. Включение же $\Delta(S) \subseteq \Phi$ обеспечивает вложимость полугруппы S в S' .

§ 3.7. Основные проблемы формальных теорий

3.7.1. Проблема непротиворечивости

Теория \mathcal{K} называется *противоречивой*, если в \mathcal{K} существует замкнутая формула F такая, что как F , так и $\neg F$ суть теоремы теории \mathcal{K} . В противном случае \mathcal{K} называется *непротиворечивой*. Если класс моделей теории \mathcal{K} не пуст, то говорят, что \mathcal{K} *имеет модель*. Ясно, что теория \mathcal{K} непротиворечива (соответственно имеет модель) тогда и только тогда, когда система аксиом \mathcal{K} непротиворечива (соответственно имеет модель). Поэтому из теоремы о непротиворечивости и ее обращения непосредственно получаем следующее утверждение.

ТЕОРЕМА. *Произвольная теория первого порядка непротиворечива в том и только в том случае, если она имеет модель.*

Из этой теоремы вытекает непротиворечивость всех теорий первого порядка, упомянутых нами в предыдущих разделах, и в частности, теорий исчисления высказываний и исчисления предикатов.

Приведем более специфический пример, демонстрирующий силу данной теоремы.

ПРИМЕР 1. Доказать непротиворечивость теории \mathcal{K} первого порядка, заданной сигнатурой $\Sigma(\mathcal{K}) = \{P^{(2)}, f^{(1)}\}$ и собственными аксиомами

$$\begin{aligned} A_1 &= \forall x_1 \forall x_2 (P^{(2)}(x_1, x_2) \vee P^{(2)}(x_2, x_1)), \\ A_2 &= \forall x_1 \forall x_2 (P^{(2)}(x_1, x_2) \longrightarrow P^{(2)}(f^{(1)}(x_2), f^{(1)}(x_1))). \end{aligned}$$

Для доказательства непротиворечивости \mathcal{K} нам достаточно указать хотя бы одну модель теории \mathcal{K} . В качестве такой модели мы возьмем множество \mathbf{R}^+ положительных действительных чисел с двухместным предикатом естественного порядка \leq и одноместной операцией $f(x) = 1/x$; легко проверяется, что аксиомы A_1 и A_2 истинны на данной системе. Следовательно, по теореме теория \mathcal{K} непротиворечива.

Вопрос о непротиворечивости теорий привлек пристальное внимание в математике на рубеже XIX и XX столетий в связи с возникшими в теории множеств парадоксами, или, как их еще называют, *антиномиями*. Теория множеств в том виде, в каком мы ею пользуемся в данном пособии, именуемая ныне *наивной*, была разработана в 70–80-х годах XIX века немецким математиком *Георгом Кантором*. Она быстро получила почти всеобщее признание и стала широко применяться в различных разделах математики и ее приложениях. С первым парадоксом (*антиномией Бурали-Форти*), базирующимся на понятии порядкового числа, математики впервые столкнулись в 1895 году. За ним последовали и другие парадоксы теории множеств; приведем два из них.

АНТИНОМИЯ КАНТОРА (1899). Пусть \mathbf{U} – множество всех множеств. Обозначим через $\mathcal{B}(\mathbf{U})$ множество всех подмножеств из \mathbf{U} . По известной теореме Кантора, мощность множества \mathbf{U} строго меньше мощности множества $\mathcal{B}(\mathbf{U})$. С другой стороны, $\mathcal{B}(\mathbf{U}) \subseteq \mathbf{U}$ по построению. Следовательно, мощность \mathbf{U} не может быть меньше мощности $\mathcal{B}(\mathbf{U})$.

АНТИНОМИЯ РАССЕЛА (1902). Множество X назовем *обыкновенным*, если оно не содержит себя в качестве элемента, т.е. $X \notin X$, и *необыкновенным* – в противном случае. Например, обыкновенным является множество натуральных чисел \mathbf{N} , а необыкновенным – множество всех множеств \mathbf{U} . Обозначим через S множество всех обыкновенных множеств и поставим вопрос: каким является само S – обыкновенным или необыкновенным? Допустим, что

S – обыкновенное множество, т.е. $S \notin S$. Тогда оно должно, как и все обыкновенные множества, быть элементом в S , т.е. $S \in S$. Таким образом, из допущения, что S – обыкновенное множество, вытекает, что оно необыкновенно. Предположим теперь, что S – необыкновенное множество, т.е. $S \in S$. Тогда, поскольку в S входят все и только все обыкновенные множества, делаем вывод, что S обыкновенно. Опять получили противоречие.

Появившиеся в теории множеств парадоксы создали кризисную ситуацию в математике (заметим, что это уже третий по счету кризис в ее развитии; более подробную информацию об этом см. в [11]). Один из способов устранения противоречий, и тем самым выхода из кризиса, был найден в формализации теории множеств, т.е. аксиоматизации ее на языке логики первого порядка. С помощью аксиом удалось ограничить понятие множества так, чтобы в обновленной теории отсутствовали логические образования, приводящие к противоречиям, такие, например, как множества, содержащие себя в качестве элемента и т.п. В начале прошлого века появилось несколько различных вариантов аксиоматизации теории множеств. Приведем ниже наиболее известную из них – *систему аксиом Цермело-Френкеля (ZF)*. В ней два первичных понятия: множество и отношение принадлежности.

АКСИОМА ОБЪЁМНОСТИ. *Если всякий элемент множества x является элементом множества y и обратно, то $x = y$.*

$$\forall a(a \in x \longleftrightarrow a \in y) \longrightarrow x = y.$$

АКСИОМА ПУСТОГО МНОЖЕСТВА. *Существует множество, не содержащее элементов:*

$$\exists x \forall a(a \notin x).$$

Из аксиомы объёмности следует единственность такого множества; его обозначают символом \emptyset .

АКСИОМА ПАРЫ. *Для любых множеств a и b существует множество, единственными элементами которого являются a и b (как обычно, оно обозначается $\{a, b\}$ при $a \neq b$ и $\{a\}$ при $a = b$):*

$$\forall a \forall b \exists x (a \in x \wedge b \in x \wedge \forall c (c \in x \longrightarrow c = a \vee c = b)).$$

АКСИОМА СУММЫ. Для всякого множества x существует множество y , состоящее из тех и только тех элементов, которые принадлежат некоторому множеству z , принадлежащему x :

$$\forall x \exists y \forall a (a \in y \longleftrightarrow \exists z (z \in x \wedge a \in z)).$$

Это множество y является объединением семейства множеств x .

АКСИОМА СТЕПЕНИ. Для всякого множества x существует множество y , элементами которого являются подмножества множества x и только они:

$$\forall x \exists y \forall a (a \in y \longleftrightarrow \forall b (b \in a \longrightarrow b \in x)).$$

Другими словами, y есть множество всех подмножеств из x ; оно называется *булеаном* множества x .

АКСИОМА РЕГУЛЯРНОСТИ. Всякое непустое множество x содержит элемент a такой, что $a \cap x = \emptyset$:

$$\forall x (x \neq \emptyset \longrightarrow \exists a (a \in x \wedge \forall b (b \in a \longrightarrow b \notin x))).$$

АКСИОМА БЕСКОНЕЧНОСТИ. Существует такое множество x , что $\emptyset \in x$, и если $u \in x$, то множество $u \cup \{u\}$ также принадлежит x :

$$\exists x (\emptyset \in x \wedge \forall u (u \in x \longrightarrow u \cup \{u\} \in x)).$$

Эта аксиома гарантирует, по сути, наличие множества x , содержащего в качестве подмножества все натуральные числа. В самом деле, множество x , указанное в ней, удовлетворяет, очевидно, свойствам:

$$\{\emptyset\} \in x, \{\emptyset, \{\emptyset\}\} \in x, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \in x$$

и т.д. Полагая теперь $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{0, 1\}$, ..., $n = \{0, 1, \dots, n-1\}$, мы для любого целого числа $n \geq 0$ получаем включение $n \in x$, причем все так определенные числа попарно различны.

Система аксиом Цермело-Френкеля включает также *аксиому замещения*, дающую дополнительные широкие средства построения новых множеств; информацию о ней см. в [16]. Невозможность

в теории множеств Цермело-Френкеля антиномией Кантора и Рассела вытекает из аксиомы регулярности и аксиомы пары. Действительно, проверим, например, что данная система аксиом не допускает множеств, содержащих себя в качестве элемента. Предположим от противного, что это не так и потому найдется множество a такое, что $a \in a$. По аксиоме пары можно составить одноэлементное множество $x = \{a\}$ (здесь множество b совпадает с a). Тогда по аксиоме регулярности $a \cap x = \emptyset$, но это противоречит тому, что $a \in a$ и $a \in x$, т.е. $a \in a \cap x$. Заметим, что несмотря на определенные ограничения, аксиоматика Цермело-Френкеля не запрещает “слишком много” множеств. Она вполне приемлема для построения любой из известных на сегодня математических теорий: алгебры, геометрии, математического анализа и т.д.

ЗАМЕЧАНИЕ 1. Необходимо отметить, что вопрос о непротиворечивости теории множеств Цермело-Френкеля до сих пор остается открытым. Это означает, например, что доказываемые в этом учебном пособии утверждения (в частности, рассматривавшаяся ранее теорема о непротиворечивости для теорий первого порядка) являются корректными с точностью до непротиворечивости теории множеств, с которой мы имеем дело.

Любопытно также отметить, что в математике иногда возникает необходимость рассмотрения совокупностей объектов, которые не являются множествами (например, *многообразий алгебр*, см. [14]). Такие совокупности называются *классами*. Одна из принятых в математике систем аксиом – *система фон Неймана-Бернайса-Гёделя (NBG)*, см. [16] – является расширением канонической теории Цермело-Френкеля, в которой собственные классы играют роль первичных объектов наряду с множествами (собственный класс – это класс не являющийся множеством). В этой теории элементами классов могут быть только множества, и потому неприемлемо рассмотрение класса всех классов. Вместе с тем в ней допускается существование всеобщего класса – *класса всех множеств*. Как и для системы аксиом Цермело-Френкеля, непротиворечивость системы аксиом фон Неймана-Бернайса-Гёделя пока остается под вопросом.

ЗАМЕЧАНИЕ 2. Идея доказательства непротиворечивости какой-либо теории, основанная на построении соответствующей модели, впервые была осознана русским математиком *Николаем Ивановичем Лобачевским* еще в 20-х годах XIX века для обоснования

невыводимости *пятого постулата о параллельных прямых* (см. ниже) из других постулатов евклидовой геометрии. С этой целью им была создана новая геометрия, в которой имели место все аксиомы Евклида за исключением пятого постулата. Непротиворечивость этой геометрии обеспечивалась наличием модели для нее — так называемой *гиперболической плоскости Лобачевского* (указанная геометрия не является теорией первого порядка, поэтому ее модели не надо путать с теми моделями, которые мы рассматривали в этой главе) §.

В качестве дополнения к замечанию 2 приведем еще один пример.

ПРИМЕР 2. Рассмотрим несколько следующих аксиом планиметрии (см. [18]; здесь аксиома 7 соответствует пятому постулату геометрии Евклида о параллельных прямых):

1. Какова бы ни была прямая, существуют точки, принадлежащие этой прямой, и точки, не принадлежащие ей.

2. Через любые две точки можно провести прямую, и только одну.

3. Из трех точек на прямой одна и только одна лежит между двумя другими.

4. Прямая разбивает плоскость на две полуплоскости. Если концы какого-нибудь отрезка принадлежат одной полуплоскости, то отрезок не пересекает прямую. Если концы отрезка принадлежат разным полуплоскостям, то отрезок пересекает прямую.

5. Каждый отрезок имеет определенную длину, большую нуля. Длина отрезка равна сумме длин частей, на которые он разбивается любой его точкой.

6. Каждый угол имеет определенную градусную меру, большую нуля. Развернутый угол равен 180^0 . Градусная мера угла равна сумме градусных мер углов, на которые он разбивается любым лучом, проходящим между его сторонами.

7. Через точку, не лежащую на данной прямой, можно провести не более одной прямой, параллельной данной.

Доказать, что аксиома 7 не выводится из аксиом 1–6.

§ Примерно через три года после выхода работ Н. И. Лобачевского, а именно в 1832 году, была опубликована статья венгерского математика *Яноша Бойяи*, в которой он излагал похожие идеи, связанные с существованием неевклидовых геометрий.

Построим модель, которая будет удовлетворять всем аксиомам 1–6 и отрицанию аксиомы 7. Под плоскостью будем понимать открытый круг (см. рис.10), а под прямыми – хорды внутри этого круга. Всякая хорда разбивает круг на две части, называемые нами полуплоскостями. Понятия точки, отрезка и угла – такие же как в обычной геометрии. Как принято, две прямые в плоскости мы называем параллельными, если они не имеют общих точек. Хорошо видно, что в данной модели истинны все шесть первых аксиом. Однако через точку, лежащую вне произвольной прямой, можно провести более одной прямой, параллельной данной, т.е. имеет место отрицание седьмой аксиомы. Это обстоятельство доказывает, что список аксиом 1–6 вместе с отрицанием аксиомы 7 определяет непротиворечивую теорию, а значит, последняя аксиома не выводится из остальных.

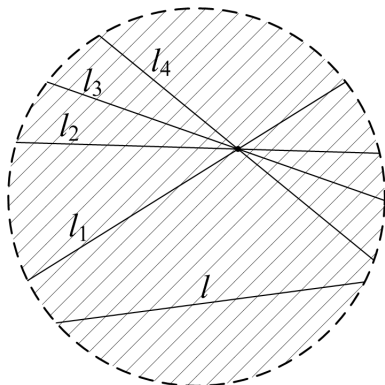


Рис.10

В следующем пункте мы продолжим для теорий первого порядка исследовать вопрос, связанный с невыводимостью аксиом одного списка из аксиом другого списка.

3.7.2. Проблема независимости аксиом

Подмножество X множества всех аксиом данной формальной теории называется *независимым*, если какая-нибудь формула из X не может быть выведена с помощью правил вывода из аксиом, не входящих в X .

ТЕОРЕМА. *Каждая из схем аксиом (A1)–(A3) теории \mathcal{T} исчисления высказываний независима.*

Доказательство. Проверим независимость (A1). Для этого построим одноместный предикат P на множестве всех формул теории \mathcal{T} , обладающий следующими свойствами:

1. $P(F) = \mathbf{1}$ для любой аксиомы из схем (A2), (A3).
2. Если $\frac{F_1, F_2}{F}$ (MP) и $P(F_1) = P(F_2) = \mathbf{1}$, то и $P(F) = \mathbf{1}$.
3. $P(A \rightarrow (B \rightarrow A)) = \mathbf{0}$.

Чтобы задать такой предикат P , рассмотрим следующие таблицы:

A	$\neg A$
0	1
1	1
2	0

A	B	$A \rightarrow B$
0	0	0
1	0	2
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	0
2	2	0

Для всякого отображения ϕ множества X логических переменных формулы F в множество значений $\{0, 1, 2\}$ эти таблицы позволяют найти соответствующее значение $\phi(F)$ (полная аналогия с тем, как вычисляются истинностные значения формул логики высказываний при интерпретациях в множестве логических констант). Например, если $\phi(A) = 0$ и $\phi(B) = 1$, то $\phi(A \rightarrow (B \rightarrow A)) = \phi(A) \rightarrow (\phi(B) \rightarrow \phi(A)) = 0 \rightarrow (1 \rightarrow 0) = 0 \rightarrow 2 = 2$. Полагаем, по определению, $P(F) = \mathbf{1}$ тогда и только тогда, когда $\phi(F) = 0$ для любой интерпретации ϕ букв формулы F в множестве $\{0, 1, 2\}$. Из определения непосредственно получаем, что $P(A \rightarrow (B \rightarrow A)) \neq \mathbf{1}$, т.е. выполнено свойство 3 выше.

Пусть $\frac{F_1, F_2}{F}$ (MP) и $P(F_1) = P(F_2) = \mathbf{1}$. Тогда для любой интерпретации ϕ в $\{0, 1, 2\}$ имеют место равенства $\phi(F_1) = \phi(F_2) = 0$. Так как F есть следствие F_1 и F_2 по правилу вывода MP, считаем, что $F_2 = F_1 \rightarrow F$. отсюда получаем $0 = \phi(F_2) = \phi(F_1 \rightarrow F) = \phi(F_1) \rightarrow \phi(F) = 0 \rightarrow \phi(F)$. По второй таблице находим, что это может быть только в одном случае, когда $\phi(F) = 0$. Поэтому $P(F) = \mathbf{1}$ ввиду произвольного выбора ϕ . Таким образом, мы проверили свойство 2 предиката P .

Из следующей таблицы видно, что $P(F) = \mathbf{1}$ для любой аксиомы $F = (\neg G \rightarrow \neg H) \rightarrow ((\neg G \rightarrow H) \rightarrow G)$ из схемы (A3):

G	H	$\neg G$	$\neg H$	$\neg G \rightarrow \neg H$	$\neg G \rightarrow H$	$(\neg G \rightarrow H) \rightarrow G$	F
0	0	1	1	2	2	0	0
1	0	1	1	2	2	0	0
2	0	0	1	2	0	2	0
0	1	1	1	2	2	0	0
1	1	1	1	2	2	0	0
2	1	0	1	2	2	0	0
0	2	1	0	2	0	0	0
1	2	1	0	2	0	2	0
2	2	0	0	0	2	0	0

Аналогично доказывається, что $P(F) = \mathbf{1}$ для любой аксиомы $F = (R \rightarrow (G \rightarrow H)) \rightarrow ((R \rightarrow G) \rightarrow (R \rightarrow H))$ из схемы (A2), и значит, справедливо свойство 1 предиката P .

Теперь осталось заметить, что из существования такого предиката P следует невозможность вывода аксиомы $A \rightarrow (B \rightarrow A)$, принадлежащей (A1), из схем аксиом (A2), (A3). Действительно, если бы она выводилась из этих аксиом, то ввиду свойств 1 и 2 предиката P имели бы $P(A \rightarrow (B \rightarrow A)) = \mathbf{1}$, но это не так по свойству 3. Независимость схемы аксиом (A1) доказана.

Аналогично проверяется независимость схем (A2) и (A3). Для каждой из них по правилу, установленному выше, строится свой одноместный предикат с необходимыми свойствами. Ниже для каждого из оставшихся двух случаев мы указываем область значений для функции ϕ , а также приводим соответствующие таблицы значений для операций \neg и \rightarrow . Читателю предоставляется возможность самостоятельно провести необходимые выкладки.

(A2): $\phi(X) = \{0, 1, 2\}$

A	$\neg A$
0	1
1	0
2	1

A	B	$A \rightarrow B$
0	0	0
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	1
1	2	0
2	2	0

$$(A3): \phi(X) = \{0, 1\}$$

A	$\neg A$
0	0
1	1

A	B	$A \rightarrow B$
0	0	0
1	0	0
0	1	1
1	1	0

Несколько более сложно устанавливается независимость схем (A1)–(A5) аксиом теории исчисления предикатов.

Исследования, связанные с независимостью аксиом в различных теориях, получили широкое распространение в математике, начиная с доказательства независимости упоминавшегося выше пятого постулата Евклида и кончая самыми современными работами по алгебре, теории множеств, логике и другим дисциплинам. В этой связи заслуживают внимания результаты американского математика Пола Джозефа Коэна (1963–1964) о независимости аксиомы выбора и гипотезы континуума для системы аксиом теории множеств Цермело-Френкеля **ZF** (см. предыдущий пункт этого параграфа). Приведем формулировку первой аксиомы.

Для множества A обозначим через $\mathcal{B}(A)$ множество всех подмножеств из A (см. аксиому степени системы аксиом Цермело-Френкеля). Отображение ψ из $\mathcal{B}(A) \setminus \{\emptyset\}$ в A такое, что $\psi(B) \in B$ для любого непустого подмножества $B \subseteq A$, называется *выбирающей функцией* для множества A .

АКСИОМА ВЫБОРА. *Для любого непустого множества существует своя выбирающая функция.*

Другими словами, если имеется произвольный набор (конечный или бесконечный) множеств, то всегда можно, выбрав из каждого множества по одному элементу, составить из этих элементов новое множество.

Данная аксиома не входит в систему аксиом **ZF**. Однако это обстоятельство никак не отражается на ее значимости для математики. До вычленения аксиомы выбора в явном виде математики использовали ее бессознательно во многих рассуждениях. Кантор неявно применил ее в 1887 году для доказательства теоремы о том, что любое бесконечное множество содержит счетное подмножество. Эта аксиома находит применение при доказательстве теоремы о том, что в любом ограниченном множестве действительных чисел всегда можно выбрать сходящуюся последовательность. Аксиома выбора используется также при построении действительных чисел

на основе системы аксиом Пеано для натуральных чисел (данную систему аксиом см. в следующем пункте).

Наряду с аксиомой выбора внимание математиков было привлечено еще к одному положению – гипотезе континуума, впервые высказанной Кантором в 1877 году. Приведем ее формулировку.

ГИПОТЕЗА КОНТИНУУМА. *Любое бесконечное подмножество множества действительных чисел либо счетно, либо имеет мощность континуума.*

Напомним, что мощность континуума – это мощность всех действительных чисел; она совпадает с мощностью множества всех подмножеств натуральных чисел. В 1940 году Гёдель доказал, что если теория **ZF** непротиворечива, то в ней не выводится отрицание аксиомы выбора, т.е. теория **ZFC**=**ZF** + (аксиома выбора) также будет непротиворечивой и, более того, непротиворечивой в этом случае будет и теория **ZFC** + (гипотеза континуума). Попытки же вывести аксиому выбора и гипотезу континуума из системы аксиом Цермело-Френкеля **ZF** или же, наоборот, доказать независимость этих положений оставались безуспешными вплоть до 60-х годов прошлого столетия, когда Коэном было установлено, что если теория **ZF** непротиворечива, то в ней невыводима аксиома выбора, а гипотеза континуума невыводима в теории **ZFC**[¶]. Из этих результатов вытекает следующее наблюдение, представляющее определенный интерес. Если мы, допуская непротиворечивость теории **ZF**, добавим к ней аксиому, являющуюся отрицанием аксиомы выбора, то получим непротиворечивую теорию, которая, вообще говоря, также имеет право на существование. Однако, очевидные сомнения возникают в целесообразности дальнейшего развития такой теории.

3.7.3. Проблемы категоричности и полноты. Теорема Гёделя о неполноте

Теория с равенством называется *категоричной*, если она имеет единственную (с точностью до несущественных различий) нормаль-

[¶] В действительности, Коэн получил более сильный результат – независимость так называемой *обобщенной гипотезы континуума*; она утверждает, что для любого бесконечного множества A между его мощностью и мощностью булеана $\mathcal{B}(A)$ не существует промежуточной мощности. Любопытно отметить, что В. Серпинский в 1947 г. и Э. Шпеккер в 1952 г. доказали, что аксиома выбора вытекает из обобщенной континуум-гипотезы.

ную модель, иначе говоря, если она непротиворечива и любые две ее нормальные модели изоморфны в обычном смысле. Примеры категоричных формальных теорий хорошо известны читателю из курсов алгебры и математического анализа. Так, любое множество аксиом X , определяющее ту или иную числовую систему \mathfrak{M} (будь то натуральные, рациональные или действительные числа) удовлетворяет одному неперемемному условию: \mathfrak{M} по X восстанавливается однозначно. Это означает, что соответствующая теория категорична и \mathfrak{M} является ее единственной нормальной моделью. Рассмотрим простейшую из таких теорий – *теорию натуральных чисел*, или, как ее обычно называют, *элементарную арифметику*. Первое аксиоматическое построение этой теории известно под названием *системы аксиом Пеано*; оно было предложено немецким математиком *Рихардом [Юлиусом Вильгельмом] Дедекиндом* в 1901 году. Аксиомы этой теории выглядят следующим образом:

(П1) 0 есть натуральное число;

(П2) для любого натурального числа x существует другое натуральное число, обозначаемое x' и называемое “*непосредственно следующее за x* ”;

(П3) $0 \neq x'$ для любого натурального числа x ;

(П4) если $x' = y'$, то $x = y$;

(П5, *принцип индукции*) если Q есть какое-то свойство натуральных чисел и оно удовлетворяет двум условиям:

(i) натуральное число 0 обладает свойством Q ,

(ii) для всякого натурального числа x из того, что x обладает свойством Q следует, что и натуральное число x' обладает свойством Q ,

то свойством Q обладают все натуральные числа.

Нетрудно понять, что арифметика, соответствующая указанной пеановской системе аксиом, является категоричной, т.е. множество \mathbf{N} натуральных чисел с естественным предикатом равенства $=$ и операциями $\{0, '\}$ образует единственную ее нормальную модель. Однако в этих аксиомах содержится интуитивное понятие “свойства”, что не позволяет всей системе быть строгой формализацией натуральных чисел. Поэтому возникает необходимость в построении теории первого порядка, основанной на пеановской аксиоматике, которая была бы так же пригодна для вывода всех основных результатов элементарной арифметики. Ниже мы указываем одну

из таких теорий, обозначаемую нами Ar и называемую *формальной арифметикой*.

Теория Ar содержит единственный предикатный символ $=$ и, в отличие от пеановской, четыре функциональных символа: нульместный 0 , одноместный $'$ и двухместные $+$ и \cdot ; последние два из них соответствуют операциям сложения и умножения на натуральных числах. Ее собственные аксиомы имеют следующий вид:

- (Ar 1) $\forall x \forall y (x = y \wedge y = z \longrightarrow x = z)$;
- (Ar 2) $\forall x \forall y (x = y \longrightarrow x' = y')$;
- (Ar 3) $\forall x (0 \neq x')$;
- (Ar 4) $\forall x \forall y (x' = y' \longrightarrow x = y)$;
- (Ar 5) $\forall x (x + 0 = x)$;
- (Ar 6) $\forall x \forall y (x + y' = (x + y)')$;
- (Ar 7) $\forall x (x \cdot 0 = 0)$;
- (Ar 8) $\forall x \forall y (x \cdot (y') = x \cdot y + x)$;
- (Ar 9) $F(0) \wedge \forall x (F(x) \longrightarrow F(x')) \longrightarrow \forall x F(x)$,

где $F(x)$ – произвольная формула теории Ar .

Заметим, что аксиомы (Ar 1)–(Ar 8) являются конкретными формулами, в то время как (Ar 9) представляет собой схему аксиом, порождающую бесконечное множество аксиом. При этом схема аксиом (Ar 9), называемая *принципом математической индукции*, не соответствует полностью аксиоме (П5) системы аксиом Пеано, поскольку в (П5) интуитивно предполагается континуум свойств натуральных чисел, а схема аксиом (Ar 9) имеет дело лишь со счетным множеством таких свойств.

К сожалению, выиграв в строгости аксиом формальной арифметики перед аксиомами Пеано, мы *неизбежно* “проигрываем” в способности этой арифметики адекватно отражать всю совокупность свойств натуральных чисел. Объективные и очень глубокие причины, объясняющие этот феномен “неизбежности”, будут вскрыты нами в конце данного пункта. Однако уже сейчас мы можем выявить расхождение указанных аксиоматик элементарной арифметики по актуальной для нас проблеме – проблеме категоричности. Если, как мы отмечали, арифметика, соответствующая пеановской аксиоматике, категорична, то формальная арифметика Ar таковой, вообще говоря, не является. Все дело в том, что *любая теория первого порядка с равенством, имеющая бесконечную нормальную модель, будет иметь и модель какой угодно бесконечной мощности* (этот факт вытекает из упомянутой в §3.6 теоремы Лёвенгейма-Сколема в усиленной формулировке), и потому она не может быть

категоричной. Поскольку теория первого порядка $\mathcal{A}r$ имеет своей моделью \mathbf{N} , она не категорична.

Таким образом, мы приходим к необходимости ослабления для теорий первого порядка свойства категоричности. Это мы сделаем, введя в рассмотрение \mathfrak{m} -категоричные теории, где \mathfrak{m} – произвольная фиксированная мощность. Теория \mathcal{K} первого порядка с равенством называется \mathfrak{m} -категоричной, если, во-первых, всякие две нормальные модели теории \mathcal{K} , имеющие мощность \mathfrak{m} , изоморфны и, во-вторых, \mathcal{K} имеет хотя бы одну нормальную модель мощности \mathfrak{m} .

Обозначим через \aleph_0 счетную мощность. Ниже приводится классический пример \aleph_0 -категоричной теории первого порядка.

ПРИМЕР 1. *Теория плотно упорядоченных множеств без наибольшего и наименьшего элементов.* Ее сигнатура содержит только предикатные символы равенства $=$ и строгого порядка $<$. Собственные аксиомы имеют вид:

- (а) $\forall x(x = x)$;
- (б) $\forall x\forall y(x = y \rightarrow y = x)$;
- (в) $\forall x\forall y\forall z(x = y \wedge y = z \rightarrow x = z)$;
- (г) $\forall x\exists y\exists z(x < y \wedge z < x)$;
- (д) $\forall x\forall y\forall z(x < y \wedge y < z \rightarrow x < z)$;
- (е) $\forall x\forall y(x = y \rightarrow x \not< y)$;
- (ж) $\forall x\forall y(x < y \vee x = y \vee y < x)$;
- (з) $\forall x\forall y(x < y \rightarrow \exists z(x < z \wedge z < y))$.

Нетрудно показать, что всякая счетная нормальная модель этой теории изоморфна множеству $(\mathbf{Q}, <)$ рациональных чисел, естественным образом упорядоченному. При этом оказывается, что данная теория не является \mathfrak{m} -категоричной ни для какого \mathfrak{m} , отличного от \aleph_0 .

ПРИМЕР 2. Укажем теорию первого порядка с равенством, которая не была бы \aleph_0 -категоричной, но была бы \mathfrak{m} -категоричной при любом $\mathfrak{m} > \aleph_0$.

С этой целью рассмотрим теорию абелевых групп (см. пример 1 из §3.6). Пусть для натурального числа n выражение nx обозначает терм $\underbrace{(\dots(x+x) + \dots + x)}_n$. Присоединим к указанной теории

новые аксиомы: $\forall x\exists!y(ny = x)$, $n = 2, 3, \dots$, что означает для любого натурального $n \geq 2$ и любого элемента x наличие *единственного*

элемента y со свойством $ny = x$. Новая теория называется *теорией абелевых групп с однозначным делением*. Указанные аксиомы позволяют определить однозначным образом результат умножения элементов группы на произвольное рациональное число, поэтому нормальные модели этой теории являются по существу линейными пространствами над полем $(\mathbf{Q}, +, \cdot)$ рациональных чисел. Хорошо известно, что любые два таких пространства одной и той же несчетной мощности изоморфны и в то же время существуют счетные не изоморфные друг другу линейные пространства над полем рациональных чисел; в качестве последних можно взять любые два конечномерных линейных пространства над этим полем, размерности которых не совпадают.

Далее мы увидим, что формальная арифметика не является m -категоричной ни для какой мощности m .

Категоричность теории связана еще с одним важным свойством – свойством полноты. Теория \mathcal{K} называется *полной*, если для любой ее замкнутой формулы F либо $\vdash_{\mathcal{K}} F$, либо $\vdash_{\mathcal{K}} \neg F$.

Из леммы 3 параграфа 3.4 вытекает, что всякая непротиворечивая теория \mathcal{K} первого порядка может быть расширена добавлением некоторого числа аксиом до полной непротиворечивой теории \mathcal{K}' (по сути, это другая формулировка леммы Линденбаума). В самом деле, пусть Γ – множество аксиом теории \mathcal{K} . Оно непротиворечиво и, следовательно, по упомянутой выше лемме содержится в некотором полном непротиворечивом множестве Γ' формул из \mathcal{K} . Возьмем Γ' в качестве множества аксиом новой теории \mathcal{K}' . Ясно, что \mathcal{K}' будет полной непротиворечивой теорией.

Один из важных способов построения полных непротиворечивых теорий дает следующий пример.

ПРИМЕР 3. Зафиксируем какую-либо алгебраическую систему \mathfrak{M} произвольной сигнатуры Σ и рассмотрим *множество Δ всех формул этой сигнатуры, истинных на \mathfrak{M}* . Пусть \mathcal{K} – теория первого порядка с сигнатурой Σ и множеством собственных аксиом, выбранных из Δ так, что *класс всех теорем \mathcal{K} совпадает с Δ* . Тогда теория \mathcal{K} полна. Действительно, для любой замкнутой формулы F из \mathcal{K} либо F истинна на \mathfrak{M} , либо $\neg F$ истинна на \mathfrak{M} . Это означает, по построению, что одна из формул F , $\neg F$ принадлежит множеству Δ , т.е. является теоремой \mathcal{K} . Теория \mathcal{K} непротиворечива, поскольку своей моделью имеет систему \mathfrak{M} .

Заметим, что мы получим теорию \mathcal{K} с указанными условиями,

если, например, возьмем в качестве множества ее собственных аксиом *все* множество формул Δ . Тогда, с одной стороны, Δ будет содержаться в множестве Th теорем теории \mathcal{K} . С другой стороны, по теореме Гёделя о полноте, каждая теорема $G \in Th$ логически общезначима в \mathcal{K} и потому G истинна на \mathfrak{M} , т.е. $G \in \Delta$. Таким образом, в этом случае множества Th и Δ совпадают, откуда, как мы видели, следует свойство полноты теории \mathcal{K} .

Связь свойства полноты формальной теории с ее категоричностью в некоторой бесконечной мощности подтверждается следующей теоремой.

ТЕОРЕМА ВООТА (1954). *Если теория \mathcal{K} первого порядка с равенством \mathfrak{m} -категорична (причем мощность \mathfrak{m} бесконечна) и не имеет конечных моделей, то \mathcal{K} полна.*

Доказательство. Допустим от противного, что \mathcal{K} неполна и, следовательно, имеется некоторая замкнутая формула F , для которой $\not\vdash_{\mathcal{K}} F$ и $\not\vdash_{\mathcal{K}} \neg F$. Тогда ввиду леммы 2 из §3.4 каждая из формул $\neg F$ и F непротиворечива. Отсюда и из того, что \mathcal{K} содержит только бесконечные модели, вытекает, как мы знаем, наличие нормальных моделей \mathfrak{M}_1 и \mathfrak{M}_2 теории \mathcal{K} мощности \mathfrak{m} , на которых соответственно истинны формулы $\neg F$ и F (см. усиленную формулировку теоремы Лёвенгейма-Сколема для теорий первого порядка с равенством из §3.6). Из условия \mathfrak{m} -категоричности получаем изоморфность моделей \mathfrak{M}_1 и \mathfrak{M}_2 , что, однако, противоречит тому, что F истинна на \mathfrak{M}_2 и ложна на \mathfrak{M}_1 .

Данная теорема позволяет легко устанавливать полноту целого ряда формальных теорий. Так, поскольку теория плотно упорядоченных множеств без наибольшего и наименьшего элементов (см. пример 1) является \aleph_0 -категоричной и, очевидно, не имеет конечных моделей, она полна. Аналогично доказывается полнота теории *нетривиальных абелевых групп с однозначным делением*. Эта теория получается из теории в примере 2 добавлением новой аксиомы $\exists x \exists y (x \neq y)$; наличие этой аксиомы обеспечивает, разумеется, бесконечность соответствующих групп.

Значительно легче привести примеры теорий, не являющихся полными, так как их в некотором смысле больше. Тем не менее в ряде случаев доказательство неполноты формальной теории бывает весьма сложным. Это относится прежде всего к следующей замечательной теореме, полученной Гёделем в 1931 году.

ТЕОРЕМА О НЕПОЛНОТЕ ФОРМАЛЬНОЙ АРИФМЕТИКИ. *Теория Ar не является полной.*

Данное утверждение означает, что существует такое высказывание о натуральных числах, записываемое формулой в сигнатуре $\{=, 0, ', +, \cdot\}$, что ни оно, ни его отрицание не доказуемы в теории Ar . В связи с этим возникает естественный вопрос: *нельзя ли каким-нибудь разумным способом расширить систему аксиом формальной арифметики* (понятно, за счет формул истинных на \mathbf{N}) *так, чтобы уже в новой теории любое высказывание о натуральных числах либо выводилось, либо опровергалось?* Слова “разумным способом” имеют тот смысл, что в полученной теории множество аксиом должно быть как-то обозримо, т.е. должен существовать алгоритм, распознающий по каждой формуле, является она аксиомой этой теории или нет. Напомним, что такая теория называется *эффективно аксиоматизированной*. Ответ на поставленный вопрос оказывается, как это ни удивительно, отрицательным и содержится в той же теореме Гёделя о неполноте, формулируемой ниже в гораздо более общем виде.

ТЕОРЕМА О НЕПОЛНОТЕ (общий случай). *Пусть S – произвольная непротиворечивая теория первого порядка с сигнатурой $\{=, 0, ', +, \cdot\}$ и собственными аксиомами, включающими аксиомы $(Ar\ 1)$ – $(Ar\ 9)$ формальной арифметики. Тогда если теория S эффективно аксиоматизирована, то она неполна.*

Ясно, что сама теория Ar является эффективно аксиоматизированной, и потому первая формулировка этой теоремы является частным случаем последней. Доказательство теоремы мы не приводим, так как для этого необходимо знать строгое определение алгоритма, и наивное его понимание, просто как некой эффективной процедуры, здесь уже не вполне пригодно.

Теорема Гёделя о неполноте по своей значимости далеко выходит за рамки не только математической логики, но и математики в целом, являясь важным элементом ее философии. Остановимся на этом чуть подробнее.

Появившиеся в математике на рубеже XIX–XX веков противоречия (см. первый пункт параграфа) и последовавшие затем попытки их устранения привели к идее формализации математической науки, т.е. построения ее на основе некоторой дедуктивной финитарной системы мышления. Указанное построение возглавил выдающийся немецкий математик *Давид Гильберт*, который к 1922 году пред-

ложил целую программу формализации или, другими словами, аксиоматизации математики. При этом на роль самого многообещающего языка этой аксиоматизации претендовал хорошо знакомый нам язык логики первого порядка. Аксиоматическое построение математики следовало начать с пострадавшего от антиномий раздела теории множеств и продолжить на другие ее разделы. В настоящей главе мы видели, в частности, как это делается для логики высказываний и логики предикатов, а также познакомились с частичной аксиоматизацией элементарной арифметики в форме теории *Ar*. Полная же аксиоматизация арифметики означает нахождение адекватной ей теории первого порядка такой, что любое истинное в ней (т.е. истинное на системе \mathbf{N} натуральных чисел) утверждение, записываемое в виде некоторой формулы сигнатуры $\{=, 0, ', +, \cdot\}$, должно быть теоремой этой теории. Предполагается, что искомая теория должна быть эффективно аксиоматизированной, иначе не было бы смысла в подобной формализации. Из гёделевского результата вытекает, что последнее не осуществимо. В самом деле, если бы эту теорию удалось построить, то она была бы полной в силу примера 3 данного пункта, а это противоречит теореме Гёделя. Таким образом, мы приходим к очень глубокому и вместе с тем печальному по своим последствиям выводу о том, что *эффективная аксиоматизация элементарной арифметики, а с ней и всей математики, невозможна*.

Из теоремы о неполноте следует еще один примечательный факт: *никакая разумная (частичная) формализация арифметики в виде некоторой теории первого порядка не будет категоричной ни в одной мощности*. Действительно, в противном случае по теореме Воота она была бы полна, что не так.

3.7.4. Проблема разрешимости

Формальная теория называется *разрешимой*, если существует алгоритм, позволяющий узнавать по любой формуле, является она теоремой данной теории или нет; в противном случае теория называется *неразрешимой*.

ТЕОРЕМА. *Теория \mathcal{T} исчисления высказываний разрешима.*

Доказательство. По теореме Гёделя о полноте (см. §3.5, следствие 1) класс теорем теории \mathcal{T} совпадает с классом тавтологий. Поэтому определить, будет ли та или иная формула теории \mathcal{T} теоремой, очень легко, исходя из ее таблицы истинности.

Ниже мы приводим весьма полезное утверждение, указывающее на тесную связь между понятиями разрешимости и полноты.

ПРИЗНАК РАЗРЕШИМОСТИ. *Всякая эффективно аксиоматизированная полная непротиворечивая теория разрешима.*

Доказательство. Допустим, что теория \mathcal{S} эффективно аксиоматизирована, полна и непротиворечива. Рассмотрим произвольную формулу F этой теории, и пусть \bar{F} – ее замыкание. Из счетности алфавита теории \mathcal{S} следует, что ее формулы можно перенумеровать с помощью натуральных чисел, из чего в свою очередь нетрудно получить пересчет s_1, s_2, \dots всех конечных последовательностей формул. Эффективная аксиоматизируемость влечет за собой существование алгоритма, с помощью которого мы можем из перечня последовательностей формул s_1, s_2, \dots отобрать только те, которые являются доказательствами, и тем самым получить эффективный пересчет p_1, p_2, \dots всех доказательств. Отсюда, поскольку теоремы – это заключительные формулы доказательств, мы получаем эффективный пересчет F_1, F_2, \dots всех теорем теории \mathcal{S} . Полнота и непротиворечивость теории \mathcal{S} гарантируют нам, что ровно одна из замкнутых формул \bar{F} или $\neg\bar{F}$ является теоремой теории \mathcal{S} , а значит, появится в указанном пересчете. В первом случае мы сделаем вывод, что как \bar{F} , так и сама формула F суть теоремы в \mathcal{S} ; во втором случае эти формулы теоремами не будут. Таким образом, нами указана эффективная процедура, позволившая для любой формулы F теории \mathcal{S} ответить на вопрос, является F теоремой теории \mathcal{S} или нет. Следовательно, теория \mathcal{S} разрешима.

Объединяя это утверждение с теоремой Вюота, мы получаем важное

СЛЕДСТВИЕ. *Всякая эффективно аксиоматизированная теория первого порядка с равенством, которая не имеет конечных моделей и категорична в некоторой бесконечной мощности, является разрешимой.*

Приведенный признак разрешимости вместе с отмеченным следствием помогает устанавливать разрешимость многих теорий, в частности, известных нам: теории плотно упорядоченных множеств без наибольшего и наименьшего элементов и теории нетривиальных абелевых групп с однозначным делением (см. предыдущий пункт).

В числе наиболее важных разрешимых теорий первого порядка следует также назвать теорию абелевых групп, теорию полей

(см. §3.6, примеры 1 и 2), теории полей действительных и комплексных чисел. Классическим примером разрешимой формальной теории является евклидова геометрия. Действительно, ее образы с помощью аппарата аналитической геометрии легко переводятся на язык алгебраических образов. Это позволяет простыми средствами алгебры доказывать или опровергать истинность геометрических положений.

Список неразрешимых теорий первого порядка содержит хорошо знакомые нам теории групп, полугрупп и колец (в том числе ассоциативных). Важным примером неразрешимой теории является *теория графов*; ее сигнатура содержит единственный двухместный предикатный символ, а моделями являются множества с определенным на них единственным бинарным отношением. Важность этого примера кроется в простоте языка теории графов, благодаря которой последний удобно интерпретируется в языках многих других теорий для доказательства их неразрешимости.

Классический пример неразрешимой теории дает

СЛЕДСТВИЕ ИЗ ТЕОРЕМЫ О НЕПОЛНОТЕ. *Теория первого порядка \mathcal{S} , теоремами которой являются все истинные на множестве \mathbf{N} натуральных чисел формулы элементарной арифметики, неразрешима.*

Доказательство. Предположим от противного, что теория \mathcal{S} разрешима. Тогда ее можно было бы эффективно аксиоматизировать, взяв в качестве множества аксиом множество всех истинных на \mathbf{N} формул. Тогда по теореме Гёделя \mathcal{S} неполна, но в то же самое время, как теория, определенная посредством единственной модели \mathbf{N} , она обязана быть полной (см. пример 3 из предыдущего пункта). Полученное противоречие доказывает неразрешимость \mathcal{S} .

Еще одним классическим образцом неразрешимой теории является теория исчисления предикатов (см. §3.2, пример 4). Впервые этот факт был установлен А. Чёрчем в 1936 году. Мы уже упоминали о нем в семантической форме, разбирая в §2.6 проблему разрешения. Напомним, что по теореме Гёделя о полноте понятие теоремы в теории исчисления предикатов адекватно понятию общезначимой формулы в логике предикатов. Поэтому неразрешимость теории исчисления предикатов равносильна отсутствию в проблеме разрешения соответствующего универсального алгоритма, распознающего общезначимые формулы.

Заметим, что доказательства на неразрешимость обычно более

трудоемки, нежели доказательства на разрешимость. Несмотря на это, неразрешимых теорий в определенном смысле гораздо больше, чем разрешимых, и последние встречаются, скорее, как исключения из общего правила.

Литература

- [1] *Важенин Ю. М.* Введение в математическую логику: Учебное пособие // Ю. М. Важенин, А. П. Замятин. – Свердловск : Изд-во Урал. Ун-та, 1984. – 93 с.
- [2] *Важенин Ю. М.* Множества, логика, алгоритмы в задачах: Учебное пособие // Ю. М. Важенин, В. Ю. Попов. – Екатеринбург : Изд-во Урал. ун-та, 1997. – 56 с.
- [3] *Ершов Ю. Л.* Математическая логика // Ю. Л. Ершов, Е. А. Палютин. – М. : Наука, 1979. – 320 с.
- [4] *Ершов Ю. Л.* Элементарные теории // Ю. Л. Ершов, И. А. Лавров, А. Д. Тайманов, М. А. Тайцлин. – Успехи математических наук. Т. 20, вып. 4 (124), 1965, с. 37–108.
- [5] *Замятин А. П.* Множества, отношения, алгебраические структуры: Учебное пособие // А. П. Замятин. – Екатеринбург : Изд-во Урал. ун-та, 2003. – 108 с.
- [6] *Замятин А. П.* Математическая логика: Учебное пособие // А. П. Замятин. – Екатеринбург : Изд-во Урал. ун-та, 2004. – 140 с.
- [7] *Игошин В. И.* Математическая логика и теория алгоритмов: Учебное пособие // В. И. Игошин. – Саратов : Изд-во Саратов. ун-та, 1991. – 256 с.
- [8] *Кислов А. Г.* Логика в гуманитарных контекстах: Учебное пособие // А. Г. Кислов. – Екатеринбург : Изд-во ЕАСИ, 2009. – 147 с.

- [9] *Клини С.* Математическая логика // С. Клини. – М. : Мир, 1973. – 480 с.
- [10] *Куратовский К.* Теория множеств // К. Куратовский, А. Мостовский. – М. : Мир, 1970. – 416 с.
- [11] *Клайн М.* Математика. Утрата определенности // М. Клайн. – М. : Мир, 1984. – 434 с.
- [12] *Лавров И. А.* Задачи по теории множеств и теории алгоритмов, 2-е изд. // И. А. Лавров, Л. Л. Максимова. – М. : Наука, 1984. – 224 с.
- [13] *Линдон Р.* Заметки по логике // Р. Линдон. – М. : Мир, 1968. – 128 с.
- [14] *Мальцев А. И.* Алгебраические системы // А. И. Мальцев. – М. : Наука, 1970. – 392 с.
- [15] *Мальцев А. И.* Алгоритмы и рекурсивные функции, 2-е изд. // А. И. Мальцев. – М. : Наука, 1986. – 368 с.
- [16] *Мендельсон Э.* Введение в математическую логику // Э. Мендельсон. – М. : Наука, 1971. – 320 с.
- [17] *Новиков П. С.* Элементы математической логики // П. С. Новиков. – М. : Наука, 1973. – 399 с.
- [18] *Погорелов А. В.* Геометрия, 7–11 классы // А. В. Погорелов. – М. : Просвещение, 2000. – 384 с.
- [19] *Робинсон А.* Введение в теорию моделей и метаматематику алгебры // А. Робинсон. – М. : Наука, 1967. – 376 с.
- [20] *Столл Р.* Множества. Логика. Аксиоматические теории // Р. Столл. – М. : Просвещение, 1968. – 231 с.
- [21] *Успенский В. А.* Теорема Гёделя о неполноте // В. А. Успенский. – М. : Наука, 1982. – 112 с.
- [22] *Чень Ч.* Математическая логика и автоматическое доказательство теорем // Ч. Чень, Р. Ли. – М. : Наука, 1983. – 360 с.
- [23] *Шенфилд Дж.* Математическая логика // Дж. Шенфилд. – М. : Наука, 1975. – 527 с.

Учебное издание

Репницкий Владимир Брониславович
Овсянников Александр Яковлевич

Основы математической логики

Редактор Е. М. Струччинская
Корректор Е. А. Зимова
Компьютерная верстка Е. В. Соколов

Подписано в печать 12.10.2015. Формат 60x80/16
Бумага для множительных аппаратов.
Печать плоская. Усл. печ. л. 6,89. Уч.-изд. л. 5,21.
Тираж 150 экз. Заказ № 1047.
Екатеринбургская академия современного искусства
620078, Екатеринбург, ул. Мира, 40а
Библиотечно-информационный центр ЕАСИ
620012, Екатеринбург, Красных партизан, 9