ВНИМАНИЕ! Эта электронная версия книги содержит
исправления ошибок и опечаток, замеченных
на АПРЕЛЬ 2016 года и ряд небольших улучшений по сравнению
с бумажной версией. Актуальная обновляемая версия книги
доступна на сайте http://inponomarev.ru.

И. Н. Пономарёв

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ И РОДЫ СТРУКТУР

Учебное пособие

Москва
МФТИ
2007

УДК 510.6+510.22(075)
ББК 22.12я73
П56

Р е ц е н з е н т ы:
кафедра «Криптология и дискретная математика»
Московского инженерно-физического института,
доктор физ.-мат. наук, профессор Ю. Н. Павловский

Пономарёв И. Н.

П56 Введение в математическую логику и роды структур: Учебное пособие. — М.: МФТИ, 2007. — 244 с.

ISBN 5-7417-0174-4

В учебном пособии, написанном по материалам семинаров, проводившихся автором в Московском физико-техническом институте, изложены элементы классической логики и аксиоматической теории множеств, а также аппарат родов структур Бурбаки. В книге применяется стандартная (не бурбаковская) терминология и аксиоматика логики и теории множеств, что позволяет использовать это пособие совместно с другими учебниками.

Предназначено для студентов младших курсов факультета инноваций и высоких технологий МФТИ. Пособие разработано в рамках инновационной образовательной программы «Разработка методического обеспечения учебного процесса» по направлению «Наукоемкие технологии и экономика инноваций».

УДК 510.6+510.22(075)
ББК 22.12я73

ISBN 5-7417-0174-4

ПРЕДИСЛОВИЕ

1. Аппарат родов структур был разработан группой французских математиков под коллективным псевдонимом «Никола Бурбаки» в 40-х годах XX в. Цель, поставленная Бурбаки, заключалась в создании универсального способа описания (экспликации) математических объектов средствами теории множеств. Бóльшая часть современных на тот момент разделов анализа, абстрактной алгебры и топологии была изложена в родах структур в многотомном трактате Н. Бурбаки «Начала математики».

Основная идея школы концептуального анализа и проектирования заключается в использовании аппарата родов структур для описания нематематических предметных областей. Такое описание производится в виде концептуальных схем — родов структур, снабжённых комментариями, указывающими на соответствие между термами и объектами описываемой предметной области. Одно из главных приложений концептуальных методов — создание автоматизированных систем управления предприятиями с использованием концептуальных схем.

Кафедра концептуального анализа и проектирования (КАиП) Московского физико-технического института готовит специалистов в этой области с 1991 года. Однако систематическое изложение математического аппарата концептуальных методов до сих пор представляет собой нерешённую задачу. Отчасти это имеет место из-за того, что оригинальное изложение аппарата родов структур, содержащееся в книге Бурбаки [15], использует специфическую терминологию и аксиоматику, отличающуюся от принятой в большинстве современных учебников по логике и теории множеств, что серьёзно затрудняет использование этой книги в учебном процессе.

Настоящая книга, основанная на семинарах, проводившихся автором на кафедре КАиП МФТИ, — первая попытка строго изложить весь необходимый для построения аппарата родов структур

материал, придерживаясь при этом терминологии и аксиоматики стандартных учебников, таких, как [1], [2], [5], и многих других, что позволяет использовать её совместно с другими учебными пособиями.

2. Что может служить отправной точкой изложения? Студенты, начинающие заниматься концептуальными методами, как правило, знакомы с понятиями и символикой математической логики и теории множеств на уровне, который требуется для усвоения стандартных программ высшей математики технического вуза. Кроме того, в нашем распоряжении имеются программные продукты с функциями синтаксического и семантического контроля родоструктурных текстов концептуальных схем. Всё это облегчает освоение формального языка родов структур. Но от знакомства с языком ещё далеко до успешной практики создания концептуальных схем — точно так же, как от знакомства с синтаксическими конструкциями языка программирования далеко до успешного программирования на этом языке. В процессе обучения требуется развить навыки преобразований логических формул и теоретико-множественных выражений, что невозможно без хотя бы базового знакомства с математической логикой и теорией множеств.

Разделы книги, посвящённые логике и теории множеств, содержат элементарные сведения, которые необходимы в процессе изложения и обоснования аппарата концептуальных методов. Из математической логики это (глава 1): исчисления высказываний и предикатов, теоремы об их непротиворечивости и полноте, а также материал, направленный на развитие навыков формального логического вывода и эквивалентных преобразований логических формул. Приступая к изучению теории множеств (глава 2), мы, таким образом, будем способны работать с теорией множеств как с аксиоматической теорией, используя формальный язык и исчисление для построения доказательств теорем. Изучение отображений и порядков позволяет не только продемонстрировать основные результаты теории множеств, связанные с мощностями и порядковыми числами, но и познакомиться с целым рядом стандартных ро-

дов структур (бинарными отношениями и множествами множеств), способами их определения и их свойствами.

Наконец, глава 3 посвящена изложению аппарата родов структур. Затрагиваются вопросы синтаксиса биективно переносимых термов и формул, приводятся примеры родов структур и их интерпретаций, описываются вывод структур и операции над родами структур. Сведения глав 1 и 2 существенным образом используются для обоснования результатов главы 3.

Текст книги снабжён упражнениями для самоконтроля. Многие из них были заимствованы из других книг — в этих случаях за номером задачи следует библиографическая ссылка.

3. На протяжении всего текста, если не оговаривается особо, используются следующие обозначения:

1) заглавные буквы латинского алфавита обозначают знакосочетания формального языка, имеющие характер высказываний или утверждений (формулы);

2) буквы Γ, $\mathcal{T}$ (возможно, с индексами) обозначают наборы замкнутых формул;

3) малые буквы латинского алфавита обозначают предметные переменные и константы (в главах 2 и 3 таковыми являются множества);

4) малые буквы греческого алфавита обозначают знакосочетания формального языка, имеющие характер объектов (термы);

5) знаками $\lhd$ и $\rhd$ отмечается начало и конец доказательства;

6) знак $\rightleftharpoons$ используется при вводе сокращающих обозначений и заменяет слова «есть по определению»;

7) утверждения главы 2, зависящие от аксиомы выбора, помечаются знаком $^\circ$.

Нумерация теорем и лемм общая и сквозная по всей книге.

ГЛАВА 1

ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

§ 1.1. Булевы функции. Пропозициональные формулы

1. *Высказывания*, или *суждения*, в естественном языке формулируются в виде повествовательных предложений. Относительно некоторых высказываний мы можем утверждать, являются они истинными или ложными. «Вода — продукт горения водорода» — пример истинного высказывания. «Все нечётные числа — простые» — пример ложного. При помощи соответствующих грамматических конструкций высказывания (как истинные, так и ложные) можно строить и в формальных языках, например: $2+2=5$, $\int_{-\infty}^{+\infty} e^{-x^2}dx = \sqrt{\pi}$.

Заметим, что истинность или ложность может быть приписана не всякому грамматически верно построенному высказыванию: так, например, относительно предложения

то, что написано в этой строке, — ложно

принципиально нельзя решить, истинное оно или ложное: оба варианта противоречат смыслу утверждения. (Приведённый пример известен как «парадокс лжеца».) Предположим, что имеем дело с набором высказываний $P_1, \dots P_n \dots$, истинность или ложность которых можно как-либо определить.

В грамматике различают простые и сложные предложения: сложное предложение состоит из предложений, соединённых союзами. При помощи союзов-связок из утверждений $P_1, \dots P_n$ можно строить новые утверждения, такие, как «P_1 и P_2», «не P_1», «если P_1 или P_2, то P_3».

Некоторые из союзов обладают важной особенностью: по истинности предложений, входящих в сложное высказывание, можно однозначно определить истинность самого сложного высказывания, построенного при помощи союза. К примеру, высказывание «P_1 и P_2» истинно в том и только том случае, когда P_1 и P_2 одновременно истинны, и ложно — во всех остальных случаях (причём утверждать это возможно вне зависимости от того, *в чём* собственно состоят P_1 и P_2).

На протяжении §§ 1.1, 1.2 мы будем изучать формы таких составных высказываний, абстрагировавшись от структуры и содержания каждого простого P_i и рассматривая все высказывания *только* в аспекте их истинности. Таким образом, в общем случае форма составного высказывания для нас представляет собой функцию n переменных, каждый аргумент и результат которой может принимать одно из двух значений: *истина* и *ложь*.

Значения *истина* и *ложь* мы, как в книге [3], обозначим готическими буквами $\mathfrak{t}$ и $\mathfrak{f}$, хотя, вообще говоря, всё равно, какие два знака принять для сокращения: $\top$ и $\bot$ или же 1 и 0. Буквы P, Q, $R\ldots$, возможно, с индексами, теперь будут обозначать *пропозициональные переменные*, которые могут принимать только значения $\mathfrak{t}$ и $\mathfrak{f}$. Функции n пропозициональных переменных, принимающие только значения $\mathfrak{t}$ и $\mathfrak{f}$, называются *булевыми функциями* n переменных.

2. Булеву функцию можно задать путём явного указания её значений на каждом наборе аргументов. Число различных наборов аргументов булевой функции n переменных равно 2^n, поэтому таблица, содержащая 2^n строк, полностью задаёт такую функцию. Например, так:

P	Q	$f(P,Q)$
$\mathfrak{f}$	$\mathfrak{f}$	$\mathfrak{t}$
$\mathfrak{f}$	$\mathfrak{t}$	$\mathfrak{f}$
$\mathfrak{t}$	$\mathfrak{f}$	$\mathfrak{t}$
$\mathfrak{t}$	$\mathfrak{t}$	$\mathfrak{f}$

Эта таблица называется *таблицей истинности* функции f.

Из возможности задать функцию таблицей истинности видно, что число не тождественных между собой булевых функций n аргументов равно числу различных наборов из 2^n истинностных значений, т. е. 2^{2^n}. Так, существует всего две функции от нуля переменных — константы $\mathfrak{t}$ и $\mathfrak{f}$, четыре функции одной переменной и т. д.

Назовём i-й аргумент булевой функции $f(P_1, \ldots P_n)$ *существенным*, если имеется такой набор значений аргументов рассматриваемой функции, при котором изменение значения одного только i-го аргумента приводит к изменению значения функции. В противном случае, i-й аргумент назовём *фиктивным*. Проще говоря, существенные аргументы — это те, от которых булева функция «действительно зависит», и их количество может быть меньше, чем «формальное» количество аргументов n. Булева функция называется *существенной*, если она не имеет фиктивных аргументов. В приведённом выше примере функции существенным является только второй аргумент, первый — фиктивный, и $f(P, Q)$ не является существенной.

Используя комбинаторику и свойства биномиальных коэффициентов, можно доказать[1], что количество существенных булевых функций n аргументов равно $\sum_{i=0}^{n} (-1)^i C_n^i 2^{2^{n-i}}$. Результаты вычисления по указанным формулам приведены в таблице:

аргументов	булевых функций (2^{2^n})	существенных булевых функций
0	2	2
1	4	2
2	16	10
3	256	218
4	65536	64594

[1] Балюк А. С., Винокуров С. Ф. и др. Избранные вопросы теории булевых функций. — М.: ФИЗМАТЛИТ, 2001. — 192 с.

3. Из четырёх булевых функций одного аргумента

P	$f_1(P)$	$f_2(P)$	$f_3(P)$	$f_4(P)$
ƒ	ƒ	t	ƒ	t
t	ƒ	ƒ	t	t

функции f_1 и f_4 несущественны (вырождены в константы t и ƒ), а f_3 тождественно повторяет аргумент. Так что нетривиальной является только $f_2(P)$, называемая операцией отрицания или операцией НЕ. Для обозначения этой функции используют специальный знак «$\neg$». С точки зрения истинностного значения $\neg P$ соответствует высказыванию «не P».

4. Каждая из десяти существенных булевых функций двух аргументов имеет своё название и обозначение. В приведённой ниже таблице функции сгруппированы так, что каждая из функций в правом столбце может быть рассмотрена как результат применения отрицания к значению соответствующей функции из левого столбца и наоборот:

P	ƒ	ƒ	t	t
Q	ƒ	t	ƒ	t
конъюнкция $P \,\&\, Q$	ƒ	ƒ	ƒ	t
дизъюнкция $P \vee Q$	ƒ	t	t	t
импликация $P \Rightarrow Q$	t	t	ƒ	t
эквивалентность $P \Leftrightarrow Q$	t	ƒ	ƒ	t
обратная импликация $P \Leftarrow Q$	t	ƒ	t	t

P	ƒ	ƒ	t	t
Q	ƒ	t	ƒ	t
штрих Шеффера $P \mid Q$	t	t	t	ƒ
стрелка Пирса $P \uparrow Q$	t	ƒ	ƒ	ƒ
коимпликация $P \not\Rightarrow Q$	ƒ	ƒ	t	ƒ
исключающее ИЛИ $P \oplus Q$	ƒ	t	t	ƒ
обратная коимпликация $P \not\Leftarrow Q$	ƒ	t	ƒ	ƒ

Особую важность для нас в дальнейшем будут иметь конъюнкция, дизъюнкция и импликация, т. к. они соотносятся с союзами естественного языка.

Конъюнкция (логическое «И») принимает значение «истина» только в том случае, когда истинны оба аргумента, и ложна во всех остальных случаях.

Дизъюнкция (логическое «ИЛИ») истинна, когда истинным является хотя бы один аргумент, и ложна только если оба аргумента ложны.

Импликация (логическое следование) соотносится с конструкцией «если..., то...», и её следует понимать так: P есть достаточное (но не обязательно необходимое) условие для Q. Т. е. если P — истинно, то для истинности всей импликации Q обязано быть истинным, если же P — ложно, то Q, вообще говоря, может быть произвольным. Таблица истинности импликации не является такой же интуитивно понятной, как для конъюнкции и дизъюнкции, поэтому для её иллюстрации уместен пример. Пусть P — утверждение «функция f дифференцируема в точке x_0», Q — «функция f непрерывна в точке x_0». Как известно, достаточным условием непрерывности в точке является дифференцируемость в этой же точке, т. е. $P \Rightarrow Q$. Легко привести примеры недифференцируемой разрывной функции (первая строка таблицы истинности импликации), недифференцируемой непрерывной функции (вторая строка таблицы), дифференцируемой непрерывной функции (четвёртая строка таблицы). Не существует лишь дифференцируемых разрывных функций.

Эквивалентность выполняет роль знака равенства: она истинна тогда и только тогда, когда её аргументы принимают одинаковые истинностные значения.

Все прочие существенные булевы функции двух аргументов получаются из четырёх перечисленных при помощи перестановки аргументов и отрицания.

Идти далее по тому же пути и изучать 218 существенных булевых функций трёх аргументов не имеет смысла, потому что, как будет показано в теореме 1, уже рассмотренных функций с избытком хватает для того, чтобы построить вообще любую булеву функцию.

5. Построим теперь формальный язык, допустимые строки ко-

торого будут формулами, выражающими те булевы функции, которые можно получить суперпозицией уже введённых ранее операций. Понятие *пропозициональной формулы* (или *пропозиционального соотношения*) определим следующим образом:

1) пропозициональная переменная (одна из букв $P, Q, R\ldots$, возможно, с индексом) есть формула;

2) если A — формула, то $\neg A$ — формула;

3) если A и B — формулы, то $(A\gamma B)$, где γ — какая-либо из связок $\&$, $\vee$, $\Rightarrow$,$\ldots$, — формула;

4) других формул не существует.

Упр. 1. [2]. Являются ли в соответствии с данным определением формулами последовательности символов «$(P \,\&\, R)R\neg P$», «$(P \,\&\, Q) \Rightarrow \Rightarrow R$», «$(((\neg P) \Rightarrow Q) \Rightarrow (R \vee S))$»? Почему?

Обязательные внешние скобки на каждом шаге построения формулы нам понадобились для того, чтобы последовательность вычисления пропозициональной формулы как выражения для булевой функции n переменных была однозначной. На практике, однако, обилие подряд идущих скобок затрудняет читаемость формулы. По этой причине вводятся соглашения, позволяющие опускать некоторые скобки без потери однозначности последовательности вычисления.

Прежде всего откажемся от внешних скобок на последнем шаге построения формулы: например, формулу

$$((P \Rightarrow Q) \vee (P \Rightarrow (Q \,\&\, P)))$$

перепишем как

$$(P \Rightarrow Q) \vee (P \Rightarrow (Q \,\&\, P)).$$

Кроме того, мы будем пользоваться соглашениями относительно приоритета выполнения логических операций (аналогично арифметическим операциям):

1. $\neg$
2. $\vee, \&$
3. $\Rightarrow, \Leftrightarrow$

Т. е. в первую очередь всегда выполняется отрицание, следом выполняются дизъюнкция и конъюнкция (между собой равноправные, аналогично умножению и делению в арифметике) и в последнюю очередь — импликация и эквивалентность (также равноправные между собой, аналогично сложению и вычитанию). Данная расстановка приоритетов предлагается, например, в [5]. Таким образом, из рассматриваемой нами формулы можно выбросить ещё пару скобок и записать

$$(P \Rightarrow Q) \vee (P \Rightarrow Q \,\&\, P).$$

6. Для построения вручную таблицы истинности булевой функции, заданной формулой алгебры высказываний, удобнее всего пользоваться *таблицей Куайна*, пример заполнения которой приведён далее:

$(P$	$\Rightarrow$	$Q)$	$\vee$	$(P$	$\Rightarrow$	Q	$\&$	$P)$
ƒ	t	ƒ	t	ƒ	t	ƒ	ƒ	ƒ
ƒ	t	t	t	ƒ	t	t	ƒ	ƒ
t	ƒ	ƒ	ƒ	t	ƒ	ƒ	ƒ	t
t	t	t	t	t	t	t	t	t

Таблица Куайна строится следующим образом.

1) Под каждую пропозициональную переменную и логический оператор выделяется столбец.

2) Столбцы под пропозициональными переменными заполняются в первую очередь, всеми возможными комбинациями значений переменных.

3) Остальные столбцы заполняются в порядке приоритета выполнения операций, на основании таблицы истинности соответствующей операции. (В нашем примере сперва заполняется столбец под конъюнкцией, далее — столбцы под импликациями и последним — столбец под дизъюнкцией.)

4) Последний заполненный столбец (в нашем примере выделен) будет столбцом значений соответствующей булевой функции.

7. Всякую формулу A, определяющую булеву функцию, в столбце значений которой находятся только $\mathbf{t}$, будем называть *тавтологией*, или *общезначимой* формулой, и обозначать $\models A$. Общезначимая формула A, таким образом, остаётся истинной при подстановке любых значений в пропозициональные переменные. Для доказательства $\models A$ достаточно проверить (например, при помощи таблицы Куайна) её значения для всех 2^n комбинаций значений пропозициональных переменных, что теоретически возможно всегда.

Примеры общезначимых утверждений приводятся в следующем упражнении. Все они будут использованы нами в дальнейшем.

Упр. 2. Докажите (при помощи таблиц Куайна), что для любых формул A и B имеют место: $\models A \vee \neg A$ — *закон исключённого третьего;* $\models \neg\neg A \Leftrightarrow A$ — *закон двойного отрицания;* $\models \neg(A \,\&\, \neg A)$ — *закон противоречия;* $\models (A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A)$ — *принцип сведения к противоречию.*

8. Формулы A и B будем называть*эквивалентными* и писать $A \sim B$, если и только если столбцы результатов их таблиц истинности совпадают.

Упр. 3. Докажите, что $A \sim B$ тогда и только тогда, когда одновременно имеет место $\models A \Rightarrow B$ и $\models B \Rightarrow A$.

Упр. 4. Докажите *законы де Мóргана* $A \vee B \sim \neg(\neg A \,\&\, \neg B)$, $A \,\&\, B \sim \sim \neg(\neg A \vee \neg B)$; *закон контрапозиции* $A \Rightarrow \neg B \sim B \Rightarrow \neg A$.

Упр. 5. Обобщите законы де Моргана на произвольное конечное количество формул, т. е. докажите, что для любого n

$$A_1 \vee \ldots \vee A_n \sim \neg(\neg A_1 \,\&\, \ldots \,\&\, \neg A_n),$$
$$A_1 \,\&\, \ldots \,\&\, A_n \sim \neg(\neg A_1 \vee \ldots \vee \neg A_n).$$

9. Теперь мы рассмотрим некоторые стандартные представления булевых функций в виде пропозициональных формул.

Теорема 1 (о функциональной полноте системы $\&, \vee, \neg$). *Любая булева функция от переменных $P_1, \dots P_n$ может быть представлена некоторой суперпозицией операций $\&$, $\vee$ и $\neg$ над переменными $P_1, \dots P_n$.*

$\lhd$Пусть функция f задана таблицей истинности

P_1	P_2		P_n	$f(P_1, \dots P_n)$
$\mathfrak{f}$	$\mathfrak{f}$	$\dots$	$\mathfrak{f}$	$f(\mathfrak{f}, \mathfrak{f}, \dots, \mathfrak{f})$
		$\dots$		
α_1^k	α_2^k	$\dots$	α_n^k	$f(\alpha_1^k, \alpha_2^k, \dots \alpha_n^k)$
		$\dots$		
$\mathfrak{t}$	$\mathfrak{t}$	$\dots$	$\mathfrak{t}$	$f(\mathfrak{t}, \mathfrak{t}, \dots, \mathfrak{t})$

Предположим сначала, что f принимает значение $\mathfrak{t}$ на строках $k_1, \dots k_p$, $p > 0$. Построим для каждой k_i-й строки формулу C_i вида

$$\neg_{\alpha_1^{k_i}} P_1 \,\&\, \neg_{\alpha_2^{k_i}} P_2 \,\&\, \dots \,\&\, \neg_{\alpha_n^{k_i}} P_n.$$

Здесь обозначение $\neg_\alpha A$ служит сокращением формулы $\neg A$, когда α принимает значение $\mathfrak{f}$, и формулы A, когда α принимает значение $\mathfrak{t}$. Иначе говоря, в выражении C_i операция отрицания перед j-й переменной ставится в том случае, когда $\alpha_j^{k_i} = \mathfrak{f}$, и не ставится, когда $\alpha_j^{k_i} = \mathfrak{t}$.

Легко проверить, что каждая формула C_i истинна тогда и только тогда, когда истинностное значение P_j есть $\alpha_j^{k_i}$ для любого $j = 1 \dots n$.

Объединив $C_1 \vee C_2 \vee \dots \vee C_p$, получим исходную функцию в виде

$$f(P_1, \dots P_n) \sim C_1 \vee C_2 \vee \dots \vee C_p.$$

Формулы данного вида называются *дизъюнктивными нормальными формами (ДНФ)*.

Заметим, что этот метод не годится для тождественно ложных функций, т. к. для построения ДНФ нужна хотя бы одна функция C_i (в начале доказательства мы сделали предположение, что $p > 0$). Заметим также, что можно подойти к решению задачи и с другой стороны.

Выделим в таблице истинности $f(P_1, \dots P_n)$ строки $l_1, \dots l_{2^n-p}$, на которых f принимает значение $\mathfrak{f}$. Построим $2^n - p$ формул D_i вида

$$\neg_{\neg\alpha_1^{l_i}} P_1 \vee \neg_{\neg\alpha_2^{l_i}} P_2 \vee \dots \vee \neg_{\neg\alpha_n^{l_i}} P_n,$$

где символ отрицания перед j-й переменной ставится в том случае, когда $\alpha_j^{l_i} = \mathfrak{t}$, и не ставится, когда $\alpha_j^{l_i} = \mathfrak{f}$. Легко видеть, что D_i ложно тогда и только тогда, когда P_j принимает значение $\alpha_j^{l_i}$ для любого $j = 1 \dots n$.

Объединив $D_1 \,\&\, D_2 \,\&\, \dots \,\&\, D_{2^n-p}$, получим исходную функцию в виде

$$f(P_1, \dots P_n) \sim D_1 \,\&\, D_2 \,\&\, \dots \,\&\, D_{2^n-p}$$

Формулы данного вида называются *конъюнктивными нормальными формами (КНФ)*. Построить КНФ можно для любой функции, не являющейся всюду истинной. Ясно, что выражение КНФ будет короче выражения ДНФ, если исходная функция чаще принимает значение $\mathfrak{f}$, чем $\mathfrak{t}$, и наоборот.▷

Упр. 6. Постройте формулу для «функции голосования» от трёх пропозициональных переменных (т. е. такой $f(P, Q, R)$, которая принимает значение $\mathfrak{t}$ в тех и только тех случаях, когда не менее двух переменных принимают значение $\mathfrak{t}$).

Ответ: $(\neg P \,\&\, Q \,\&\, R) \vee (P \,\&\, \neg Q \,\&\, R) \vee (P \,\&\, Q \,\&\, \neg R) \vee (P \,\&\, Q \,\&\, R)$.

10. *Полиномом Жегалкина n переменных* называется формула вида

$$\begin{aligned}&\varepsilon_0 \oplus (\varepsilon_1 \,\&\, P_1) \oplus (\varepsilon_2 \,\&\, P_2) \oplus \dots \oplus (\varepsilon_n \,\&\, P_n) \oplus \\ &\quad \oplus (\varepsilon_{n+1} \,\&\, P_1 \,\&\, P_2) \oplus \dots \oplus (\varepsilon_{n+C_n^2} \,\&\, P_{n-1} \,\&\, P_n) \oplus \\ &\quad \dots \\ &\quad \oplus (\varepsilon_{2^n-1} \,\&\, P_1 \,\&\, P_2 \,\&\, \dots \,\&\, P_n).\end{aligned}$$

Здесь ε_i обозначает булеву константу $\mathfrak{t}$ или $\mathfrak{f}$. Полином Жегалкина представляет из себя построенную на операторах $\oplus$ сумму, каждым слагаемым которой является конъюнкция коэффициента ε_i и некоторой выборки пропозициональных переменных (сначала по одной, затем по две, по три и так далее). Полином содержит все возможные выборки переменных, поэтому число его слагаемых равно 2^n.

Теорема 2. *Любая булева функция может быть представлена полиномом Жегалкина, и это представление единственно с точностью до перестановки слагаемых или компонент в конъюнкциях.*

$\lhd$Как и при доказательстве теоремы 1, рассмотрим таблицу истинности интересующей нас функции. Отсортируем в ней строки таким образом, чтобы первой была строка, состоящая из одних аргументов $\mathfrak{f}$, далее шли все строки, в которых только один аргумент принимает значение $\mathfrak{t}$, затем — строки с двумя аргументами, принимающими значение $\mathfrak{t}$, и т. д. до последней строки, состоящей из одних аргументов $\mathfrak{t}$.

Запишем полином Жегалкина с неопределёнными коэффициентами ε_i. Подставим во все P_i значение из первой строки отсортированной таблицы истинности, т. е. одни $\mathfrak{f}$. Эта подстановка заведомо «занулит» все слагаемые полинома, кроме ε_0. Следовательно, значение ε_0 должно быть равно $f(\mathfrak{f},\mathfrak{f},\ldots,\mathfrak{f})$.

Затем по очереди подставляем все возможные наборы переменных из строк отсортированной таблицы истинности и находим один за другим остальные коэффициенты. Легко видеть, что на i-м шаге заведомо «зануляются» все слагаемые полинома, начиная с $i+1$-го, и, если на предыдущих шагах коэффициенты ε_0, ε_1,$\ldots$ ε_{i-1} уже определены, то коэффициент ε_i также может быть выбран таким образом, чтобы функция принимала необходимое значение на заданном наборе переменных.

Таким образом, каждая булева функция может быть представлена полиномом Жегалкина. Но не равных между собой полиномов

Жегалкина не больше, чем возможных комбинаций значений коэффициентов ε_i. Для случая n переменных имеется всего 2^n коэффициентов и 2^{2^n} комбинаций, т. е. ровно столько, сколько булевых функций. Отсюда следует однозначность представления булевой функции полиномом Жегалкина.$\triangleright$

Упр. 7. Постройте полиномы Жегалкина для дизъюнкции, импликации и функции из упр. 6. Ответы: $P \vee Q \sim P \oplus Q \oplus (P \,\&\, Q)$, $P \Rightarrow Q \sim \sim \mathfrak{t} \oplus P \oplus (P \,\&\, Q)$, $(P \,\&\, Q) \oplus (P \,\&\, R) \oplus (Q \,\&\, R)$.

11. Итак, мы показали, что, используя, к примеру, одни только операции $\&, \vee, \neg$, можно построить любую булеву функцию. Но из законов де Мóргана сразу следует, что, вообще говоря, для этого достаточно набора операций $\neg$, $\&$ или $\neg$, $\vee$, из которых можно выразить все остальные.

Наборы $\{\neg, \&\}$, $\{\neg, \vee\}$ и $\{\mathfrak{t}, \mathfrak{f}, \&, \oplus\}$ — примеры *базисов* логических операций, т. е. суперпозицией входящих в них операций возможно построение любой булевой функции. Интересно, что базис может состоять и всего из одной двухместной логической операции (для этого достаточно выразить через неё операции $\neg, \&$ или $\neg, \vee$).

Упр. 8. Докажите, что наборы операций $\{|\}$, $\{\uparrow\}$, $\{\neg, \Rightarrow\}$ являются базисами.

Способность операций $|$ и $\uparrow$ служить базисом используется в цифровой электронике: для создания схемы, реализующей произвольную булеву функцию n переменных, достаточно однотипных микросхем, реализующих операции И-НЕ (или ИЛИ-НЕ).

В то же время набор операций $\&, \vee$ не является базисом по следующей причине: если все пропозициональные переменные принимают значение $\mathfrak{f}$, то любая формула, содержащая только связки $\&$, $\vee$, тоже примет значение $\mathfrak{f}$, а значит, операция $\neg$ невыразима через $\&$, $\vee$ (говорят, что эти операции «сохраняют нуль»). Вообще, любое доказательство того, что предложенная система операций не является базисом, должно основываться на том, что суперпозиция этих операций не выводит конструируемые булевы функции за пределы некоторого подкласса булевых функций. В более по-

дробных руководствах (напр., [6]) рассматривается общий критерий (Поста), определяющий, является ли набор операций базисом.

Упр. 9. [2]. Докажите, что набор операций $\{\&, \vee, \Rightarrow, \Leftrightarrow\}$ не является базисом, $\{\neg\}$ не является базисом.

Мы начали этот параграф с последовательного перебора всех возможных булевых функций, а завершаем замечанием, что всё разнообразие этих функций может быть построено с помощью единственной операции, такой, как штрих Шеффера или стрелка Пирса. Если бы мы стремились к максимальной примитивности нашего формального языка, то могли бы выбрать одну из этих операций и в дальнейшем работать только с ней, определив все остальные как сокращающие обозначения для соответствующих комбинаций. К примеру, $P \,\&\, Q$ можно было бы определить как сокращение для $(P \mid Q) \mid (P \mid Q)$. Однако формулы такого языка было бы довольно трудно воспринимать (в этом можно убедиться при выполнении упр. 8). Поэтому традиционно математическая логика пользуется четырьмя связками: $\neg$, $\&$, $\vee$, $\Rightarrow$ — которые, как уже отмечалось, соотносятся с союзами естественного языка. В дальнейшем мы также будем применять в формулах в основном только эти связки.

§ 1.2. Исчисление высказываний

1. В предыдущем параграфе мы показали, как при помощи таблиц истинности можно механическим образом решать задачи, касающиеся свойств любой пропозициональной формулы. К примеру, чтобы доказать общезначимость, достаточно вычислить истинностное значение формулы при всех комбинациях аргументов. Однако, когда мы дойдём до формул, содержащих кванторы $\exists$ и $\forall$, подобных простых методов уже не окажется в нашем распоряжении, поэтому нам необходимо познакомиться с другим, более общим подходом к работе с логическими формулами. Рассмотрим множество пропозициональных формул, построенных только при помощи связок $\Rightarrow$, $\&$, $\vee$, $\neg$, пока безотносительно их интерпретации в булевых функциях. Введём десять *схем аксиом*:

1) $A \Rightarrow (B \Rightarrow A)$.

2) $(A \Rightarrow B) \Rightarrow ((A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C))$.

3) $A \,\&\, B \Rightarrow A$.

4) $A \,\&\, B \Rightarrow B$.

5) $(A \Rightarrow B) \Rightarrow ((A \Rightarrow C) \Rightarrow (A \Rightarrow B \,\&\, C))$.

6) $A \Rightarrow A \vee B$.

7) $B \Rightarrow A \vee B$.

8) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$.

9) $(A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A)$.

10) $\neg\neg A \Rightarrow A$.

На первый взгляд этот список может показаться длинным и с трудом поддающимся запоминанию. Всё становится проще, если заметить, что схемы аксиом делятся на группы: первые две схемы задают свойства импликации, схемы 3–5 — конъюнкции, 6–8 — дизъюнкции, 9–10 — отрицания. Самая длинная вторая схема задаёт транзитивность импликации. Схемы 3–5 и 6–8 — симметричны и состоят из правил, одни из которых говорят, *что* можно получить из конъюнкции (дизъюнкции), а другие — *как* их можно получить. Девятая схема имеет отношение к способу рассуждения, известному как «сведение к противоречию». Наконец, самая простая десятая схема говорит о том, как избавиться от двух знаков отрицания, стоящих подряд.

Будем говорить, что формула E *доказуема*, или *выводима* в исчислении высказываний (и писать $\vdash E$), если выполняется хотя бы одно из следующих условий:

- формула E получается из какой-либо схемы аксиом заменой букв A, B, C на произвольные пропозициональные переменные или формулы (в этом случае мы говорим, что E является аксиомой),

- одновременно доказуемы некоторая формула A и формула $A \Rightarrow E$. В этом случае мы говорим, что E следует из доказуемости A и $A \Rightarrow E$ по правилу modus ponens, которое обозначим следующим образом:

$$\frac{\vdash A, \vdash A \Rightarrow E}{\vdash E}.$$

Выводом формулы E будем называть такую последовательность формул $B_1, \ldots B_n$, в которой каждая формула либо является аксиомой, либо следует из двух предшествующих формул предъявленной последовательности по modus ponens, и где B_n совпадает с E.

Лемма 3. *Для любой формулы A имеет место $\vdash A \Rightarrow A$.*

$\lhd$Продемонстрируем вывод:

1) $A \Rightarrow (A \Rightarrow A)$ — схема 1 (B заменено на A),

2) $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$ — схема 1 (B заменено на $A \Rightarrow A$),

3) $(A \Rightarrow (A \Rightarrow A)) \Rightarrow ((A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow (A \Rightarrow A))$ — схема 2 (B заменено на $A \Rightarrow A$, C заменено на A),

4) $(A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow (A \Rightarrow A)$ — modus ponens из шагов 1 и 3,

5) $A \Rightarrow A$ — modus ponens из шагов 2, 4.$\rhd$

2. На нынешнем уровне развития теории тот факт, что для формулы $A \Rightarrow A$ найден вывод, можно считать случайностью. Проявив изобретательность, мы, наверное, могли бы найти вывод и для некоторых других формул, но такой неформальный процесс поиска вывода не имел бы ничего общего с механической работой по построению таблиц истинности (к примеру, нам не составило бы труда доказать тот факт, что $\models A \Rightarrow A$). Естественно поставить

вопрос: как определить доказуемость или недоказуемость формулы в общем случае? Ответ даёт утверждение, которое мы докажем в этой главе: пропозициональная формула доказуема тогда и только тогда, когда она общезначима, т. е. в действительности знаки $\vdash$ и $\models$ взаимозаменяемы, а поиск вывода можно заменить построением таблиц истинности. Доказать это в одну сторону мы можем уже сейчас.

Теорема 4. *Всякая доказуемая формула общезначима.*

$\lhd$Пусть $\vdash B$ и дан вывод $B_1, \dots B_n$. Покажем по индукции, что все формулы в выводе общезначимы, а следовательно, общезначимо B.

Всякая аксиома общезначима. Действительно: формулы, выражающие схемы аксиом 1–10 — общезначимы, в чём можно убедиться при помощи таблиц истинности. Следовательно, будут общезначимы и все формулы, получаемые из схем аксиом подстановкой других формул вместо букв A, B, C.

Заметим, что B_1 обязана быть аксиомой, следовательно, $\models B_1$.

Каждая $B_i (i > 1)$ является либо аксиомой (и тогда $\models B_i$), либо получена по modus ponens из предшествующих формул, которые можно считать общезначимыми по предположению индукции.

Если $\models B_j \Rightarrow B_i$ $(j < i)$, то, по определению импликации, исключается случай, когда B_j — истинно, а B_i — ложно. Но $\models B_j$ означает, что B_j — истинно на любом наборе пропозициональных переменных. Следовательно, $\models B_i$.$\rhd$

Следствие. *Ни для какой формулы B не может быть одновременно $\vdash B$ и $\vdash \neg B$.*

$\lhd$Пусть B — доказуема, тогда по теореме 4 столбец значений таблицы истинности для B содержит только единицы, а формулы $\neg B$ — только нули. Но если допустить, что $\neg B$ также доказуема, то столбец значений формулы $\neg B$ должен содержать только единицы. Противоречие.$\rhd$

Доказать утверждение, обратное теореме 4, гораздо сложнее, и нам для этого потребуется развить навыки работы с выводом и рассмотреть ряд вспомогательных теорем.

3. В обычных рассуждениях мы часто применяем такой метод: допускаем, что какие-то утверждения истинны, и смотрим, какие логические следствия получаются из этого допущения. Введём такую возможность в исчисление высказываний. Будем говорить, что формула E *выводима из посылок* $A_1,\dots A_n$ и писать $A_1,\dots A_n \vdash E$, если мы можем предоставить последовательность формул $B_1,\dots B_n$, в которой каждая формула либо является одной из посылок $A_1,\dots\ A_n$, либо аксиомой, либо непосредственно следует из двух предшествующих формул предъявленной последовательности по modus ponens, и где B_n совпадает с E.

Упр. 10. Используя определение, докажите, что если имеет место $\Gamma_1 \vdash A$ и $\Gamma_2, A \vdash B$, то $\Gamma_1, \Gamma_2 \vdash B$, где A, B — произвольные формулы, Γ_1, Γ_2 — произвольные последовательности формул.

Упр. 11. Докажите, что $A \Rightarrow B, B \Rightarrow C, A \vdash C$.

Теорема 5 (о дедукции в исчислении высказываний)**.** *Для любого набора формул* Γ *и формул* A, B *имеет место* $\Gamma, A \vdash B$ *тогда и только тогда, когда* $\Gamma \vdash A \Rightarrow B$.

$\lhd$В одну сторону утверждение является, по сути, переформулировкой правила modus ponens. Действительно: пусть $\Gamma \vdash A \Rightarrow B$, т. е. существует вывод формулы $A \Rightarrow B$ из посылок Γ. Тогда, если добавить A к числу посылок, B будет выводима из $A \Rightarrow B$ и A по modus ponens.

Докажем обратное утверждение. Пусть $B_1,\dots B_n$ — вывод формулы B из набора посылок Γ и посылки A. Добавим к каждой формуле вывода импликацию из A, так что у нас получится список $A \Rightarrow B_1,\dots A \Rightarrow B_n$ (т. к. B_n совпадает с B, то в конце списка у нас будет формула $A \Rightarrow B$). Сам по себе этот список ещё не является доказательством формулы $A \Rightarrow B$, но мы покажем, что его можно дополнить до доказательства.

Действительно, для каждой из формул $B_1,\dots B_n$ имеет место один из четырёх случаев: она либо является аксиомой, либо сов-

падает с одной из формул Γ, либо совпадает с A, либо выводится из двух предшествующих по modus ponens.

1) Если B_i есть A, то по лемме 3 доказуемо $A \Rightarrow A$ (безо всяких посылок), поэтому мы добавляем перед $A \Rightarrow A$ её вывод.

2) Если B_i принадлежит Γ, то по первой схеме $B_i \Rightarrow (A \Rightarrow B_i)$, применяя modus ponens к B_i и последней формуле, получаем $\Gamma \vdash A \Rightarrow B_i$.

3) То же самое, если B_i является аксиомой.

4) Наконец, пусть B_i получается по modus ponens из B_j и $B_j \Rightarrow \Rightarrow B_i$, $j < i$. По второй схеме аксиом имеем

$$\vdash (A \Rightarrow B_j) \Rightarrow ((A \Rightarrow (B_j \Rightarrow B_i)) \Rightarrow (A \Rightarrow B_i)).$$

Т. к. $j < i$, $A \Rightarrow B_j$ можно считать доказуемой из Γ и по modus ponens

$$\Gamma \vdash (A \Rightarrow (B_j \Rightarrow B_i)) \Rightarrow (A \Rightarrow B_i).$$

Построим вывод левой части импликации. По первой схеме

$$\vdash (B_j \Rightarrow B_i) \Rightarrow (A \Rightarrow (B_j \Rightarrow B_i)),$$

из $\Gamma \vdash B_j \Rightarrow B_i$ имеем $\Gamma \vdash A \Rightarrow (B_j \Rightarrow B_i)$, и окончательно $\Gamma \vdash A \Rightarrow B_i$.

Мы доказали, что $\Gamma \vdash A \Rightarrow B_i$ для всех $i = 1, \ldots n$, а значит, и $\Gamma \vdash A \Rightarrow B$.$\triangleright$

Упр. 12. [6]. Докажите, что для любых A, B, C имеет место

$$\vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$$

(указание: используйте теорему 5 и результат упражнения 11).

4. Теорема о дедукции позволит нам сокращать вывод формул, а также обосновать целый ряд дополнительных правил вывода, которые можно использовать в исчислении высказываний.

Теорема 6 (правила введения и удаления)**.** *Для любых формул* A, B, C *и списка формул* Γ *справедливы следующие правила вывода:*

	введение	удаление
$\Rightarrow$	$\dfrac{\Gamma, A \vdash C}{\Gamma \vdash A \Rightarrow C}$	$\dfrac{\Gamma \vdash A \Rightarrow C}{\Gamma, A \vdash C}$
$\&$	$A, B \vdash A \,\&\, B$	$A \,\&\, B \vdash A$, $A \,\&\, B \vdash B$
$\vee$	$A \vdash A \vee B$, $B \vdash A \vee B$	$\dfrac{\Gamma, A \vdash C;\ \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$ (доказательство разбором случаев)
$\neg$	$\dfrac{\Gamma, A \vdash C;\ \Gamma, A \vdash \neg C}{\Gamma \vdash \neg A}$ (reductio ad absurdum)	$A, \neg A \vdash C$ (слабое $\neg$-удаление) $\neg\neg A \vdash A$ (сильное $\neg$-удаление, или $\neg\neg$-удаление)

◁Действительно:

- $\Rightarrow$-введение и $\Rightarrow$-удаление доказаны теоремой 5;
- $\&$-введение: продемонстрируем сокращённый вывод:
  1) $\vdash (A \Rightarrow A) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow A \,\&\, B))$ — схема 5,
  2) $\vdash (A \Rightarrow B) \Rightarrow (A \Rightarrow A \,\&\, B)$ — modus ponens к шагу 1 и лемме 3,
  3) $B \vdash A \Rightarrow B$ — схема 1 и $\Rightarrow$-удаление,
  4) $B \vdash A \Rightarrow A \,\&\, B$ — результат упр. 10 к шагам 2, 3,
  5) $A, B \vdash A \,\&\, B$ — $\Rightarrow$-удаление к шагу 4;
- $\&$-удаление есть результат $\Rightarrow$-удаления из схем 3, 4;
- $\vee$-введение есть результат $\Rightarrow$-удаления из схем 6, 7;
- доказательство разбором случаев:
  1) $\Gamma \vdash A \Rightarrow C$ — $\Rightarrow$-введение к первому соотношению,
  2) $\Gamma \vdash B \Rightarrow C$ — $\Rightarrow$-введение ко второму соотношению,
  3) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$ — схема 8,
  4) $\Gamma \vdash (B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C)$ — modus ponens из шагов 1 и 3,
  5) $\Gamma \vdash A \vee B \Rightarrow C$ — modus ponens из шагов 2 и 4;
- $\neg$-введение:
  1) $\Gamma \vdash A \Rightarrow C$ — $\Rightarrow$-введение к первому соотношению,
  2) $\Gamma \vdash A \Rightarrow \neg C$ — $\Rightarrow$-введение ко второму соотношению,
  3) $(A \Rightarrow C) \Rightarrow ((A \Rightarrow \neg C) \Rightarrow \neg A)$ — схема 9,
  4) $\Gamma \vdash (A \Rightarrow \neg C) \Rightarrow \neg A$ — modus ponens из шагов 1, 3,
  5) $\Gamma \vdash \neg A$ — modus ponens из шагов 2, 4;
- $\neg\neg$-удаление есть результат $\Rightarrow$-удаления из схемы 10;
- $\neg$-удаление:

1) $\neg C, A, \neg A \vdash A$,

2) $\neg C, A, \neg A \vdash \neg A$,

3) $A, \neg A \vdash \neg\neg C$ — $\neg$-введение к шагам 1, 2,

4) $\neg\neg C \vdash C$ — $\neg\neg$-удаление,

5) $A, \neg A \vdash C$ — результат упр. 10 к шагам 3, 4.$\triangleright$

Обратим особое внимание на то, что правило $\neg$-удаления, по сути, гласит: *при наличии противоречивых посылок доказуемо всё, что угодно.*

5. Правила введения и удаления дают нам новый и очень эффективный способ построения вывода формул: даже если формула выводится безо всяких посылок, мы можем начать с утверждений о выводимости из посылок, а затем «перебросить» все посылки направо от знака выводимости. Примером применения этой методики служит доказательство следующей леммы.

Лемма 7 (закон исключённого третьего)**.** $\vdash A \vee \neg A$.

$\triangleleft$Продемонстрируем вывод:

1) $\neg(A \vee \neg A), A \vdash A \vee \neg A$ — $\vee$-введение,

2) $\neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)$,

3) $\neg(A \vee \neg A) \vdash \neg A$ — $\neg$-введение к шагам 1, 2,

4) $\neg(A \vee \neg A), \neg A \vdash A \vee \neg A$ — $\vee$-введение,

5) $\neg(A \vee \neg A), \neg A \vdash \neg(A \vee \neg A)$,

6) $\neg(A \vee \neg A) \vdash \neg\neg A$ — $\neg$-введение к шагам 4, 5,

7) $\vdash \neg\neg(A \vee \neg A)$ — $\neg$-введение к шагам 3, 6,

8) $\vdash A \vee \neg A$ — $\neg\neg$-удаление.$\triangleright$

Упр. 13. Используя правила введения и удаления, докажите

$$\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$$

(указание: достаточно получить противоречие из посылок $(A \Rightarrow B), \neg B, A$).

Упр. 14. Используя правила введения и удаления, докажите законы де Моргана (необходимо доказать четыре соотношения: $\neg(A \vee B) \vdash \neg A \,\&\, \neg B$, $\neg(A \,\&\, B) \vdash \neg A \vee \neg B$ и обратные им).

Частичное решение. Докажем $\neg(A \vee B) \vdash \neg A \,\&\, \neg B$:

1) $\neg(A \vee B), A \vdash A \vee B$ — $\vee$-введение,

2) $\neg(A \vee B), A \vdash \neg(A \vee B)$,

3) $\neg(A \vee B) \vdash \neg A$ — $\neg$-введение к шагам 1, 2,

4) $\neg(A \vee B) \vdash \neg B$ (аналогично шагам 1–3),

5) $\neg(A \vee B) \vdash \neg A \,\&\, \neg B$ — &-введение к шагам 3, 4.

Докажем $\neg A \vee \neg B \vdash \neg(A \,\&\, B)$:

1) $\neg A, A \,\&\, B \vdash A$ — &-удаление,

2) $\neg A, A \,\&\, B \vdash \neg A$,

3) $\neg A, \vdash \neg(A \,\&\, B)$ — $\neg$-введение к шагам 1, 2,

4) $\neg B \vdash \neg(A \,\&\, B)$ (аналогично шагам 1–3),

5) $\neg A \vee \neg B \vdash \neg(A \,\&\, B)$ — $\vee$-удаление к шагам 3, 4.

Упр. 15. [6]. Используя правила введения и удаления, докажите

$$\begin{gathered}(A \Rightarrow B) \Rightarrow C \vdash B \Rightarrow C,\\ A \vee B \Rightarrow C \vdash (A \Rightarrow C) \,\&\, (B \Rightarrow C),\\ (A \,\&\, C) \vee (B \,\&\, C) \vdash (A \vee B) \,\&\, C,\\ (A \,\&\, B) \vee C \vdash (A \vee C) \,\&\, (B \vee C),\\ (A \vee B) \,\&\, C \vdash (A \,\&\, C) \vee (B \,\&\, C),\\ (A \vee C) \,\&\, (B \vee C) \vdash (A \,\&\, B) \vee C.\end{gathered}$$

(указание: при необходимости воспользуйтесь законами де Моргана).

6. Следующие две леммы установят связь между «миром булевых функций» и «миром исчисления высказываний», после чего мы сможем доказать главную теорему этого раздела.

Лемма 8. *Для произвольных формул A и B имеют место следующие 14 утверждений о выводимости:*

$$\begin{array}{rcrlll}
\neg A & \vdash & \neg A & & \\
A & \vdash & \neg\neg A & & \\
\neg A, & \neg B & \vdash & A \Rightarrow B & \neg(A \,\&\, B) & \neg(A \vee B) \\
\neg A, & B & \vdash & A \Rightarrow B & \neg(A \,\&\, B) & A \vee B \\
A, & \neg B & \vdash & \neg(A \Rightarrow B) & \neg(A \,\&\, B) & A \vee B \\
A, & B & \vdash & A \Rightarrow B & A \,\&\, B & A \vee B
\end{array}$$

◁Какие-то из этих утверждений уже доказаны теоремой 6, сокращённые доказательства большинства остальных просты и не превышают трёх-четырёх строк, например:

1) $A, \neg B, A \Rightarrow B \vdash B$ — modus ponens из A, $A \Rightarrow B$,

2) $A, \neg B, A \Rightarrow B \vdash \neg B$,

3) $A, \neg B \vdash \neg(A \Rightarrow B)$ — reductio ad absurdum из шагов 1, 2.

Изобретательности, пожалуй, требует только доказательство утверждения $\neg A, \neg B \vdash \neg(A \vee B)$:

1) $\neg A, \neg B, B \vdash B$,

2) $\neg A, \neg B, A \vdash B$ — $\neg$-удаление (противоречивы $\neg A$, A),

3) $\neg A, \neg B, A \vee B \vdash B$ — разбор случаев из шагов 1, 2,

4) $\neg A, \neg B, B \vdash \neg B$,

5) $\neg A, \neg B, A \vdash \neg B$,

6) $\neg A, \neg B, A \vee B \vdash \neg B$ — разбор случаев из шагов 4, 5,

7) $\neg A, \neg B \vdash \neg(A \vee B)$ — reductio ad absurdum из шагов 3, 6.

(Но если использовать закон де Моргана, то и в этом случае доказательство будет тривиальным: $\neg A, \neg B \vdash \neg A \& \neg B \vdash \neg(A \vee B)$.)▷

Упр. 16. Докажите остальные 12 утверждений леммы 8.

Лемма 9. *Пусть F — произвольная формула, построенная из n пропозициональных переменных $A_1, \dots A_n$. Тогда для каждой строки таблицы истинности формулы F имеет место соответствующее утверждение о выводимости: если $F(\alpha_1, \dots \alpha_n) = \alpha$, то*

$$\neg_{\alpha_1} A_1, \neg_{\alpha_2} A_2, \dots \neg_{\alpha_n} A_n \vdash \neg_\alpha F.$$

Как и в доказательстве теоремы 1, $\neg_\alpha F$ обозначает формулу F, если $\alpha = \mathfrak{t}$, и $\neg F$, если $\alpha = \mathfrak{f}$.

◁Заметим, что если формула содержит в себе только один логический оператор, то мы имеем случаи, доказанные леммой 8. Общее утверждение можно доказать индукцией по построению формулы F. Применяя лемму 8, можно построить соответствующие утверждения о выводимости для всех подформул формулы F, поднимаясь от пропозициональных переменных к самой формуле.▷

Теорема 10 (о полноте исчисления высказываний)**.** *Всякая общезначимая формула исчисления высказываний доказуема.*

◁Пусть F построена из n пропозициональных переменных. Если $\models F$, то в силу леммы 9 из 2^n наборов посылок выводится она, а не её отрицание. Покажем, что F можно вывести безо всяких посылок.

Сгруппируем соотношения выводимости в 2^{n-1} пар вида

$$A_1, \neg_{\alpha_2} A_2, \dots \neg_{\alpha_n} A_n \vdash F,$$

$$\neg A_1, \neg_{\alpha_2} A_2, \dots \neg_{\alpha_n} A_n \vdash F.$$

По правилу разбора случаев получим 2^{n-1} соотношений вида

$$A_1 \vee \neg A_1, \neg_{\alpha_2} A_2, \dots \neg_{\alpha_n} A_n \vdash F,$$

и в силу леммы 7

$$\neg_{\alpha_2} A_2, \dots \neg_{\alpha_n} A_n \vdash F,$$

где фигурируют только $n - 1$ посылок. Повторив процесс n раз, получим $\vdash F$, что и требовалось.▷

§ 1.3. Язык логики предикатов

1. Рассматривая формулы алгебры исчисления высказываний, мы отвлеклись от природы входящих в них переменных, которые интересовали нас лишь в аспекте истинностного значения. Тот факт, что пропозициональные переменные представляют собой высказывания, до сих пор никак не использовался. Теперь мы продвинемся глубже и рассмотрим высказывание само по себе.

Из школьного курса грамматики известно, что обычным образом построенное предложение имеет подлежащее и сказуемое, или, если пользоваться латинскими терминами, субъект и предикат. К примеру, в предложении «Сократ — человек» слово «Сократ» является субъектом, а «человек» — предикатом. Мы будем понимать термины «субъект» и «предикат» несколько шире, чем лингвисты: всё то, *о чём* говорится в высказывании, мы назовём субъектами, а всё то, *что* говорится — предикатом.

Таким образом, для нас часть высказывания, выражаемая шаблоном «x — человек», будет представлять собой предикат, из которого получится истинное высказывание, если в качестве субъекта (вместо переменной x) подставить «Сократ», и ложное, если субъект — «Хирон» (кентавр). Можно рассмотреть предикат «x в нормальных условиях кипит при 100 °C», дающий истинное высказывание, если субъект — «вода», и ложное, если субъект — «олово». Таким образом, мы приходим к пониманию предиката как *функции*, принимающей значения $\mathfrak{t}$ и $\mathfrak{f}$ в зависимости от подставляемых в неё аргументов. Мы рассматривали предикаты только одного аргумента (одноместные), вот пример двухместного предиката: «x муж y», дающий истинное высказывание, если в качестве первого и второго субъектов выступают соответственно «Сократ» и «Ксантиппа», и ложное, скажем, в случае субъектов «Вронский» и «Анна Каренина». Пример трёхместного предиката: «$x + y = z$», дающий $\mathfrak{t}$ для набора субъектов «2, 2, 4» и $\mathfrak{f}$ для «1, 1, 1». Наконец, можно рассмотреть и нуль-местные предикаты: предикаты, не требующие субъектов; различных между собой нуль-местных предикатов всего два: $\mathfrak{t}$ и $\mathfrak{f}$.

Подведём итог. Пусть дано непустое множество M, которое назовём *предметной областью*. *n-местным предикатом* на множестве M называется функция, ставящая в соответствие каждому упорядоченному набору n элементов множества M одно из значений $\mathfrak{t}$ или $\mathfrak{f}$. Предикаты, таким образом, принимают те же значения, что и булевы функции, но коренное отличие в том, что предикат может быть определён на произвольном множестве.

На данном этапе мы можем воспринимать *множества* и *функции* как некие умозрительные объекты: множество — как совокупность объектов, рассматриваемую как единое целое, и функцию — как некоторый закон, согласно которому каждому объекту-аргументу (или набору объектов-аргументов) поставлен в соответствие один единственный результат. Разумеется, это нельзя считать определением понятий «множество» и «функция», более формальный разговор о которых пойдёт в гл. 2. Но там потребуется определённый навык вывода в *исчислении предикатов*, приобрести который на практике, по-видимому, невозможно без начальных рассуждений о предметных областях, моделях и оценках, так или иначе задействующих термин «множество».

Для обозначения предикатов в формулах будет использоваться набор символов (как правило, заглавных латинских букв P, Q, $R\ldots$, возможно, с индексами), называемых *предикатными символами*. Для обозначения элементов предметной области в формулах будет использоваться набор строчных латинских букв, возможно, с индексами, называемых *термами*. Понятие *терм* в общем случае означает некоторое выражение, указывающее на объект (в отличие от *формулы*, которая имеет характер высказывания об одном или нескольких объектах).

2. *Сигнатурой* σ называется произвольный набор термов $c_1,\ldots c_l$ (*предметных констант*), а также предикатных символов $P_1,\ldots P_k$, обладающих целыми неотрицательными *валентностями* $n_1,\ldots n_k$[2]. Определим, какие цепочки символов

[2] Для упрощения изложения намеренно игнорируются «функциональные символы», традиционно входящие в определение сигнатуры, т. к. для постро-

являются *формулами* (или *соотношениями*) *сигнатуры*, пока что не рассматривая их смысл:

1) Константы сигнатуры $c_1, \dots c_l$ и буквы $x_1, \dots x_n$, называемые *индивидными переменными*, являются *термами* сигнатуры. Предполагается, что, глядя на выражение, всегда можно различить, где малая латинская буква в нём обозначает константу, а где — переменную.

2) Если P — предикатный символ валентности n сигнатуры, а $t_1, \dots t_n$ — термы, то цепочка символов

$$P(t_1, \dots t_n)$$

называется *атомарной формулой сигнатуры*. Кроме того, любой предикатный символ нулевой валентности есть атомарная формула сигнатуры. Атомарная формула сигнатуры есть формула сигнатуры.

3) Если A — формула сигнатуры, то $\neg A$ — формула сигнатуры.

4) Если A и B — формулы, а γ — какая-либо из логических связок $\vee$, $\&$, $\Rightarrow$, то $(A\,\gamma\,B)$ — формула сигнатуры.

5) Если A — формулы сигнатуры, x — индивидная переменная, а Q — какой-либо из кванторов $\forall$, $\exists$, то $\mathsf{Q}xA$ — формула сигнатуры.

6) Других формул не существует.

К примеру, если σ содержит предикатные символы P, Q и R валентностей 2, 1 и 2 соответственно, то цепочка символов

ения аксиоматической теории множеств и аппарата родов структур без функциональных символов можно обойтись.

$$\neg\forall x(P(x,y)\,\&\,\exists z(Q(z)\vee R(z,y)))$$

является корректной формулой σ.

Упр. 17. Найдите все подформулы указанной формулы.

Легко видеть (ср. определение пропозициональной формулы на с. 12), что из любой пропозициональной формулы можно построить формулу сигнатуры, если вместо пропозициональных переменных подставить формулы сигнатуры. Применяя соглашения о приоритете логических операций, введённые на с. 12, в формулах сигнатур мы также будем опускать избыточные скобки, когда это не ведёт к разночтениям. Примем, кроме того, соглашение, по которому при отсутствии группирующих скобок квантор действует только на первую следующую за ним подформулу, т. е. выражение $\exists xP(x)\,\&\,Q(y)$ интерпретируется как $(\exists xP(x))\,\&\,Q(y)$.

Упр. 18. [2]. Покажите, что выражение $\exists n\forall x_1\ldots\forall x_n(P(x_1)\,\&\ldots\&\,\&\,P(x_n))$, где P — одноместный предикат, не является формулой. Указание: является ли n индивидной переменной?

3. Теперь мы можем определить, что такое *модель* $\mathfrak{M}$ сигнатуры σ, *оценка* π в модели $\mathfrak{M}$ и *истинностное значение* формулы A сигнатуры σ на оценке π.

Моделью $\mathfrak{M}$ сигнатуры σ называются: непустое множество M (предметная область), набор элементов этого множества, соответствующих предметным константам $c_1,\ldots c_l$, и такой набор определённых на данном множестве предикатов, что каждому предикатному символу валентности n из σ соответствует один и только один n-местный предикат из $\mathfrak{M}$. Ясно, что сигнатура может иметь много моделей. Например, если в сигнатуре содержится один предикатный символ P валентности 3, то её моделями могут быть, например, такие: M — множество натуральных чисел, предикат для символа P есть «$x+y=z$»; M — множество точек плоскости, предикат для символа P есть «точки x, y и z лежат на одной прямой».

Оценкой π в модели $\mathfrak{M}$ называется набор элементов множества M, поставленный в соответствие индивидным переменным таким образом, что каждой индивидной переменной соответству-

ет один и только один элемент множества M. Другими словами, задавая оценку, мы указываем, каким именно элементам M соответствуют переменные, участвующие в рассматриваемых нами формулах. Для того чтобы сослаться на элемент M, обозначаемый буквой x на оценке π, будем пользоваться, как в книге [6], обозначением $[x]\pi$. (Естественно, константы будут обозначать один и тот же элемент на любой оценке — их значения задаются уже моделью.)

Наконец, *истинностное значение* формулы A сигнатуры σ на оценке π, равное $\mathfrak{t}$ или $\mathfrak{f}$ и обозначаемое $[A]\pi$, определяется следующим образом:

1) Истинностное значение атомарной формулы $P(x_1, \ldots x_n)$ есть результат подстановки в предикат, соответствующий символу P, элементов $[x_1]\pi, \ldots [x_n]\pi$, т. е. $[P(x_1, \ldots x_n)]\pi = P([x_1]\pi, \ldots [x_n]\pi)$.

2) $[\neg A]\pi = \neg([A]\pi)$.

3) $[A \gamma B]\pi = [A]\pi \gamma [B]\pi$ (пп. 2 и 3, по-видимому, в комментариях не нуждаются).

4) Формула $\exists x A$ (которая читается «существует такой x, что A») является истинной тогда и только тогда, когда существует хотя бы одна оценка π', отличающаяся от π *только* значением переменной x, такая, что $[A]\pi' = \mathfrak{t}$.

   Когда предметная область M состоит из конечного числа элементов $m_1, \ldots m_N$, формула $\exists x A$ сводится к обычной дизъюнкции по всем элементам M: $[\exists x A]\pi = [A](\pi + x \mapsto m_1) \vee \vee \ldots \vee [A](\pi + x \mapsto m_N) = \bigvee\limits_{i=1}^{N} [A](\pi + x \mapsto m_i)$.

   Здесь $\pi + x \mapsto m_i$ обозначает, как в книге [6], оценку, отличающуюся от π только значением переменной x, такую, что $[x](\pi + x \mapsto m_i) = m_i$. Для случая, когда M состоит из произвольного (возможно, бесконечного) количества элементов,

нам потребуется «всеобщая дизъюнкция»:

$$[\exists x A]\pi = \bigvee_{m \in M} [A](\pi + x \mapsto m).$$

5) Аналогично, истинность формулы $\forall x A$ («для всех x имеет место A) определяется как

$$[\forall x A]\pi = \mathop{\&}_{m \in M} [A](\pi + x \mapsto m).$$

Когда даны модель и оценка, истинностное значение имеет каждая формула сигнатуры. Здесь ситуация несколько сложнее, чем в алгебре высказываний, где достаточно было задать истинностные значения пропозициональных переменных.

4. Заметим, что по определению истинности истинностные значения формул $\exists x A$, $\forall x A$ *не зависят* от индивидной переменной x, «пробегающей значения» по предметной области. Легко указать аналогию с другими математическими формулами: к примеру, формулы вида

$$\sum_j A_{ij} f_j, \quad \int_D K(x,y) f(y)\, dy$$

обозначают соответственно вектор, индексируемый переменной i, и функцию, зависящую от x, не зависимые j и y соответственно. В приведённых примерах переменные j и y являются *связанными*, а i и x — *свободными*. Одна и та же буква может входить в формулу и в качестве свободной, и в качестве связанной переменной. В формуле

$$\int_0^1 x^2 y\, dx + 3x$$

y свободна, а для x ситуация сложнее: первые два её вхождения связаны, а третье — свободно. Аналогичную ситуацию имеем

в формуле $\exists x Q(x,y) \vee P(x)$, где два первых вхождения x «подпадают под действие» квантора $\exists$, а последнее — «не подпадает».

Упр. 19. [2]. Определите свободные и связанные вхождения переменных в формулах

$$\forall x(P(x,y) \Rightarrow \forall y Q(x,y)),$$
$$\forall x P(x,y) \Rightarrow \forall y R(x,y),$$
$$\neg\exists y Q(y,y) \,\&\, R(y,y).$$

Рассмотрим формулу $\int_0^1 x^2 y\,dx + 3x$. Функция двух переменных x и y, выражаемая этой формулой, не изменится, если все связанные вхождения переменной x заменить, например, буквой t: $\int_0^1 t^2 y\,dt + 3x$. Вместо буквы t могла бы быть использована любая другая буква, кроме y, ибо замена связанных вхождений x на y даст побочный эффект: $\int_0^1 y^2 y\,dy + 3x$ вообще перестаёт быть функцией двух переменных. В последнем случае произошла *коллизия переменных*, причина которой в том, что переменная y входит в качестве свободной в формулу под интегралом.

Аналогичная ситуация имеет место в формулах сигнатуры. Как мы увидим далее, в формулах сигнатуры возможны при определённых условиях переименования связанных переменных, после которых формула будет выражать тот же самый предикат.

Для наглядной иллюстрации свободных и связанных вхождений переменных удобно пользоваться надстрочными линиями, демонстрирующими, какой квантор связывает какие вхождения переменных. К примеру,

$$\forall y(P(y) \,\&\, \exists t Q(t,z)) \Rightarrow \exists x R(x,x) \vee Q(z,x),$$
$$\forall z(P(z) \,\&\, \exists x Q(x,z)) \Rightarrow \exists x R(x,x) \vee Q(z,x),$$
$$\forall x(P(x) \,\&\, \exists x Q(x,z)) \Rightarrow \exists y R(y,y) \vee Q(z,x).$$

Обратим внимание, что в третьей формуле переменная x в $Q(x,z)$ связывается с ближайшим к ней слева квантором $\exists x$,

а не более далёким $\forall x$. Если теперь стереть все связанные переменные и заменить их пустыми «окнами», получим *схему* формулы, содержащую всю существенную информацию о ней:

$$\forall\overline{\square(P(\square)\ \&\ \exists\overline{\square Q(\square,z)})} \Rightarrow \exists\overline{\square R(\square,\square)} \vee Q(z,x),$$

$$\overline{\forall\overline{\square(P(\square)\ \&\ \exists\overline{\square Q(\square,\square)})} \Rightarrow \exists\overline{\square R(\square,\square)}} \vee Q(z,x),$$

$$\forall\overline{\square(P(\square)\ \&\ \exists\overline{\square Q(\square,z)})} \Rightarrow \exists\overline{\square R(\square,\square)} \vee Q(z,x).$$

Конгруэнтными, или *подобными*, называются формулы, схемы которых совпадают. В приведённом примере первая и третья формулы конгруэнтны. Кажется интуитивно очевидным, что конгруэнтные формулы «обозначают одно и то же», и далее (теорема 16 на с. 53) будет строго доказана эквивалентность конгруэнтных формул.

Упр. 20. [3]. Какие из этих формул конгруэнтны?

$$\begin{array}{l}\forall z\exists y(P(z,y)\ \&\ \forall z Q(z,x) \Rightarrow R(z)),\\ \forall x\exists y(P(x,y)\ \&\ \forall y Q(y,x) \Rightarrow R(x)),\\ \forall y\exists z(P(y,z)\ \&\ \forall z Q(z,x) \Rightarrow R(y)),\\ \forall z\exists x(P(z,x)\ \&\ \forall z Q(z,y) \Rightarrow R(z)),\\ \forall y\exists z(P(z,y)\ \&\ \forall z Q(z,x) \Rightarrow R(y)).\end{array}$$

5. Введём классификацию формул сигнатуры σ:

- Формула A называется *тавтологией*, или *общезначимой формулой*, и обозначается $\models A$, если она истинна *на любой* оценке *любой* модели.

- Формула, не являющаяся общезначимой ($\not\models A$), называется *опровержимой*. Формула опровержима тогда и только тогда, когда можно указать хотя бы одну модель и оценку, на которой эта формула ложна.

- Формула называется *невыполнимой*, если она ложна *на любой* оценке *любой* модели. Ясно, что формула невыполнима тогда и только тогда, когда её отрицание является тавтологией, т. е. имеет место $\models \neg A$.

- Формула называется *выполнимой*, если можно указать хотя бы одну модель и оценку, на которой эта формула истинна, т. е. имеет место $\not\models \neg A$.

Соотношение между общезначимыми, выполнимыми, опровержимыми и невыполнимыми формулами показывает следующая диаграмма:

Упр. 21. [2]. Докажите, что выполнимы следующие формулы (дайте модели и оценки, на которых они истинны):

$$\begin{array}{ll} \exists x P(x), & \exists x \exists y (P(x) \,\&\, \neg P(y)), \\ \forall x P(x), & P(x) \Rightarrow \forall y P(y). \end{array}$$

6. Чтобы доказать выполнимость (опровержимость) формулы логики предикатов, достаточно придумать хотя бы одну модель и оценку, в которых формула истинна (ложна). Как определить, что формула логики предикатов является общезначимой (невыполнимой)? Для этого необходим новый метод рассуждения. Здесь мы рассмотрим некоторые классы общезначимых формул, а в § 1.4 построим *исчисление предикатов*, которое будет порождать все общезначимые формулы логики предикатов и только их.

Теорема 11. *Если формула логики высказываний является пропозициональной тавтологией, то подстановка в неё вместо пропозициональных переменных любых формул сигнатуры будет давать общезначимую формулу логики предикатов.*

◁Возьмём некоторую модель и оценку. Тогда каждая из формул сигнатуры, подставленная в пропозициональную тавтологию, примет значение $\mathfrak{t}$ или $\mathfrak{f}$. Однако результирующая формула примет значение $\mathfrak{t}$, т. к. она даёт истину вне зависимости от истинностных значений своих переменных. Это будет иметь место для произвольной модели и оценки; следовательно, результирующая формула является общезначимой в логике предикатов.▷

Например, формула $\exists x P(x) \vee \neg\exists x P(x)$ является общезначимой формулой логики предикатов, т. к. получена из пропозициональной тавтологии $A \vee \neg A$. Однако даваемый теоремой 11 класс общезначимых формул ещё недостаточно широк: например, никакая формула вида $\forall x A$ или $\exists x A$ не может попасть в класс формул, общезначимых в силу теоремы 11.

7. В то же время заметим, что, например, должна быть общезначимой формула $\forall x P(x) \Rightarrow P(y)$, где P — одновалентный предикатный символ: если в выбранной модели $P(x)$ истинен для каждого значения x, то он должен быть истинным и для произвольного значения y, если же $[\forall x P(x)]\pi = \mathfrak{f}$, то вся импликация будет истинной уже в силу того, что её левая часть ложна. Можно ли обобщить это наблюдение для произвольной формулы вместо $P(x)$ и произвольного терма (переменной или константы) вместо y? По традиции Бурбаки [15], результат текстовой замены x на t в формуле A обозначим следующим образом: $(t \mid x)A$. Мы стремимся доказать общезначимость чего-то вроде

$$\forall x A \Rightarrow (t \mid x)A,$$

где A — произвольная формула, x — произвольная переменная, t — произвольный терм.

В общем виде это, однако, не имеет места. Например, если формула A имеет вид $\exists x P(x)\ \&\ Q(x)$, то результатом простой замены всех вхождений переменной x на константу c будет синтаксически некорректная последовательность символов $\exists c P(c) \& Q(c)$ (за квантором всегда должна следовать переменная, квантор по константе недопустим). Таким образом, первое условие на *корректную под-*

становку терма вместо переменной формулируется следующим образом: корректная подстановка $(t \mid x)A$ должна выполнять замену только *свободных* вхождений переменной x.

Но и первого ограничения недостаточно, как показывает следующий пример: замена свободного вхождения x на y в формуле $\exists y P(x, y)$ приведёт к тому, что переменная x подпадёт под действие квантора, в результате чего частный случай схемы $\forall x A \Rightarrow$ $\Rightarrow (t \mid x)A$ — формула $\forall x \exists y P(x, y) \Rightarrow \exists y P(y, y)$ — не будет общезначимым.

Упр. 22. Проверьте, что формула $\forall x \exists y P(x, y) \Rightarrow \exists y P(y, y)$ не общезначима.

Итак, необходимо ввести ещё одно ограничение и говорить, что подстановка терма t вместо свободных вхождений переменной x в формуле A корректна, если после этой подстановки терм t не подпадает под действие квантора. Иными словами, эта подстановка не должна менять схемы формулы A (за исключением имён свободных переменных). В дальнейшем, говоря о подстановке $(t \mid x)A$, мы будем иметь в виду только корректные подстановки.

Упр. 23. Допустим, что подстановка $(y \mid x)A$ корректна. Всегда ли при этом будет корректна обратная подстановка $(x \mid y)(y \mid x)A$? (Ответ: нет, как, например, в случае $\forall z P(z, x) \vee \forall x Q(x, y)$.)

Для дальнейшего нам понадобится лемма, использующая свойства, заложенные в определение корректной подстановки.

Лемма 12. *Для произвольных формулы A, переменной x и терма t, если подстановка $(t \mid x)A$ корректна, имеет место*

$$[(t \mid x)A]\pi = [A](\pi + x \mapsto [t]\pi).$$

$\lhd$Эта лемма утверждает довольно простую вещь: если, например, переменная x является единственным параметром формулы A, а c — константа, то корректная подстановка $(c \mid x)A$ даст формулу без параметров, истинностное значение которой (в соответствии с леммой) должно равняться истинностному значению формулы A на оценке, в которой значение переменной x является элементом предметного множества, соответствующего константе c.

Доказательство проведём индукцией по построению формулы A. Для атомарных формул корректная подстановка есть простая текстовая замена, поэтому $[(t \mid x)P(\ldots,x,\ldots)]\pi = [P(\ldots,t,\ldots)]\pi = P(\ldots,[t]\pi,\ldots) = P(\ldots,[x](\pi + x \mapsto [t]\pi),\ldots) = [P(\ldots,x,\ldots)](\pi + x \mapsto [t]\pi)$.

В случае формулы вида $A\gamma B$ доказательство прямолинейно: $[(t \mid x)(A\gamma B)]\pi = [(t \mid x)A\gamma(t \mid x)B]\pi = [(t \mid x)A]\pi\gamma[(t \mid x)B]\pi = [A](\pi + x \mapsto [t]\pi)\gamma[B](\pi + x \mapsto [t]\pi) = [A\gamma B](\pi + x \mapsto [t]\pi)$.

Случай $\neg A$ аналогичен предыдущему.

Остаётся случай, когда формула начинается с квантора. Пусть, например, формула имеет вид $\exists yA$, x — её параметр (отсюда x не совпадает с y). Тогда в предположении корректной подстановки t не совпадает с y. Тогда $[(t \mid x)\exists yA]\pi = [\exists y(t \mid x)A]\pi = \bigvee\limits_{m\in M} [(t \mid x)A](\pi + y \mapsto m)$.

Отсюда, по предположению индукции, $[(t \mid x)\exists yA]\pi = \bigvee\limits_{m\in M} [A](\pi + y \mapsto m + x \mapsto [t](\pi + y \mapsto m))$.

В силу корректности подстановки t не является y, поэтому значение t не изменится, если оценку $\pi + y \mapsto m$ заменить просто на π. Далее, т. к. x не совпадает с y, два изменения оценки π можно поменять местами, откуда $[(t \mid x)\exists yA]\pi = \bigvee\limits_{m\in M} [A](\pi + x \mapsto [t]\pi + y \mapsto m) = \exists y[A](\pi + x \mapsto [t]\pi)$, что и требовалось доказать. Для случая $\forall yA$ доказательство то же, только дизъюнкцию необходимо заменить на конъюнкцию.$\triangleright$

Теорема 13. *Для произвольных формулы A и терма t, если подстановка $(t \mid x)A$ корректна, справедливо*

$$\models \forall xA \Rightarrow (t \mid x)A,$$

$$\models (t \mid x)A \Rightarrow \exists xA.$$

$\triangleleft$Докажем первое утверждение. Если на некоторой оценке $\forall xA$ ложна, то вся импликация будет истинна. Если в некоторой оценке $\forall xA$ истинна, то по определению истинности формула A будет истинна на всякой оценке, отличающейся π только лишь значением

переменной x. Значит, формула A будет истинна и на оценке $\pi + x \mapsto [t]\pi$, откуда по лемме 12 следует, что $[(t \mid x)A]\pi = \mathfrak{t}$, и вся импликация принимает значение $\mathfrak{t}$.▷

Упр. 24. Докажите второе утверждение теоремы 13.

Упр. 25. Приведите пример случая, когда некорректная подстановка даёт не общезначимую формулу вида $(t \mid x)A \Rightarrow \exists x A$. (Ответ: $\forall y A(y, y) \Rightarrow \exists x \forall y A(x, y)$.)

Используя аналогичные рутинные рассуждения об истинностных значениях формул на оценках, можно доказать общезначимость и в других случаях. Но гораздо экономнее (во многих смыслах) пользоваться исчислением предикатов, чему и будет посвящён следующий параграф.

§ 1.4. Исчисление предикатов

1. В этом параграфе мы, по аналогии с проделанным в § 1.2, построим исчисление, позволяющее выводить все тавтологии языка логики предикатов (и только их) из аксиом при помощи правил вывода. Основным результатом, как и тогда, станет доказательство эквивалентности понятия общезначимости формулы и её выводимости в построенном исчислении.

Прежде, однако, обсудим один принципиальный вопрос.

Доказуемость формулы исчисления высказываний эквивалентна её общезначимости, то же самое (как будет доказано ниже) имеет место для исчисления предикатов. Чтобы проверить, является ли тавтологией формула алгебры высказываний, достаточно подставить в неё все возможные комбинации переменных. Эту работу можно «поручить», например, компьютеру, который за конечное (хотя, может быть, и большое) время гарантированно выдаст ответ. Можно ли нечто подобное придумать для формул логики предикатов? Т. е. возможно ли «раз и навсегда» построить такой алгоритм, подавая на вход которого произвольную формулу произвольной сигнатуры, мы гарантированно получали бы на выходе ответ на вопрос: является ли эта формула выполнимой? (В этом

случае можно было бы определять и общезначимость, для чего достаточно было бы проверить выполнимость A и $\neg A$.)

Ответ на этот вопрос — отрицательный: в общем виде такого алгоритма не существует. Соответствующая теорема была доказана Чёрчем в 1936 г. (см. напр. [3]). Алгоритмы можно предложить лишь для некоторых очень ограниченных классов сигнатур: к примеру, если в сигнатуре содержатся только нуль-местные предикатные символы, то задача сводится к алгебре высказываний (кванторы в этом случае роли играть не будут). Алгоритмически разрешимым является также вопрос и о выполнимости формулы в сигнатуре, состоящей только из одноместных предикатных символов.

Упр. 26. [6]. Пусть сигнатура состоит из n одноместных предикатных символов. Докажите, что если формула такой сигнатуры выполнима, то она также выполнима в некоторой модели с множеством, состоящим из 2^n элементов. Придумайте на основании этого алгоритм установления выполнимости формулы данной сигнатуры.

Не имея возможности в общем случае установить общезначимость формулы алгоритмическим путём, мы тем не менее всегда можем алгоритмически проверить корректность вывода формулы, если таковой предоставлен.

2. Для построения исчисления предикатов естественно взять десять схем аксиом и правило modus ponens исчисления высказываний (см. § 1.2), применив их для нового понятия формулы (§ 1.3, с. 33). Как мы уже знаем (см. теорему 4 и теорему 11), их применение будет давать общезначимые формулы сигнатуры. Добавим, кроме того, следующие схемы и правила вывода, касающиеся кванторов:

- $\forall$-схема: для любой формулы A, переменной x и терма t, если подстановка $(t|x)A$ корректна, $\forall x A \Rightarrow (t|x)A$.

- $\forall$-правило Бернайса: если x не входит в A свободно, то

$$\frac{\vdash A \Rightarrow B}{\vdash A \Rightarrow \forall x B}.$$

- $\exists$-схема: для любой формулы A, переменной x и терма t, если подстановка $(t|x)A$ корректна, $(t|x)A \Rightarrow \exists x A$.

- $\exists$-правило Бернайса: если x не входит в B свободно, то

$$\frac{\vdash A \Rightarrow B}{\vdash \exists x A \Rightarrow B}.$$

В этих схемах и правилах вновь проявляется «родство» квантора $\forall$ с конъюнкцией и квантора $\exists$ с дизъюнкцией. К примеру, $\forall$-схема схожа со схемами $A \,\&\, B \Rightarrow A$, $A \,\&\, B \Rightarrow B$ (они говорят о том, *что* можно получить из конъюнкции и квантора всеобщности), а $\forall$-правило схоже со схемой $(A \Rightarrow B) \Rightarrow ((A \Rightarrow C) \Rightarrow (A \Rightarrow \Rightarrow B \,\&\, C))$ (они говорят о том, *как* можно получить конъюнкцию и квантор). Отметим также, что только лишь $\forall$- и $\exists$-схем нам было бы недостаточно: исчисление, не содержащее правил Бернайса, согласовывалось бы, например, с такой интерпретацией, при которой формула вида $\exists x A$ всегда истинна, а $\forall x A$ всегда ложна.

Упр. 27. [2]. Являются ли выводами в исчислении предикатов следующие последовательности формул:

1) $\forall x \exists y A(x, y) \Rightarrow \exists y A(y, y)$;

2) $\forall x P(x) \Rightarrow P(y)$, $\forall x P(x) \Rightarrow \forall y P(y)$;

3) $A(x) \Rightarrow \exists x A(x)$, $(A(x) \Rightarrow \exists x A(x)) \Rightarrow (\forall x A(x) \Rightarrow (A(x) \Rightarrow \exists x A(x)))$, $\forall x A(x) \Rightarrow (A(x) \Rightarrow \exists x A(x))$?

Ответы: 1) нет: попытка воспользоваться $\forall$-схемой, но некорректная подстановка, 2) да: $\forall$-схема, $\forall$-правило, 3) да: $\exists$-схема, первая схема исчисления высказываний, modus ponens.

Упр. 28. Докажите, что для произвольной формулы A выводимо $\forall x A \Rightarrow \exists x A$.

Теорема 14. *Всякая выводимая в исчислении предикатов формула является общезначимой (если $\vdash A$, то $\models A$).*

$\lhd$Как и при доказательстве теоремы 4, необходимо проверить, что схемы дают общезначимые формулы, а правила вывода сохраняют общезначимость. Схемы, перенесённые из исчисления высказываний, являются пропозициональными тавтологиями; следовательно, в силу теоремы 11 при подстановке в них вместо букв A,

B, C произвольных формул сигнатуры они будут давать общезначимые формулы.

Теорема 13 показывает, что $\forall$- и $\exists$-схемы дают общезначимые формулы.

Доказательство того факта, что правило modus ponens сохраняет общезначимость, полностью аналогично данному в теореме 4, за тем исключением, что фразу *на любом наборе пропозициональных переменных* необходимо заменить на *на любой модели и оценке.*

Остаются правила Бернайса. Пусть $\models A \Rightarrow B$ и x не входит в A свободно. Пусть A истинна на некоторой оценке π. В силу того, что она не зависит от x, она истинна также и на любой оценке π', отличающейся от π значением переменной x. В силу $\models A \Rightarrow B$, в этих случаях B также является истинной, а значит, является истинной $\forall x B$. Значит, истинность A в некоторой оценке π является достаточным условием истинности $\forall x B$ в той же оценке; следовательно, $\models A \Rightarrow \forall x B$, что и требовалось доказать.

Для второго правила Бернайса рассуждение симметричное. Пусть $\models A \Rightarrow B$ и x не входит свободно в B. Пусть $\exists x A$ истинна на некоторой оценке π. Это значит, что существует оценка π', отличающаяся от π только значением переменной x, на которой A истинна. В силу $\models A \Rightarrow B$ на оценке π' также должна быть истинна и B. Но π' отличается от π только значением переменной x, от которой B не зависит; следовательно, B будет истинным и в оценке π. Значит, истинность $\exists x A$ в некоторой оценке π является достаточным условием истинности B в той же оценке; следовательно, $\models \exists x A \Rightarrow B$, что и требовалось доказать.$\triangleright$

Как и в случае с исчислением высказываний, тут же вытекает

Следствие. *Не существует формулы A, такой, что одновременно $\vdash A$ и $\vdash \neg A$ в исчислении предикатов.*

$\triangleleft$Доказательство полностью аналогично доказательству следствия из теоремы 4, нужно лишь рассуждать не в терминах наборов пропозициональных переменных, а в терминах моделей и оценок.$\triangleright$

3. Будем говорить, что формулы A и B *доказуемо эквивалент-*

ны, и писать

$$A \sim B,$$

если одновременно имеет место $\vdash A \Rightarrow B$ и $\vdash B \Rightarrow A$. (Это определение с учётом теоремы о полноте исчисления высказываний согласуется с данным на с. 14 для пропозициональных формул.) Таким образом, установление доказуемой эквивалентности сводится к поиску вывода двух указанных импликаций.

4. Ниже рассматриваются некоторые наиболее употребимые на практике классы выводимых формул логики предикатов. Прежде всего отметим, что запас навыков, набранный при изучении исчисления высказываний, пригодится и при решении задач формального вывода в исчислении предикатов. Если известно, что A — формула, выводимая в исчислении высказываний, то замена в ней пропозициональных переменных на формулы исчисления предикатов будет формулой, выводимой в исчислении предикатов (из аксиом по правилу modus ponens). Кроме того, можно пользоваться теоремой о полноте исчисления высказываний и считать выводимой любую формулу, полученную из пропозициональной тавтологии. Мы пока что не ввели понятие вывода из посылок для исчисления предикатов и не будем пользоваться приёмами вывода из посылок по причине, которая станет ясна ниже. Но это ни в коем случае не «дисквалифицирует» формулы, выведенные в исчислении высказываний с помощью таких приёмов, т. к. для всех них можно эффективно построить и обычный вывод из аксиом по правилу modus ponens.

5. Правило обобщения. Докажем, что для любой формулы A, если она выводима, то выводима также $\forall x A$, т. е. справедливо правило вывода

$$\frac{\vdash A}{\vdash \forall x A}.$$

Возьмём какую-нибудь замкнутую (т. е. не содержащую свободных переменных) выводимую формулу B. Такая формула существует: например, можно воспользоваться формулой $A' \Rightarrow A'$,

где A' получена из A навешиванием любых кванторов по всем свободным переменным. Тогда

1) $\vdash A \Rightarrow (B \Rightarrow A)$ — схема 1,

2) $\vdash B \Rightarrow A$ — modus ponens к шагу 1 и $\vdash A$,

3) $\vdash B \Rightarrow \forall x A$ — $\forall$-правило к шагу 2, которое допустимо применить в силу замкнутости формулы B,

4) $\vdash \forall x A$ — modus ponens к шагу 3 и $\vdash B$, что и требовалось.

6. Законы коммутативности кванторов формулируются следующим образом: если A — произвольная формула, то справедливы следующие соотношения:

1) $\forall x \forall y A \sim \forall y \forall x A$,

2) $\exists x \exists y A \sim \exists y \exists x A$,

3) $\vdash \exists x \forall y A \Rightarrow \forall y \exists x A$.

Заметим, что в последнем случае импликация верна только в одну сторону.

Упр. 29. Покажите, что $\nvdash \forall y \exists x A \Rightarrow \exists x \forall y A$.

Докажем первое утверждение.

$$\vdash \forall x \forall y A \Rightarrow \forall y A \text{ — } \forall\text{-схема},$$

$$\vdash \forall y A \Rightarrow A \text{ — } \forall\text{-схема}.$$

Теперь если бы в нашем распоряжении было правило вывода

$$\frac{\vdash A \Rightarrow B, \vdash B \Rightarrow C}{\vdash A \Rightarrow C}$$

(а мы его сейчас обоснуем), то мы могли бы заключить также

$$\vdash \forall x \forall y A \Rightarrow A.$$

Левая часть этой импликации не зависит от x и от y (эти переменные связаны кванторами), поэтому можно дважды применить $\forall$-правило Бернайса и получить

$$\vdash \forall x \forall y A \Rightarrow \forall y \forall x A,$$

что и требовалось доказать. Доказательство утверждения в обратную сторону будет тем же, только с переставленными именами переменных.

Теперь обоснуем обещанное правило вывода, которым будем пользоваться и в дальнейшем. Пусть $\vdash A \Rightarrow B$ и $\vdash B \Rightarrow C$. Тогда

1) $\vdash (A \Rightarrow B) \Rightarrow ((A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C))$ — схема 2,

2) $\vdash (A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ — modus ponens к $\vdash A \Rightarrow B$ и шагу 1.

3) $\vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))$ — схема 1,

4) $\vdash A \Rightarrow (B \Rightarrow C)$ — modus ponens к $\vdash B \Rightarrow C$ и 3,

5) $\vdash A \Rightarrow C$ — modus ponens к шагам 4 и 2, что и требовалось доказать.

Упр. 30. Докажите второй и третий законы коммутативности кванторов. Указание: доказывая $\exists x \forall y A \Rightarrow \forall y \exists x A$, докажите сперва $\vdash \forall y A \Rightarrow \Rightarrow \exists x A$.

Упр. 31. Обоснуйте правила вывода

$$\frac{\vdash \exists x A, \vdash A \Rightarrow B}{\vdash \exists x B}, \qquad \frac{\vdash \forall x A, \vdash A \Rightarrow B}{\vdash \forall x B}.$$

7. Законы де Мóргана для кванторов: для произвольной формулы A,

1) $\exists x A \sim \neg \forall x \neg A$,

2) $\forall x A \sim \neg \exists x \neg A$.

Действительно: докажем, например, что $\vdash \exists x A \Rightarrow \neg\forall x\neg A$. Т. к. правая часть импликации не содержит x, то достаточно доказать $A \Rightarrow \neg\forall x\neg A$, откуда можно было бы перейти к требуемой формуле по правилу Бернайса. По закону контрапозиции достаточно доказать $\forall x\neg A \Rightarrow \neg A$, но это аксиома. Переписывая наше рассуждение в обратном порядке, получим вывод для $\exists x A \Rightarrow \neg\forall x\neg A$.

Остальные импликации, составляющие содержание законов де Моргана, доказываются аналогично. Докажем, что $\vdash \neg\forall x\neg A \Rightarrow \Rightarrow \exists x A$. Имея в виду закон контрапозиции, достаточно доказать $\neg\exists x A \Rightarrow \forall x\neg A$, имея в виду $\forall$-правило — $\neg\exists x A \Rightarrow \neg A$. Применяя контрапозицию ещё раз, достаточно доказать $A \Rightarrow \exists x A$, но это аксиома. Переписывая формулы в обратном порядке, получим вывод для $\neg\forall x\neg A \Rightarrow \exists x A$.

Упр. 32. Докажите второй закон де Моргана.

При помощи контрапозиции мы можем перейти и к такой форме законов де Моргана: $\neg\exists x A \sim \forall x\neg A$, $\neg\forall x A \sim \exists x\neg A$.

8. Пусть для некоторых формул A, B имеет место $\vdash A \Rightarrow B$. Докажем, что при этом $\vdash \forall x A \Rightarrow \forall x B$ и $\vdash \exists x A \Rightarrow \exists x B$.

В силу $\forall$-схемы, $\vdash \forall x A \Rightarrow A$, откуда $\vdash \forall x A \Rightarrow B$. Т. к. x не входит в $\forall x A$ свободно, то $\vdash \forall x A \Rightarrow \forall x B$. Аналогично, в силу $\exists$-схемы $\vdash B \Rightarrow \exists x B$, $\vdash A \Rightarrow \exists x B$ и по правилу Бернайса $\vdash \exists x A \Rightarrow \exists x B$.

Таким образом, если $A \sim B$, то $\forall x A \sim \forall x B$ и $\exists x A \sim \exists x B$. Отсюда легко доказывается следующая важная лемма.

Лемма 15 (о замене подформулы)**.** *Замена подформулы на доказуемо эквивалентную даёт формулу, доказуемо эквивалентную исходной.*

$\lhd$Проведём доказательство индукцией по построению, начиная с заменённой подформулы и рассматривая всё более длинные части формулы. Заменённая подформула эквивалентна исходной подформуле по условию. Теперь

- если $A \sim A'$, то $\neg A \sim \neg A'$, т. к. имеют место тавтологии $(A \Rightarrow A') \Rightarrow (\neg A' \Rightarrow \neg A)$ и $(A' \Rightarrow A) \Rightarrow (\neg A \Rightarrow \neg A')$,

- если $A \sim A'$ и $B \sim B'$, то $A \,\&\, B \sim A' \,\&\, B'$, т. к. имеют место тавтологии $(A \Rightarrow A') \Rightarrow ((B \Rightarrow B') \Rightarrow ((A \,\&\, B) \Rightarrow (A' \,\&\, B')))$, $(A' \Rightarrow A) \Rightarrow ((B' \Rightarrow B) \Rightarrow ((A' \,\&\, B') \Rightarrow (A \,\&\, B)))$,
- аналогично для других пропозициональных связок,
- если $A \sim B$, то, по доказанному выше, $\forall x A \sim \forall x B$ и $\exists x A \sim \sim \exists x B$.$\triangleright$

9. Законы **пронесения квантора всеобщности через конъюнкцию** и **пронесения квантора существования через дизъюнкцию** формулируются следующим образом: для любых формул A, B

1) $\forall x A \,\&\, \forall x B \sim \forall x (A \,\&\, B)$,
2) $\exists x A \vee \exists x B \sim \exists x (A \vee B)$.

В самом деле: $\vdash \forall x A \& \forall x B \Rightarrow \forall x A$, $\vdash \forall x A \Rightarrow A$, откуда $\vdash \forall x A \& \& \forall x B \Rightarrow A$ и аналогично $\vdash \forall x A \,\&\, \forall x B \Rightarrow B$. Воспользовавшись схемой аксиом $(A \Rightarrow B) \Rightarrow ((A \Rightarrow C) \Rightarrow (A \Rightarrow B \,\&\, C))$ и правилом modus ponens, имеем

$$\vdash \forall x A \,\&\, \forall x B \Rightarrow A \,\&\, B.$$

Но переменная x не входит свободно в левую часть доказанной конъюнкции, поэтому можно воспользоваться правилом Бернайса и заключить

$$\vdash \forall x A \,\&\, \forall x B \Rightarrow \forall x (A \,\&\, B),$$

что и требовалось. В обратную сторону: от $\forall x (A \,\&\, B)$ доказываем импликацию к $A \,\&\, B$, затем по отдельности к A и B, затем по правилу обобщения — к $\forall x A$ и $\forall x B$ и объединяем в конъюнкцию с помощью аксиомы $(\forall x (A \,\&\, B) \Rightarrow \forall x A) \Rightarrow ((\forall x (A \,\&\, B) \Rightarrow \forall x B) \Rightarrow \Rightarrow (\forall x (A \,\&\, B) \Rightarrow \forall x A \,\&\, \forall x B))$.

Упр. 33. Докажите по аналогии закон пронесения квантора существования через дизъюнкцию.

Заметим, что *нельзя* аналогичным образом выносить квантор в начало формул вида $\forall x A \vee \forall x B$ и $\exists x A \,\&\, \exists x B$. Обдумайте это[3].

Упр. 34. Докажите, что $\vdash \forall x A \,\&\, \exists x B \Rightarrow \exists x (A \,\&\, B)$.

Рассмотренные нами законы де Моргана, коммутативности и пронесения кванторов не предполагали каких-либо ограничений на вид подчиняющимся им формул. Выведем теперь ряд законов, предполагающих определённые ограничения на свободные вхождения переменных в формулы.

10. Корректное переименование связанных переменных. Пусть A — формула. Рассмотрим две последовательности формул:

1) $\forall x A \Rightarrow (y \mid x)A$, $\forall x A \Rightarrow \forall y (y \mid x)A$.

2) $(y \mid x)A \Rightarrow \exists x A$, $\exists y (y \mid x)A \Rightarrow \exists x A$.

Чтобы эти последовательности были корректными выводами, требуется, во-первых, чтобы подстановка $(y \mid x)A$ была корректной (и тогда первый шаг станет аксиомой), а во-вторых — чтобы переменная y не содержалась свободно в A (и тогда второй шаг будет получаем из первого по правилу Бернайса).

Если оба условия выполняются, то мы можем утверждать, что $\vdash \forall x A \Rightarrow \forall y (y \mid x)A$ и $\vdash \exists y (y \mid x)A \Rightarrow \exists x A$. Но тогда импликации будут верны и в обратную сторону! В самом деле: т. к. подстановка $(y \mid x)A$ заменяет все свободные вхождения x на y, то формула $(y \mid x)A$ не содержит x свободно. Может ли быть некорректной обратная подстановка $(x \mid y)(y \mid x)A$, т. е. возможно ли, чтобы переменная x, подставленная вместо какого-либо из свободных вхождений y в формулу $(y \mid x)A$, подпала под действие одноимённого квантора? Т. к. переменная y не входила свободно в формулу A, то все свободные вхождения y в формулу $(y \mid x)A$ есть результат

[3] В книге [6] при обсуждении законов пронесения кванторов авторы приводят такой пример: «В одном из выступлений начала перестройки М. С. Горбачёв сказал, что нужны „преданные делу социализма, но квалифицированные специалисты“... Так вот, их существование не следует из отдельного существования тех и других.»

текстовой замены *свободных*, т. е. не связанных кванторами, вхождений буквы x в формулу A. Обратная подстановка вновь заменит все эти свободные вхождения y в формуле $(y \mid x)A$ на x, и в силу только что сказанного все эти x будут свободными. Таким образом, обратная подстановка $(x \mid y)(y \mid x)A$ корректна и в результате её мы получим исходную формулу A.

Условия «подстановка $(y \mid x)A$ корректна и y не входит в A свободно» мы будем называть *условиями на корректное переименование связанной переменной*. Из изложенного следует, что если эти условия выполняются, то

1) $\forall x A \sim \forall y (y \mid x)A$,

2) $\exists x A \sim \exists y (y \mid x)A$.

Только что доказанное и лемма 15 о замене подформулы дают нам возможность строго обосновать эквивалентность конгруэнтных формул.

Теорема 16. *Конгруэнтные формулы доказуемо эквивалентны.*

◁Заметим, что переименование связанных переменных, сохраняющее схему формулы, является корректным. В самом деле, пусть формула имеет, например, вид

$$\forall x \underbrace{\ldots z \ldots \forall y \ldots y \ldots x}_{A}.$$

Нарушение условия на корректность подстановки привело бы к появлению новых связей в формуле $(y \mid x)A$:

$$\forall y \underbrace{\ldots z \ldots \forall y \ldots y \ldots y}_{(y|x)A},$$

а нарушение условия на отсутствие свободных вхождений — к связыванию прежде свободных переменных:

$$\underbrace{\forall z \ldots z \ldots \forall y \ldots y \ldots z}_{(z|x)A}.$$

Используя ранее не использованные ни в A, ни в B переменные для замены связанных, мы можем две конгруэнтные формулы A и B привести к третьей формуле C, которая будет конгруэнтна и доказуемо эквивалентна формулам A и B. Т. к. обе формулы A и B эквивалентны C, то они эквивалентны и друг другу.▷

11. Навешивание фиктивных кванторов. Если x не входит свободно в формулу B, то

$$B \sim \forall x B \sim \exists x B.$$

Доказательство простое. Если x не входит в B свободно, то $B \Rightarrow \Rightarrow \forall x B$ и $\exists x B \Rightarrow B$ — аксиомы, а $\forall x B \Rightarrow B$ и $B \Rightarrow \exists x B$ получаются из выводимой формулы $B \Rightarrow B$ (вспомним лемму 3!) по $\forall$- и $\exists$-правилам Бернайса.

12. Законы пронесения кванторов в общем виде: для любой формулы A и формулы B, такой, что x не содержится в B свободно, справедливы следующие восемь утверждений об эквивалентности:

1) $\forall x A \,\&\, B \sim \forall x (A \,\&\, B)$,
2) $B \,\&\, \forall x A \sim \forall x (A \,\&\, B)$,
3) $\exists x A \vee B \sim \exists x (A \vee B)$,
4) $B \vee \exists x A \sim \exists x (A \vee B)$,
5) $\exists x A \,\&\, B \sim \exists x (A \,\&\, B)$,
6) $B \,\&\, \exists x A \sim \exists x (A \,\&\, B)$,
7) $\forall x A \vee B \sim \forall x (A \vee B)$,
8) $B \vee \forall x A \sim \forall x (A \vee B)$.

Первые четыре утверждения являются несложным обобщением законов пронесения квантора всеобщности через конъюнкцию и квантора существования через дизъюнкцию. В самом деле, раз x

не содержится в B свободно, мы можем навесить на B фиктивный квантор, воспользоваться леммой 15 о замене подформулы и соответствующими законами пронесения кванторов: например,

$$\forall x A \,\&\, B \sim \forall x A \,\&\, \forall x B \sim \forall x (A \,\&\, B),$$

и аналогично в других случаях.

Утверждения с пятого по восьмое доказать уже не так просто — без использования сведения к противоречию не обойтись.

Докажем пятое и шестое утверждения в одну сторону. Для краткости обозначим буквой F формулу

$$(\exists x A \,\&\, B) \,\&\, \neg(\exists x (A \,\&\, B)),$$

доказуемо эквивалентную формуле $\neg(\exists x A \,\&\, B \Rightarrow \exists x (A \,\&\, B))$.

Выведем из F противоречие, т. е. докажем сначала $\vdash F \Rightarrow \exists x A$, а затем $\vdash F \Rightarrow \neg\exists x A$, откуда будет следовать $\vdash \neg F$ и $\vdash \exists x A \,\&\, B \Rightarrow$ $\Rightarrow \exists x (A \,\&\, B)$, что нам и требуется.

Формула $\vdash F \Rightarrow \exists x A$ выводится элементарно — двойным применением схемы $A \,\&\, B \Rightarrow A$. Выведем теперь $\vdash F \Rightarrow \neg\exists x A$.

Действительно, из F можно последовательно вывести импликации к формулам $\neg\exists x (A \,\&\, B)$, $\forall x \neg (A \,\&\, B)$ — закон де Моргана, $\neg(A \& B)$ —$\forall$-схема, наконец, в силу того что $\neg(A \& B) \Rightarrow (B \Rightarrow \neg A)$, имеем

$$\vdash F \Rightarrow (B \Rightarrow \neg A).$$

С другой стороны, $\vdash F \Rightarrow B$, по второй схеме $\vdash (F \Rightarrow B) \Rightarrow$ $\Rightarrow ((F \Rightarrow (B \Rightarrow \neg A)) \Rightarrow (F \Rightarrow \neg A))$ и, применяя дважды modus ponens, имеем

$$\vdash F \Rightarrow \neg A.$$

Но F не содержит свободно x (вот где мы задействовали тот факт, что x не содержится в B свободно), поэтому можно применить правило Бернайса и заключить $F \Rightarrow \forall x \neg A$, $\vdash F \Rightarrow \neg\exists x A$, но это противоречие с $\vdash F \Rightarrow \exists x A$. Доказательство не изменится, если поменять местами B и $\exists x A$. Тем самым пятое и шестое утверждения в одну сторону доказаны.

Докажем пятое и шестое утверждения в обратную сторону. Теперь обозначим через F формулу

$$(\exists x(A \,\&\, B)) \,\&\, \neg(\exists x A \,\&\, B),$$

доказуемо эквивалентную $\neg(\exists x(A \,\&\, B) \Rightarrow \exists x A \,\&\, B)$. Выведем противоречие: $\vdash F \Rightarrow \exists x(A \,\&\, B)$ и $\vdash F \Rightarrow \neg\exists x(A \,\&\, B)$, откуда будет $\vdash \neg F$ и $\vdash \exists x(A \,\&\, B) \Rightarrow \exists x A \,\&\, B$, что нам и требуется.

Для произвольных формул A и B имеет место

$$\vdash \neg B \Rightarrow \neg(A \,\&\, B),$$

а от формулы $\forall x \neg A$ можно последовательно вывести импликации к: $\neg A$ — $\forall$-схема, $\neg A \vee \neg B$ — схема для дизъюнкции, $\neg(A \,\&\, B)$ — закон де Моргана для высказываний. Итак, для произвольных A и B имеет место

$$\vdash \forall x \neg A \Rightarrow \neg(A \,\&\, B).$$

Воспользовавшись соответствующей схемой, имеем

$$\vdash (\neg B \Rightarrow \neg(A \,\&\, B)) \Rightarrow ((\forall x \neg A \Rightarrow \neg(A \,\&\, B)) \Rightarrow \\ \Rightarrow (\forall x \neg A \vee \neg B \Rightarrow \neg(A \,\&\, B))),$$

и, применив дважды modus ponens с учётом уже выведенных формул, получим

$$\forall x \neg A \vee \neg B \Rightarrow \neg(A \,\&\, B).$$

Т. к. x не входит свободно в левую часть (опять играет роль соглашение, принятое относительно формулы B!), можно воспользоваться правилом Бернайса и вывести последовательно $\vdash \forall x \neg A \vee \vee \neg B \Rightarrow \forall x \neg(A \,\&\, B)$, $\vdash \forall x \neg A \vee \neg B \Rightarrow \neg\exists x(A \,\&\, B)$.

Но от формулы F можно последовательно вывести импликацию к $\neg(\exists x A \,\&\, B)$ и $\forall x \neg A \vee \neg B$, откуда окончательно

$$\vdash F \Rightarrow \neg\exists x(A \,\&\, B),$$

и мы пришли к искомому противоречию.

Используя законы де Моргана и эквивалентности 5 и 6, не составляет труда доказать оставшиеся две эквивалентности 7 и 8. Например, $\neg(\forall xA \vee B) \sim \exists x\neg A \,\&\, \neg B \sim \exists x(\neg A \,\&\, \neg B) \sim \exists x\neg(A \vee \vee B) \sim \neg\forall x(A \vee B)$, откуда $\forall xA \vee B \sim \forall x(A \vee B)$.

Теперь, если предположить, что y не входит свободно в формулы $\forall xA$, $\exists xA$, а x не входит свободно в формулы $\forall yB$, $\exists yB$ (чего всегда можно добиться соответствующим корректным переименованием связанных переменных), то будут справедливы, например, следующие эквивалентности: $\forall xA \vee \forall yB \sim \forall x\forall y(A \vee B)$, $\exists xA \,\&\, \& \,\exists yB \sim \exists x\exists y(A \,\&\, B)$, $\forall xA \vee \exists yB \sim \forall x\exists y(A \vee B) \sim \exists y\forall x(A \vee B)$ и т. д. Заметим, что в последнем случае порядок следования кванторов ($\forall\exists$ или $\exists\forall$) не имеет значения, тогда как в общем случае он, как мы знаем, важен.

13. Будем говорить, что формула находится в *предварённой, или пренексной, нормальной форме*, если она имеет вид

$$\mathsf{Q}_1, \ldots \mathsf{Q}_n F,$$

где каждый Q_i — квантор $\forall$ или $\exists$, а формула F не содержит кванторов. Выведенные в этом параграфе законы позволяют доказать следующее утверждение:

Теорема 17. *Для любой формулы логики предикатов имеется эквивалентная ей формула в предварённой нормальной форме (ПНФ).*

$\lhd$Как обычно, воспользуемся индукцией по построению.

- Атомарные формулы находятся в ПНФ в соответствии с определением.
- Пусть формула имеет вид $\forall xA$, и в соответствии с предположением индукции имеется $A' \sim A$, где A' — формула в предварённой нормальной форме. Тогда $\forall xA'$ также находится в ПНФ, и в силу леммы 15 о замене подформулы $\forall xA' \sim \forall xA$.
- То же самое для случая $\exists xA$.

- Пусть формула имеет вид $\neg A$, и A' — ПНФ для A. Последовательно применяя законы де Моргана $\neg\forall x A \sim \exists x \neg A$ и $\neg\exists x A \sim \sim \forall x \neg A$, мы можем «продвинуть» знак отрицания вплоть до бескванторной части формулы A', по ходу меняя кванторы на сопряжённые, получив в итоге ПНФ для формулы $\neg A$.

- Пусть формула имеет вид $A \,\&\, B$, и имеются A', B' — ПНФ для формул A, B соответственно. Последовательно применяя законы пронесения, мы можем один за другим перенести все кванторы в начало формулы. При этом на каждом шаге, возможно, потребуется переименование связанных переменных, чтобы создать условия применимости законов пронесения кванторов.

  Если на каком-то этапе оба аргумента конъюнкции начинаются с квантора всеобщности, то переименованием связанных переменных приводим конъюнкцию к виду $\forall x A' \,\&\, \forall x B'$, что эквивалентно $\forall x(A' \,\&\, B')$. Во всех остальных случаях переименовываем связанную переменную одной из формул так, чтобы она не входила свободно в другую формулу, и пользуемся соответствующим законом пронесения в общем виде. На каждом шаге количество не перенесённых кванторов уменьшается на один или два, поэтому за конечное число шагов процесс завершится.

- Аналогично для случая $A \vee B$.

- Если формула имеет вид $A \Rightarrow B$, то заменяем её на эквивалентную $\neg A \vee B$, чем сводим задачу к уже рассмотренным случаям.$\triangleright$

Упр. 35. [2, 6]. Привести к предварённой нормальной форме следующие формулы:

$$\neg\exists x\forall y\exists z P(x,y,z), \qquad \exists x\forall y P(x,y) \,\&\, \exists x\forall y Q(x,y),$$
$$\exists x\forall y P(x,y) \vee \exists x\forall y Q(x,y), \qquad \exists x\forall y P(x,y) \Rightarrow \exists x\forall y Q(x,y),$$
$$\forall x P(x) \Rightarrow \forall x Q(x), \qquad \exists x\forall y P(x,y) \Rightarrow \forall y\exists x P(x,y).$$

Частичное решение:

1) $\neg\exists x\forall y\exists z P(x,y,z) \sim \forall x\exists y\forall z\neg P(x,y,z)$.

2) $\exists x\forall y P(x,y)\ \&\ \exists x\forall y Q(x,y) \sim \exists x\forall y P(x,y)\ \&\ \exists u\forall y Q(u,y) \sim$
$\sim \exists x\exists u(\forall y P(x,y)\ \&\ \forall y Q(u,y)) \sim \exists x\exists u\forall y(P(x,y)\ \&\ Q(u,y))$.

3) $\forall x P(x) \Rightarrow \forall x Q(x) \sim \neg\forall x P(x) \vee \forall y Q(y) \sim \exists x\neg P(x) \vee \forall y Q(y) \sim$
$\sim \exists x\forall y(P(x) \Rightarrow Q(y)) \sim \forall y\exists x(P(x) \Rightarrow Q(y))$.

4) $\exists x\forall y P(x,y) \Rightarrow \forall y\exists x P(x,y) \sim \forall x\exists z\neg P(x,z) \vee \forall y\exists z P(z,y) \sim$
$\sim \forall x\forall y(\exists z\neg P(x,z) \vee \exists z P(z,y)) \sim \forall x\forall y\exists z(P(x,z) \Rightarrow P(z,y))$.

§ 1.5. Полнота исчисления предикатов

1. Теперь, как и в случае исчисления высказываний, мы получим доказательство обратного утверждения — выводимости любой общезначимой формулы логики предикатов. Для этого потребуется ряд подготовительных шагов, аналогичных тем, что мы проделали для исчисления высказываний.

Прежде всего обобщим понятие выводимости из посылок на исчисление предикатов. Пусть формулы $A_1, \dots A_n$ *замкнуты*, т. е. не имеют свободных переменных. Будем говорить, что формула E *выводима из посылок* $A_1, \dots A_n$ и писать $A_1, \dots A_n \vdash E$, если можно предоставить последовательность формул $B_1, \dots B_n$, в которой каждая формула либо является одной из посылок $A_1, \dots A_n$, либо аксиомой, либо следует из двух предшествующих формул по modus ponens, либо следует из одной из предшествующих по $\forall$-правилу или $\exists$-правилу и где B_n совпадает с E. Условие замкнутости формул $A_1, \dots A_n$ является существенным: без него невозможно распространить теорему о дедукции на исчисление предикатов. Действительно: по правилу обобщения (с. 47) из произвольной формулы A выводится формула $\forall x A$, но формула $A \Rightarrow \forall x A$, если не требовать замкнутости A, необщезначима и потому невыводима. Если же потребовать замкнутость A, то проблем нет: можно применить правило Бернайса к $A \Rightarrow A$.

Теорема 18 (о дедукции в исчислении предикатов). *Для любого набора замкнутых формул* Γ, *замкнутой формулы* A *и формулы* B *имеет место* $\Gamma, A \vdash B$ *тогда и только тогда, когда* $\Gamma \vdash A \Rightarrow B$.

$\lhd$Как и прежде, в одну сторону утверждение является, по сути, переформулировкой правила modus ponens. Пусть существует вывод формулы $A \Rightarrow B$ из посылок Γ. Тогда, если добавить A к числу посылок, B будет выводима из $A \Rightarrow B$ и A по modus ponens.

Обратное утверждение доказывается по той же схеме, что и в теореме 5 о дедукции в исчислении высказываний. Пусть $B_1, \dots B_n$ — вывод формулы B из набора посылок Γ и посылки A. Добавим к каждой формуле вывода импликацию из A, так что у нас получится список $A \Rightarrow B_1, \dots A \Rightarrow B_n$, после чего дополним этот список до доказательства.

Для каждой из формул $B_1, \dots B_n$ имеет место один из шести случаев:

1) B_i есть A.

2) B_i принадлежит Γ.

3) B_i является аксиомой.

4) B_i получается по modus ponens из B_j и $B_j \Rightarrow B_i$, $j < i$.

   Случаи 1–4 доказываются так же, как и в теореме 5.

5) B_i выводится по $\forall$-правилу Бернайса, т. е. $\Gamma, A \vdash E \Rightarrow F$, переменная x не входит свободно в E, и B_i есть формула $E \Rightarrow \forall x F$.

   По предположению индукции $\Gamma \vdash A \Rightarrow (E \Rightarrow F)$, а нам требуется доказать, что $\Gamma \vdash A \Rightarrow (E \Rightarrow \forall x F)$. Для этого воспользуемся тем фактом, что (проверьте!)

   $$A \Rightarrow (E \Rightarrow F) \sim A \,\&\, E \Rightarrow F.$$

   Из этой эквивалентности вытекает, что $\Gamma \vdash A \,\&\, E \Rightarrow F$, где x не входит свободно в E, а формула A — замкнута. Следовательно, x не входит свободно в $A \,\&\, E$, и мы можем воспользоваться $\forall$-правилом Бернайса: $\Gamma \vdash A \,\&\, E \Rightarrow \forall x F$.

   Воспользовавшись той же эквивалентностью в обратную сторону, получаем $\Gamma \vdash A \Rightarrow (E \Rightarrow \forall x F)$, что и требовалось.

6) B_i выводится по $\exists$-правилу Бернайса, т. е. $\Gamma, A \vdash E \Rightarrow F$, переменная x не входит свободно в F, и B_i есть формула $\exists x E \Rightarrow F$.

Теперь нам, имея предположение индукции $\Gamma \vdash A \Rightarrow (E \Rightarrow F)$, требуется доказать, что $\Gamma \vdash A \Rightarrow (\exists x E \Rightarrow F)$. Воспользуемся следующей эквивалентностью (проверьте её):

$$A \Rightarrow (E \Rightarrow F) \sim E \Rightarrow (A \Rightarrow F).$$

Из этой эквивалентности вытекает, что $\Gamma \vdash E \Rightarrow (A \Rightarrow F)$, где x не входит свободно в F, а формула A — замкнута. Следовательно, x не входит свободно в $A \Rightarrow F$, и мы можем воспользоваться $\exists$-правилом Бернайса: $\Gamma \vdash \exists x E \Rightarrow (A \Rightarrow F)$.

Воспользовавшись той же эквивалентностью в обратную сторону, получаем $\Gamma \vdash A \Rightarrow (\exists x E \Rightarrow F)$, что и требовалось.

Мы доказали, что $\Gamma \vdash A \Rightarrow B_i$ для всех $i = 1, \ldots n$, а значит, и $\Gamma \vdash A \Rightarrow B$.$\triangleright$

Теорема 19. *Для любой формулы C, замкнутых формул A, B и множества замкнутых формул Γ справедливы правила введения и удаления, сформулированные в теореме 6 (табл. на с. 25).*

$\triangleleft$Почти все доказательства, данные для теоремы 6, справедливы и в исчислении предикатов, т. к. основаны на теореме о дедукции и не допускают появления формул со свободными переменными слева от знака $\vdash$. Единственное исключение составляет $\neg$-удаление: в процессе его обоснования формула C оказывается в числе посылок. Но это несущественно: мы можем сначала вывести вместо формулы C её замыкание кванторами всеобщности, а потом воспользоваться аксиомой $\forall x C \Rightarrow C$ и modus ponens.$\triangleright$

2. Назовём *моделью множества* Γ замкнутых формул такую модель $\mathfrak{M}$, на которой все формулы из Γ одновременно истинны. Множество Γ может и не иметь модели (например, если Γ состоит из формул $P(x)$ и $\neg P(x)$), тогда оно называется несовместным. Если у Γ есть модель, то Γ называется совместным множеством.

Теорема 20. *Если* $\Gamma \vdash A$ *и все формулы из* Γ *одновременно истинны в некоторой модели* $\mathfrak{M}$*, то формула* A *также истинна в модели* $\mathfrak{M}$*.*

$\lhd$Пусть Γ состоит из формул $A_1, \dots A_n$. Тогда по теореме о дедукции

$$\vdash A_1 \Rightarrow (A_2 \Rightarrow \dots (A_n \Rightarrow A) \dots).$$

В силу того, что $A \Rightarrow (B \Rightarrow C) \sim A \,\&\, B \Rightarrow C$,

$$\vdash A_1 \,\&\, A_2 \,\&\, \dots \,\&\, A_n \Rightarrow A.$$

В модели $\mathfrak{M}$ все A_i истинны, а в силу теоремы 14 вся формула также должна быть истинной в $\mathfrak{M}$. Но это возможно только тогда, когда A также истинна в $\mathfrak{M}$, что и требовалось доказать.$\rhd$

Набор Γ замкнутых формул сигнатуры может рассматриваться как набор *аксиом* — изначальных утверждений, из которых, следуя логическим правилам, выводятся производные утверждения, или *теоремы*. Именно поэтому Γ также называют *теорией*. Теория называется *противоречивой*, если существует такая формула C, что одновременно $\Gamma \vdash C$ и $\Gamma \vdash \neg C$. Если C — замкнута, то, как известно, в этом случае по правилу $\neg$-удаления выводится вообще всё, что угодно, любая формула. Но и если C — не замкнута, ситуация не меняется. По правилу обобщения, $\Gamma \vdash C'$ и $\Gamma \vdash (\neg C)'$, где штрих означает замыкание формулы кванторами всеобщности по всем свободным переменным. Воспользовавшись тем, что $\vdash \forall x C \Rightarrow \exists x C$, а также тем, что $\vdash \forall x \neg C \Rightarrow \neg \exists x C$, имеем, что $\Gamma \vdash C''$ и $\Gamma \vdash \neg C''$, где C'' означает замыкание формулы C кванторами существования по всем свободным переменным. Для C'' справедливо $\neg$-удаление и из Γ возможно вывести любую формулу.

Таким образом, все противоречивые теории сигнатуры, сколь бы внешне отличными друг от друга не были их аксиомы, эквивалентны между собой: они имеют одно и то же множество теорем, состоящее из вообще всех формул сигнатуры. Поэтому вывод новых теорем в теории имеет смысл лишь тогда, когда мы точно знаем (или имеем достаточные основания полагать), что теория непротиворечива.

Исходя из того, что в противоречивой теории доказуема любая формула, можно получить такой, например, критерий непротиворечивости: *теория* Γ *непротиворечива, если и только если существует хотя бы одна формула, не выводимая из* Γ. На практике, однако, этот критерий слабо применим, и сейчас будет сформулировано другое условие, которое затем обратится в критерий.

Теорема 21. *Любая теория, имеющая модель, непротиворечива.*

$\lhd$Пусть Γ — множество замкнутых формул, имеющее модель $\mathfrak{M}$. Выберем любую замкнутую формулу C. Если бы Γ было противоречивым, то имело бы место $\Gamma \vdash C$ и $\Gamma \vdash \neg C$. Но по теореме 20, все формулы, выводимые из Γ, должны быть истинны в модели $\mathfrak{M}$ — следовательно, C должна быть одновременно истинной и ложной, чего быть не может.$\rhd$

Можно ли превратить последнее условие в критерий, т. е. можно ли утверждать, что любое непротиворечивое множество имеет модель? Да, можно. И после доказательства этого факта уже всего один маленький шаг будет отделять нас от доказательства того, что любая общезначимая формула выводима в исчислении предикатов. Нам понадобится ещё понятие *полного* множества замкнутых формул и две леммы.

Будем говорить, что множество формул Γ *полное*, если для любой замкнутой формулы A сигнатуры имеет место либо $\Gamma \vdash A$, либо $\Gamma \vdash \neg A$. Ясно, что всякое противоречивое множество полно, но интерес представляют только полные непротиворечивые множества замкнутых формул.

Лемма 22 (Линденбаума)**.** *Любое непротиворечивое множество формул целиком содержится в некотором непротиворечивом полном множестве формул.*

$\lhd$Пусть Γ — непротиворечивое множество замкнутых формул. Заметим, что для любой замкнутой формулы A либо Γ, A, либо $\Gamma, \neg A$ — непротиворечивое множество. Предположим обратное, тогда существуют такие формулы C и D, что $\Gamma, A \vdash C$ и $\Gamma, A \vdash \neg C$;

$\Gamma, \neg A \vdash D$ и $\Gamma, \neg A \vdash \neg D$. Тогда из первой пары утверждений по $\neg$-введению следует $\Gamma \vdash \neg A$, а из второй пары — $\Gamma \vdash \neg\neg A$. Но Γ по условию — непротиворечивое множество формул.

Занумеруем всё множество формул сигнатуры так, что A_i будет обозначать i-ю по порядку формулу. Сделать это можно, например, так: любая формула A есть конечная строка в алфавите из конечного числа p символов, и потому может быть проинтерпретирована как натуральное число n, записанное в p-ичной системе счисления. Тогда номер i формулы A есть количество формул сигнатуры среди строк, соответствующих числам в p-ичной системе счисления, меньшим или равным n.

Обозначим также Γ через Γ_1 и будем на каждом i-м шаге добавлять к Γ_i формулу B_i, равную A_i или $\neg A_i$, таким образом, чтобы Γ_{i+1}, полученное добавлением формулы B_i ко множеству Γ_i, было непротиворечивым. Докажем, что результат добавления всех формул B_i к Γ (обозначим его как Γ') будет искомым полным непротиворечивым множеством.

Множество формул Γ' бесконечно, и из того факта, что любые первые n его формул образуют непротиворечивое множество, напрямую ещё не следует, что *всё* Γ' непротиворечиво. Тем не менее если бы удалось найти выводы вида $\Gamma' \vdash C$ и $\Gamma' \vdash \neg C$, то эти выводы по определению могли бы содержать лишь конечное число формул и, как следствие, лишь конечное число формул из Γ'. Пусть максимальный номер формулы, участвующей в выводах формул C и $\neg C$, равен n. Тогда вывод противоречия был бы возможен из первых n формул Γ', но это противоречит построению Γ'. Доказательство леммы завершено.$\triangleright$

Важно заметить, что только что приведённое доказательство леммы Линденбаума имеет принципиальное отличие от доказательств, рассматривавшихся нами до сих пор. Прежде, обосновывая существование какого-нибудь объекта, мы давали «рецепт», буквально следуя которому этот объект можно было бы построить в любом конкретном случае. К примеру, доказательство теоремы о дедукции содержит в себе алгоритм построения вывода $\Gamma \vdash A \Rightarrow$

$\Rightarrow B$ из предъявленного вывода $\Gamma, A \vdash B$, а доказательство теоремы 10 о полноте исчисления высказываний даёт способ построения (пусть не самого изящного) вывода любой общезначимой пропозициональной формулы. Доказательство же леммы Линденбаума бесполезно для практического построения полного непротиворечивого надмножества над данным непротиворечивым множеством формул. Почему? На каждом шаге требуется принимать решение, какую из формул A_i, $\neg A_i$ добавлять к множеству, и, хотя известно, что одну из них, действительно, можно добавить, сохранив непротиворечивость (иначе Γ было бы противоречивым), мы не имеем никакого представления о том, *какую именно* из формул надо добавлять. Поэтому ниже мы докажем существование вывода любой общезначимой формулы логики предикатов, не зная, как этот вывод построить. (Заметим ещё, что бесконечность множества тут роли не играет: в конечном итоге нас интересует не само Γ', а возможность определения принадлежности той или иной формулы к Γ'. Этот вопрос мог бы быть решён для любой формулы за конечное количество описанных в доказательстве шагов.)

Заметим ещё, что множество Γ', получаемое при доказательстве леммы Линденбаума, содержит все те и только те формулы, которые из него можно вывести.

Лемма 23. *Если множество* Γ *содержит замкнутую формулу* $\exists x A$ *и непротиворечиво, а константа* c *не входит ни в одну из формул множества* Γ*, то добавление формулы* $(c \mid x)A$ *к* Γ *оставляет это множество непротиворечивым.*

$\lhd$Прежде всего заметим, что формула $(c \mid x)A$ замкнута: в силу замкнутости $\exists x A$ единственным параметром формулы A может быть переменная x, но она заменяется на константу c. Поэтому добавлять $(c \mid x)A$ к посылкам допустимо.

Теперь проведём доказательство от противного. Если добавление формулы $(c \mid x)A$ к Γ делает множество противоречивым, то это означает ($\neg$-введение), что из Γ выводится $\neg(c \mid x)A$. Возьмём вывод формулы $\neg(c \mid x)A$ из Γ и текстуально заменим в нём

все вхождения константы c на новую переменную y, такую, что y не встречается ни в одной формуле из Γ (в т. ч. в A). При этом вывод останется выводом: аксиомы и правила вывода не различают констант и переменных, а формулы Γ не изменятся и останутся замкнутыми (тут мы впервые использовали тот факт, что c не входит в формулы из Γ).

Таким образом, имеет место $\Gamma \vdash \neg(y \mid x)A$, откуда по правилу обобщения $\Gamma \vdash \forall y \neg(y \mid x)A$ и по закону де Моргана $\Gamma \vdash \neg\exists y(y \mid x)A$. Но y не входит в формулу A — и это значит, что выполняется условие корректного переименования связанных переменных (см. с. 52). Поэтому $\exists y(y \mid x)A \sim \exists xA$ и окончательно $\Gamma \vdash \neg\exists xA$.

Но Γ содержит формулу $\exists xA$, следовательно, Γ должно быть противоречивым, но это противоречит условию.$\triangleright$

Теорема 24 (Гёделя). *Любая непротиворечивая теория* Γ *сигнатуры* σ *имеет модель.*

$\triangleleft$Мы ограничимся случаем, когда сигнатура имеет конечное количество предикатных символов и констант, хотя теорема обобщается и на бесконечные сигнатуры.

Чтобы задать модель, необходимо выбрать предметную область, после чего проинтерпретировать на этой предметной области константы и предикатные символы. В процессе доказательства сперва будет построена такая интерпретация, а потом будет доказано, что все формулы из Γ в ней истинны.

В качестве предметной области возьмём множество натуральных чисел. Если исходная сигнатура σ содержит n констант, то пусть их интерпретацией будет n первых натуральных чисел. Кроме того, для каждого натурального числа, начиная с n[4], мы добавим в исходную сигнатуру по новой константе. У нас, таким образом, получится новая сигнатура σ', которая содержит все символы из σ и счётно-бесконечное множество констант, каждая из ко-

[4] Или с $n+1$ — это зависит от того, считать ли нуль натуральным числом. По традиции в руководствах по математической логике и теории множеств нуль включают в множество натуральных чисел.

торых интерпретируется уникальным натуральным числом. Осталось проинтерпретировать предикатные символы.

Теперь мы будем действовать примерно так же, как и при доказательстве леммы Линденбаума (на самом деле, нам нужна была не она сама, а способ рассуждений при её доказательстве). Занумеруем всё множество формул сигнатуры так, что A_i будет обозначать i-ю по порядку формулу. Обозначим также Γ через Γ_1 и будем на каждом i-м шаге добавлять к Γ_i формулы

$$\begin{cases} \neg A_i, \text{ если добавление } A_i \text{ к } \Gamma_i \text{ ведёт к противоречию,} \\ \exists x B \text{ и } (c \mid x)B, \text{ если добавление } A_i \text{ к } \Gamma_i \\ \qquad \text{непротиворечиво, а формула } A_i \text{ имеет вид } \exists x B, \\ A_i \text{ в остальных случаях.} \end{cases}$$

Результатом всех этих добавлений будет полное непротиворечивое множество формул Γ': его полнота следует из построения, непротиворечивость на каждом i-м шаге следует из леммы 23, а непротиворечивость всего Γ' доказывается так же, как в лемме Линденбаума. К тому же, множество Γ' обладает тем свойством, что если $\Gamma' \vdash \exists x B$, то найдётся такая константа c_j, что $\Gamma' \vdash (c_j \mid x)B$.

Рассмотрим все замкнутые атомарные формулы σ', т. е. формулы вида

$$P(c_{j_1}, \ldots, c_{j_n}),$$

где P — предикатный символ валентности n, а c_j — j-я константа сигнатуры σ'. В силу полноты и непротиворечивости Γ' для каждой такой формулы возможны всего два варианта: либо она сама, либо её отрицание выводятся из Γ'. Естественно предложить такую модель, в которой если $\Gamma' \vdash P(c_{j_1}, \ldots, c_{j_n})$, то $[P(c_{j_1}, \ldots, c_{j_n})] = \mathfrak{t}$, в противном случае — $[P(c_{j_1}, \ldots, c_{j_n})] = \mathfrak{f}$. Т. к. нашей сигнатуре σ' константы имеются для всех элементов предметной области, мы тем самым полностью задаём интерпретацию всех предикатных символов на множестве натуральных чисел. Построение модели $\mathfrak{M}$ завершено.

Теперь нам необходимо доказать, что все формулы из Γ, рассматриваемые как формулы сигнатуры σ, одновременно истинны в $\mathfrak{M}$. Для этого нам достаточно доказать, что все замкнутые формулы, выводимые из Γ в сигнатуре σ, истинны в $\mathfrak{M}$. Для начала будем действовать в терминах расширенного множества формул Γ' расширенной сигнатуры σ' и докажем, что для любой замкнутой формулы A сигнатуры σ' имеет место пара утверждений:

$$\begin{cases} \text{если } \Gamma' \vdash A, \text{ то } A \text{ истинна в } \mathfrak{M}, \\ \text{если } \Gamma' \nvdash A, \text{ то } A \text{ ложна в } \mathfrak{M}. \end{cases}$$

В конечном итоге нам нужно только первое из этих утверждений, но в процессе доказательства индукцией по построению мы воспользуемся также и вторым из них в качестве предположения индукции, поэтому будем доказывать оба.

Итак, индукция по построению. Для всякой замкнутой формулы имеет место один из перечисленных случаев:

1) Формула является атомарной. В этом случае оба утверждения верны по построению интерпретации $\mathfrak{M}$.

2) Формула имеет вид $\neg A$. Если $\Gamma' \vdash \neg A$, то в силу непротиворечивости $\Gamma' \nvdash A$. В этом случае, по предположению индукции, A — ложна и, следовательно, $\neg A$ — истинна. Если $\Gamma' \nvdash \neg A$, то в силу полноты $\Gamma' \vdash A$. По предположению индукции, A — истинна и, следовательно, $\neg A$ — ложна.

3) Формула имеет вид $A\gamma B$, где γ — логическая связка. Возможны только четыре комбинации выводимостей для формул A и B:

$$\begin{array}{llllll} \Gamma' \vdash \neg A, \neg B, & \text{откуда} & \Gamma' \vdash & A \Rightarrow B, & \neg(A \,\&\, B), & \neg(A \vee B). \\ \Gamma' \vdash \neg A, \quad B, & \text{откуда} & \Gamma' \vdash & A \Rightarrow B, & \neg(A \,\&\, B), & A \vee B. \\ \Gamma' \vdash \quad A, \neg B, & \text{откуда} & \Gamma' \vdash & \neg(A \Rightarrow B), & \neg(A \,\&\, B), & A \vee B. \\ \Gamma' \vdash \quad A, \quad B, & \text{откуда} & \Gamma' \vdash & A \Rightarrow B, & A \,\&\, B, & A \vee B. \end{array}$$

(Тут мы воспользовались утверждениями леммы 8 из § 1.2.)

Пусть, например, $\Gamma' \vdash A \Rightarrow B$. В силу непротиворечивости Γ' исключён случай, когда $\Gamma' \vdash A, \neg B$, во всех же остальных случаях $A \Rightarrow B$ должна быть истинной по предположению индукции. Пусть теперь $\Gamma' \nvdash A \Rightarrow B$. Это возможно только в ситуации $\Gamma' \vdash A, \neg B$, в которой, по предположению индукции, A — истинна, B — ложна и, следовательно, $A \Rightarrow B$ ложна.

Аналогично разбираются случаи для всех остальных логических связок.

4) Формула имеет вид $\exists x A$. По построению Γ' имеется такая константа c, что $\Gamma' \vdash (c \mid x)A$. В силу замкнутости $\exists x A$ параметром A может являться только переменная x, поэтому $(c \mid x)A$ замкнута и имеет меньшее количество логических связок, чем $\exists x A$. Поэтому можно применить предположение индукции, в силу которого $(c \mid x)A$ истинна в $\mathfrak{M}$. Тогда по лемме 12 из § 1.3 формула A истинна на оценке $(x \mapsto c)$ и $\exists x A$ истинна.

Пусть $\Gamma' \nvdash \exists x A$. Утверждение о ложности $\exists x A$ в этом случае докажем от противного. Если предположить, что $\exists x A$ истинна, то найдётся элемент предметной области, а с ним и константа c, для которой $(c \mid x)A$ истинна. По предположению индукции, все более простые истинные формулы обязаны быть выводимыми, поэтому $\Gamma' \vdash (c \mid x)A$. Но по $\exists$-схеме $(c \mid x)A \Rightarrow \exists x A(x)$, и по modus ponens $\Gamma' \vdash \exists x A$ — противоречие.

5) Пусть формула имеет вид $\forall x A$ и выводима из Γ'. Формула $\forall x A \Rightarrow (c \mid x)A$ является аксиомой для любой константы c, поэтому и $(c \mid x)A$ выводима из Γ' для любой константы c. По предположению индукции каждая формула $(c \mid x)A$ истинна в $\mathfrak{M}$, значит, A истинна на любой оценке $(x \mapsto c)$ и (т. к. множество констант в σ' «покрывает» всю предметную область) $\forall x A$ истинна.

Покажем, наконец, что если $\Gamma' \not\vdash \forall x A$, то $\forall x A$ ложна в $\mathfrak{M}$. Действительно, если не выводима $\forall x A$, то выводимо её отрицание, доказуемо эквивалентное $\exists x \neg A$. По построению Γ' имеется такая константа c, что выводима формула $\neg(c \mid x)A$, истинная по предположению индукции. Поэтому A истинна не при всех значениях x, и формула $\forall x A$ ложна.

Итак, мы показали, что всякая замкнутая формула, выводимая из Γ' (в частности, принадлежащая множеству исходных посылок Γ, являющемуся частью Γ'), истинна в $\mathfrak{M}$. Т. е. $\mathfrak{M}$ действительно является моделью для непротиворечивого множества замкнутых формул Γ.$\triangleright$

Заметим, что, доказывая теорему 24, мы построили модель на множестве натуральных чисел. Отсюда следует ещё одно утверждение, являющееся вариантом *теоремы Лёвенгейма–Сколема.*

Теорема 25 (Лёвенгейма–Сколема)**.** *Если теория конечной сигнатуры имеет модель, то она также имеет модель на множестве натуральных чисел в качестве предметной области.*

Упр. 36. Докажите, что если формула истинна в любой модели на множестве натуральных чисел, то она общезначима.

Упр. 37. Следует ли общезначимость формулы из её истинности на любой модели с конечным числом элементов предметной области? (Попробуйте привести контрпример.)

Теперь для нас уже не составит труда доказать главный результат этого параграфа.

Теорема 26 (Гёделя о полноте исчисления предикатов)**.** *Всякая общезначимая формула выводима в исчислении предикатов: если* $\models A$*, то* $\vdash A$*.*

$\triangleleft$Сначала рассмотрим только случай замкнутых формул. Пусть $\models A$. Это значит, что нет такой модели, в которой $\neg A$ была бы истинной. Следовательно, множество, состоящее из единственной формулы $\neg A$, будет противоречивым (если бы оно не было

противоречивым, то тогда у $\neg A$ была бы модель). Значит, есть такая C, что $\neg A \vdash C$ и $\neg A \vdash \neg C$, откуда $\vdash \neg\neg A$ и $\vdash A$.

Теперь рассмотрим общезначимые формулы со свободными переменными. Если $\models A$, то по определению общезначимости и истинности формулы $\forall x A$, $\models \forall x A$. Пусть A' — замыкание формулы A кванторами всеобщности. Тогда $\models A'$ и $\vdash A'$. Осталось воспользоваться аксиомой $\forall x A \Rightarrow A$ и modus ponens для того, чтобы перейти к выводу исходной формулы A.$\triangleright$

Заметим, что утверждение теоремы 26 содержит в себе утверждение теоремы 10 об исчислении высказываний. Рассмотрим сигнатуру, содержащую только нуль-местные предикатные символы $P_1, \ldots P_n$, и тогда теорема 26 будет выражать, в частности, выводимость любой пропозициональной тавтологии над пропозициональными переменными $P_1, \ldots P_n$. Это неудивительно, если вспомнить, что в процессе доказательства мы пользовались леммой 8 из § 1.2. Поэтому если убрать из доказательства теоремы 24 о существовании модели все упоминания о кванторах, то можно получить совершенно новый способ доказательства теоремы 10. Но между приведёнными доказательствами теорем 26 и 10 есть разница, о которой мы уже упоминали. Доказывая выводимость пропозициональных тавтологий, мы получили универсальный алгоритм построения вывода за конечное число действий. Доказательство же выводимости любой общезначимой формулы исчисления предикатов не даёт инструкций относительно того, как этот вывод построить.

ГЛАВА 2

ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ

§ 2.1. Аксиомы и первые следствия

1. Что такое множество? «Под *множеством* мы понимаем соединение в некое целое определённых хорошо различимых предметов нашего созерцания или нашего мышления (которые будут называться *элементами* множества)[1]» — пишет основатель теории множеств, Георг Кантор. Но, например, уже Феликс Хаусдорф в [13] замечает, что «пытаться давать множеству определения вида: „множество есть объединение отдельных вещей в одно целое“ или „множество есть множественность, мыслимая как единство“ — значит определять то же самое при помощи того же самого, если не тёмное при помощи ещё более тёмного».

Множество, по-видимому, является основным, невыводимым понятием в математике, подобно тому, как в геометрии Евклида невыводимым является понятие точки. Множество тем более является основным понятием, что практически все математические конструкции, как мы увидим, сводимы к множествам.

Предположим, что объект x некоторым образом состоит из объектов $a, b, c\ldots$ произвольной природы и что эти объекты полностью определяют x. В этом случае мы говорим, что x — множество, a, b, $c\ldots$ — его элементы, и $x = \{a, b, c\ldots\}$. При рассмотрении элемента по отношению ко множеству существенным является лишь факт вхождения или невхождения во множество: такие понятия, *как порядок элементов*, а также *число вхождений элемента* для множества самого по себе отсутствуют. Так, можно сказать, что $\{a, b, c\} = \{c, a, b\} = \{c, b, a, c, c\}$. Факт вхождения элемента во множество записывается следующим образом: $a \in x$ («a принадлежит x»).

[1] Г. Кантор. Труды по теории множеств. — М.: Наука, 1985 — 431 с. С. 173.

Примеры множеств: множество студентов МФТИ, множество страниц этой книги, множество натуральных чисел, множество точек евклидова пространства, множество функций действительного переменного. Эти простые примеры наводят на мысль, что множеством можно считать любую совокупность объектов, выбранных по определённому условию. Это, однако, не совсем так, в чём мы вскоре убедимся.

2. Перейдём теперь к формальному построению аксиоматической теории множеств, понимая термин *теория* в смысле, определённом на с. 62. Рассмотрим сигнатуру с единственным двухместным предикатным символом $\in$. Предикат $\in (x, y)$, традиционно обозначаемый через $x \in y$, принимает значение $\mathfrak{t}$ в случае, когда x является элементом множества y. В свою очередь x тоже может иметь элементы.

Будем говорить, что x является *подмножеством* y и писать $x \subseteq y$, если все элементы x являются также элементами y. Формально

$$x \subseteq y \rightleftharpoons \forall t(t \in x \Rightarrow t \in y)$$

(здесь и далее знак $\rightleftharpoons$ означает «есть по определению»: мы будем пользоваться этим знаком для того, чтобы вводить сокращающие обозначения).

Лемма 27. *Отношение «быть подмножеством» рефлексивно* $(\vdash x \subseteq x)$ *и транзитивно* $(\vdash x \subseteq y \,\&\, y \subseteq z \Rightarrow x \subseteq z)$.

$\lhd$Для доказательства рефлексивности достаточно воспользоваться тавтологией $t \in x \Rightarrow t \in x$ и правилом обобщения по t.

Докажем транзитивность. Используя закон пронесения квантора всеобщности через конъюнкцию и $\forall$-аксиому, имеем

$$x \subseteq y \,\&\, y \subseteq z \Rightarrow (t \in x \Rightarrow t \in y) \,\&\, (t \in y \Rightarrow t \in z).$$

Заметим, что тавтологией является

$$(t \in x \Rightarrow t \in y) \,\&\, (t \in y \Rightarrow t \in z) \Rightarrow (t \in x \Rightarrow t \in z).$$

Используя правило $\frac{A \Rightarrow B, B \Rightarrow C}{A \Rightarrow C}$, имеем

$$x \subseteq y \,\&\, y \subseteq z \Rightarrow (t \in x \Rightarrow t \in z),$$

и по $\forall$-правилу Бернайса $\vdash x \subseteq y \,\&\, y \subseteq z \Rightarrow x \subseteq z$, что и требовалось.$\triangleright$

В дальнейшем в доказательствах мы будем опускать столь подробные ссылки на правила формального вывода, предоставляя их восстановление читателю.

3. Мы будем говорить, что множества *равны*, и писать $x = y$, если они состоят из одних и тех же элементов, т. е. если любой элемент t входит в x тогда и только тогда, когда t входит в y. Формально

$$x = y \rightleftharpoons \forall t(t \in x \Leftrightarrow t \in y).$$

Легко доказать, что

$$x = y \sim x \subseteq y \,\&\, y \subseteq x.$$

Проверим, что это определение удовлетворяет стандартным свойствам равенства.

Лемма 28. *Равенство множеств рефлексивно* ($\vdash x = x$), *симметрично* ($\vdash x = y \Rightarrow y = x$) *и транзитивно* ($\vdash x = y \,\&\, y = z \Rightarrow \Rightarrow x = z$).

$\triangleleft$Рефлексивность: $x = x \sim x \subseteq x \,\&\, x \subseteq x$, но последнее всегда истинно в силу рефлексивности $\subseteq$.

Симметричность: $x = y \sim x \subseteq y \& y \subseteq x \sim y \subseteq x \& x \subseteq y \sim y = x$.

Транзитивность: $x = y \,\&\, y = z \sim x \subseteq y \,\&\, y \subseteq x \,\&\, y \subseteq z \,\&\, z \subseteq \subseteq y$, откуда в силу транзитивности $\subseteq$ следует $x \subseteq z \,\&\, z \subseteq x$, что и требовалось.$\triangleright$

Упр. 38. [2]. Докажите, что если $x_1 \subseteq x_2 \subseteq \ldots \subseteq x_n \subseteq x_n$, то $x_1 = = x_2 = \ldots = x_n$.

Достаточно ли только что доказанных свойств для того, чтобы определённое нами равенство множеств полностью имело тот смысл, который мы обычно вкладываем в понятие «равенство»?

Ещё нет. Если какие-то объекты равны, то не должно существовать способа их различения, т. е. для любой формулы A (возможно, содержащей x в качестве параметра) должно быть доказуемо соотношение

$$x = y \Rightarrow (A \Rightarrow (y \mid x)A).$$

Пока что для определённого нами отношения это недоказуемо. Действительно: мы можем представить себе модель, в которой множества, состоящие из одних и тех же элементов, могут тем не менее различаться между собой по какому-нибудь дополнительному признаку — что, конечно, не согласуется с представлением о том, что множество полностью задаётся набором своих элементов и только им. Чтобы исключить такие некорректные интерпретации, вводится *аксиома экстенсиональности*, или *объёмности*, которая является первой в списке аксиом теории множеств:

$$\forall x \forall y (x = y \Rightarrow \forall z (x \in z \Rightarrow y \in z)).$$

Из этой аксиомы уже следует неразличимость множеств, состоящих из одних и тех же элементов.

Теорема 29. *Для любой формулы A, возможно, содержащей x в качестве параметра, из аксиомы экстенсиональности выводится $x = y \Rightarrow (A \Rightarrow (y \mid x)A)$.*

$\lhd$Случай, когда A не содержит свободно x, тривиален. Доказательство для случая, когда x является параметром A, мы, как обычно, проведём индукцией по построению формулы A. При этом сначала мы дополнительно предположим, что A не содержит y свободно, т. е. формула $(x \mid y)(y \mid x)A$ текстуально совпадает с A.

1) Атомарных формул с участием x может быть всего два вида: $z \in x$ и $x \in z$. В первом случае базис индукции обеспечивается определением равенства, во втором — аксиомой экстенсиональности.

2) Формула имеет вид $\neg A$. По закону контрапозиции

$$\neg A \Rightarrow \neg(y \mid x)A \sim (y \mid x)A \Rightarrow A.$$

По предположению индукции

$$y = x \Rightarrow ((y \mid x)A \Rightarrow (x \mid y)(y \mid x)A).$$

Воспользовавшись симметричностью равенства и предположением об отсутствии свободных вхождений y в A, имеем $x = y \Rightarrow (\neg A \Rightarrow \neg(y \mid x)A)$, что и требовалось.

3) Формула имеет вид $A\&B$. По предположению индукции, имеют место соотношения

$$x = y \Rightarrow (A \Rightarrow (y \mid x)A), x = y \Rightarrow (B \Rightarrow (y \mid x)B).$$

Воспользовавшись схемой $(A \Rightarrow B) \Rightarrow ((A \Rightarrow C) \Rightarrow (A \Rightarrow \Rightarrow B \,\&\, C))$ и дважды правилом modus ponens, имеем

$$x = y \Rightarrow (A \Rightarrow (y \mid x)A) \,\&\, (B \Rightarrow (y \mid x)B).$$

Воспользовавшись далее тавтологией

$$(A \Rightarrow (y \mid x)A) \,\&\, (B \Rightarrow (y \mid x)B) \Rightarrow (A \,\&\, B \Rightarrow (y \mid x)(A \,\&\, B)),$$

получим, что требовалось.

4) Формула имеет вид $\forall z A$. По предположению индукции

$$x = y \Rightarrow (A \Rightarrow (y \mid x)A),$$

что эквивалентно

$$x = y \,\&\, A \Rightarrow (y \mid x)A.$$

С другой стороны, используя $\forall$-аксиому и удаляя, а затем вводя конъюнкцию, имеем

$$x = y \,\&\, \forall z A \Rightarrow x = y \,\&\, A,$$

откуда

$$x = y \,\&\, \forall z A \Rightarrow (y \mid x)A.$$

Левая часть импликации не содержит z свободно. Используя $\forall$-правило Бернайса и замену формулы на эквивалентную, получаем

$$x = y \Rightarrow (\forall z A \Rightarrow \forall z (y \mid x)A).$$

Все прочие логические связки и квантор существования выразимы через отрицание, конъюнкцию и квантор всеобщности.

Теперь распространим доказательство на случай, когда y является параметром A. Выберем переменную z, отличную от x и такую, что z не входит свободно в A. В этом случае формула $(z \mid y)A$ не содержит y свободно и с учётом $\forall$-правила Бернайса

$$x = y \Rightarrow \forall z((z \mid y)A \Rightarrow (y \mid x)(z \mid y)A).$$

Осталось воспользоваться $\forall$-аксиомой с подстановкой $(y \mid z)$ к правой части импликации и соединить получившиеся импликации. В силу выбора переменной z формула $(y \mid z)(z \mid y)A$ текстуально совпадёт с A, а формула $(y \mid z)(y \mid x)(z \mid y)A$ — с $(y \mid x)A$.▷

Если присмотреться к тому, как была использована аксиома экстенсиональности при доказательстве неразличимости равных множеств, то можно прийти к выводу, что с тем же успехом можно было бы принять за определение равенства условие $\forall z(x \in z \Rightarrow y \in \in z)$, а свойство $x = y \Rightarrow x \subseteq y \,\&\, y \subseteq x$ считать аксиомой.

Третий возможный подход состоит в том, что вначале в качестве предикатного символа вводится отношение равенства (знак $=$). Для равенства вводятся аксиомы рефлексивности, симметричности, транзитивности и схема аксиом $x = y \Rightarrow (A \Rightarrow \Rightarrow (y \mid x)A)$. В результате получается так называемое «исчисление предикатов с равенством». Затем вводится второй предикатный символ — знак принадлежности $\in$, а также аксиома $x = y \Leftrightarrow$

$\Leftrightarrow x \subseteq y \,\&\, y \subseteq x$. Все три подхода встречаются в литературе, посвящённой теории множеств, и в конечном итоге эквивалентны.

4. Наличие знака равенства в формальной системе позволяет ввести квантор «существования и единственности», обозначаемый $\exists!$. Смысл выражения $\exists! x A$ (читается «существует единственный x такой, что A») заключается в следующем: существует такой x, что A, и все объекты, для которых A, равны между собой. Формально

$$\exists! x A \rightleftharpoons \exists x (A \,\&\, \forall y ((y \mid x) A \Rightarrow x = y)).$$

Ещё раз отметим, что формулы вида $\exists! x A$ могут быть введены только в такой системе, в которой тем или иным образом определено отношение равенства, поэтому они не рассматривались нами при обзоре чистого исчисления предикатов.

5. Введём также сокращающие обозначения

$$\begin{aligned} x \notin y &\rightleftharpoons \neg x \in y, \\ x \neq y &\rightleftharpoons \neg x = y, \\ x \subset y &\rightleftharpoons x \subseteq y \,\&\, x \neq y. \end{aligned}$$

В последнем случае ($x \subset y$) мы говорим, что «x есть строгое подмножество y». Чтобы различать $x \subseteq y$ и $x \subset y$, мы иногда в случае $x \subseteq y$ будем говорить, что x является «нестрогим подмножеством» y. (Здесь очевидна аналогия между строгим и нестрогим неравенством в арифметике.)

6. Выше уже отмечалось, что в соответствии с нашей интуицией множество может быть задано некоторым логическим условием на его элементы. Это условие может быть выписано в виде синтаксически корректной формулы сигнатуры теории множеств. Например, если x и y — некоторые известные нам заранее множества, то мы можем определить

- p_x — множество всех подмножеств x — условием

$$t \in p_x \Leftrightarrow t \subseteq x,$$

- u_{xy} — множество, образованное объединением элементов x и y по условию

$$t \in u_{xy} \Leftrightarrow t \in x \vee t \in y,$$

и т. д. и т. п.

На первый взгляд нет ничего неестественного в том, чтобы предположить, что любая синтаксически корректная формула A, содержащая x в качестве свободной переменной, определяет множество, состоящее из всех тех x, на которых A истинно. Для того чтобы обеспечить существование таких множеств, попробуем ввести следующую схему аксиом, называемую схемой аксиом неограниченного выделения:

$$\exists y \forall z (z \in y \Leftrightarrow A),$$

в которой A обозначает синтаксически корректную формулу теории множеств, не содержащую y свободно.

Из этой схемы, в частности, будет следовать существование пустого множества (множества без элементов), если в качестве A взять тождественно ложное высказывание (например, $z \neq z$), и множества всех множеств, если A тождественно истинна (например, $z = z$).

Докажем, что множество, существование которого обеспечивается схемой выделения, единственно.

Лемма 30. *Если для некоторой формулы A, не содержащей y свободно, выводима формула $\exists y \forall z (z \in y \Leftrightarrow A)$, то выводима также формула $\exists! y \forall z (z \in y \Leftrightarrow A)$.*

$\lhd$По определению $\exists! y \forall z (z \in y \Leftrightarrow A)$ означает

$$\exists y (\forall z (z \in y \Leftrightarrow A) \,\&\, \forall t (\forall z (z \in t \Leftrightarrow A) \Rightarrow \forall u (u \in y \Leftrightarrow u \in t))).$$

Имея в виду правило вывода

$$\frac{\exists x A, A \Rightarrow B}{\exists x B}$$

(обоснуйте его самостоятельно), достаточно доказать, что

$$\forall z(z \in y \Leftrightarrow A) \Rightarrow \forall t(\forall z(z \in t \Leftrightarrow A) \Rightarrow \forall u(u \in y \Leftrightarrow u \in t)).$$

Имея в виду тавтологию $A \Rightarrow (B \Rightarrow C) \sim A \,\&\, B \Rightarrow C$ и $\forall$-правило Бернайса, достаточно доказать, что

$$\forall z(z \in y \Leftrightarrow A) \,\&\, \forall z(z \in t \Leftrightarrow A) \Rightarrow \forall u(u \in y \Leftrightarrow u \in t).$$

Имея в виду тавтологию $(A \Leftrightarrow C) \,\&\, (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow B)$, достаточно доказать, что

$$\forall z(z \in y \Leftrightarrow A) \,\&\, \forall z(z \in t \Leftrightarrow A) \Rightarrow (u \in y \Leftrightarrow A) \,\&\, (u \in t \Leftrightarrow A).$$

Но последнее уже нетрудно сделать, используя соответствующие схемы логических аксиом. Переписав наши рассуждения в обратном порядке, получим формальный вывод для $\exists! y \forall z(z \in y \Leftrightarrow$ $\Leftrightarrow A)$, что и требовалось.$\triangleright$

Аксиому экстенсиональности вместе со схемой аксиом неограниченного выделения иногда называют «наивной теорией множеств». Несмотря на «интуитивную приемлемость» входящих в неё утверждений, эта система аксиом противоречива (в смысле, определённом на с. 62) и потому не может быть использована для построения корректной формальной теории.

Примем в качестве A формулу $x \notin x$. Множество, существование которого должно обеспечиваться схемой, назовём *множеством Рассела* и обозначим буквой R. Из определения следует, что R должно состоять из элементов, которые не содержат сами себя в качестве элемента. Используя соответствующую тавтологию, устанавливаем, что

$$\exists R \forall x(x \in R \Leftrightarrow x \notin x) \sim \exists R \forall x \neg(x \in R \Leftrightarrow x \in x).$$

От последней формулы можно вывести импликацию к $\exists R \neg(R \in$ $\in R \Leftrightarrow R \in R)$, что эквивалентно

$$\neg \forall R(R \in R \Leftrightarrow R \in R).$$

Но $R \in R \Leftrightarrow R \in R$ — тавтология, и по закону обобщения

$$\forall R(R \in R \Leftrightarrow R \in R).$$

Мы получили противоречие, из которого теперь можно вывести какую угодно формулу.

Рассуждая содержательно, мы приходим к противоречию таким образом: пусть R — множество всех x, таких, что x не содержит себя в качестве элемента. Содержит ли R себя в качестве элемента? Как положительный, так и отрицательный ответ на этот вопрос будет противоречить определению R, откуда мы заключаем, что такого множества попросту не может существовать. Следовательно, не может существовать и модели теории множеств, в которой выполнялась бы аксиома $\exists R \forall x(x \in R \Leftrightarrow x \notin x)$ и, как следствие, порождающая её схема $\exists z \forall x(x \in z \Leftrightarrow A)$. По этой причине схему неограниченного выделения следует отвергнуть.

Это противоречие (называемое *парадоксом Рассела* по фамилии логика, открывшего его в 1901 г.), несмотря на свою простоту, было отрыто уже после того, как стали известны другие противоречия «наивной» теории множеств, в настоящее время именуемые *парадоксом Бурали–Форти* (1897 г.) и *парадоксом Кантора* (1899 г.). Для их изложения, однако, требуется ряд нетривиальных понятий и теорем теории множеств, поэтому мы рассмотрим их позже (см. с. 123 и с. 165).

Популярная формулировка парадокса Рассела традиционно называется «задачей парикмахера» и звучит так: «Одному деревенскому парикмахеру приказали „брить всякого, кто сам не бреется, и не брить того, кто сам бреется“. Должен ли парикмахер брить самого себя?» Другой вариант: «В одном государстве вышел указ: „Мэры всех городов не должны жить в своих городах и должны жить в столице.“ Где должен жить мэр столицы?» Какие бы решения не приняли деревенский парикмахер и мэр столицы — они нарушат приказ. Причина в том, что эти приказы (как и схема ак-

сиом неограниченного выделения) внутренне противоречивы, хотя на поверхностный взгляд так может не показаться.

7. Итак, схема аксиом неограниченного выделения «чересчур сильна»: её следствиями являются противоречивые утверждения (в частности, те, что были открыты Расселом, Кантором, Бурали–Форти). Что следует предложить взамен? Признанный подход заключается в том, чтобы отказаться от произвола в построении формулы-условия A и рассматривать только некоторые заранее определённые классы условий. Этих классов условий, однако же, должно быть достаточно, чтобы образуемые с их помощью множества могли обеспечивать математические рассуждения.

В 1908 г. Э. Цермéло предложил систему аксиом теории множеств, основанную на этой идее. Позднее система Цермело была доработана А. Френкелем, и окончательный результат получил название *теории множеств Цермело–Френкеля*. В настоящий момент эта система аксиом является общепризнанным основанием теории множеств.

Тем не менее одна из предложенных Цермело и Френкелем аксиом — аксиома выбора — до сих пор вызывает полемику. С одной стороны, эта аксиома существенно упрощает доказательства ряда фундаментальных математических теорем. С другой стороны, из аксиомы выбора вытекают некоторые довольно «экзотические» следствия, среди которых — существование неизмеримых по Лебегу множеств (пример Виталй), «парадокс» Банаха–Тарского (шар может быть разрезан на конечное количество неизмеримых частей, из которых можно затем составить два шара, равных исходному) и т. д. (см., напр., [10], доступное изложение этих утверждений с доказательствами содержится также в брошюре [14]). Как показали Гёдель и Коэн (см., напр., [9], [12]), ни аксиома выбора, ни её отрицание не могут быть выведены из других аксиом системы Цермело–Френкеля.

Принятой на сегодняшний день практикой является различение теорем, которые могут быть получены без помощи аксиомы выбора, и теорем, для доказательства которых аксиома выбора су-

щественна (или, по крайней мере, неизвестно доказательство, не использующее аксиому выбора). Система аксиом Цермело–Френкеля без аксиомы выбора обозначается сокращением ZF, с аксиомой выбора — ZFC (буква C от англ. choice — выбор). Выводимость формулы A из аксиом ZF и ZFC обозначается как $\mathrm{ZF} \vdash A$ и $\mathrm{ZFC} \vdash A$ соответственно. Разумеется, если $\mathrm{ZF} \vdash A$, то $\mathrm{ZFC} \vdash A$, но не обязательно наоборот.

Полный список системы аксиом ZFC выглядит следующим образом:

1) *Аксиома экстенсиональности.* $\forall x \forall y (x = y \Rightarrow \forall z (x \in z \Rightarrow y \in \in z))$.

2) *Аксиома множества всех подмножеств.* Для любого множества x существует множество всех его подмножеств, называемое также *множеством-степенью* x: $\forall x \exists u \forall z (z \in u \Leftrightarrow z \subseteq x)$.

3) *Аксиома суммы.* Для любого множества x существует множество u, такое, что все элементы u являются элементами элементов x: $\forall x \exists u \forall z (z \in u \Leftrightarrow \exists v (z \in v \,\&\, v \in x))$.

4) *Схема аксиом подстановки.* Если v — множество, а формула A определяет двухместный предикат от z и x, то существует такое множество u, что $z \in u$ тогда и только тогда, когда существует такое $x \in v$, что A — истинно, и для этого x существует лишь одно w, такое, что $(w \mid z)A$ — истинно. Формально для всякой формулы A, не содержащей u и v свободно, но, возможно, содержащей x и z свободно, выполняется $\forall v \exists u \forall z (z \in u \Leftrightarrow \exists x (x \in v \,\&\, A \,\&\, \forall w ((w \mid z)A \Rightarrow z = w)))$.

5) *Аксиома регулярности, или фундирования.* Всякое непустое множество x содержит такой элемент y, что x и y не содержат общих элементов: $\forall x (\exists z \; z \in x \Rightarrow \exists y (y \in x \,\&\, \forall u \neg (u \in y \,\&\, u \in \in x)))$.

6) *Аксиома бесконечности.* Существует такое множество u, что его элементом является пустое множество (множество без элементов), и, кроме того, если какой-либо элемент z принадлежит u, то множество, образованное объединением элементов z и одноэлементного множества $\{z\}$, также принадлежит u: $\exists u(\forall z(\forall x \neg x \in z \Rightarrow z \in u) \,\&\, \forall z(z \in u \Rightarrow \forall v(\forall x(x \in v \Leftrightarrow x \in z \vee \vee x = z) \Rightarrow v \in u)))$.

7) *Аксиома выбора.* Для любого семейства (множества непустых множеств), такого, что любые два множества этого семейства не имеют общих элементов, существует множество, содержащее ровно по одному элементу из каждого множества исходного семейства: $\forall x(\forall y \forall z(y \in x \,\&\, z \in x \Rightarrow (\exists v\ v \in y \,\&\, (\exists u(u \in \in z \,\&\, u \in y) \Rightarrow z = y))) \Rightarrow \exists u \forall t(t \in x \Rightarrow \exists v \forall w(v = w \Leftrightarrow w \in \in u \,\&\, w \in t)))$.

Система ZFC определена.

Сразу заметим, что аксиомы 2, 3 и схема 4 являются частными случаями схемы неограниченного выделения (мы надеемся, читатель уже понимает, что стоящие впереди кванторы всеобщности в данном случае не играют роли). Следовательно, к этим формулам применима лемма 30, в соответствии с которой кванторы $\exists u$ в них могут быть заменены на $\exists! u$.

Сформулированные в следующей теореме следствия схемы 4 настолько важны с практической точки зрения, что их зачастую включают в число аксиом ZF, хотя в действительности они являются выводимыми утверждениями. Ко всем им тоже применима лемма 30, так что кванторы $\exists u$ в них могут быть заменены на $\exists! u$.

Теорема 31. *Следствием аксиом ZF 1, 2, 4 являются*

- *Схема аксиом ограниченного выделения. Для всякой формулы A, не содержащей u свободно, но, возможно, содержащей z свободно,* $\forall x \exists u \forall z(z \in u \Leftrightarrow z \in x \,\&\, A)$.
- *Аксиома пустого множества. Существует множество, не содержащее элементов:* $\exists u \forall z \neg\ z \in u$.

- *Аксиома пары. Если x, y — множества, то также существует множество, единственными элементами которого являются x и y:* $\forall x \forall y \exists u \forall z (z \in u \Leftrightarrow z = x \vee z = y)$.

$\lhd$1. *Схема аксиом ограниченного выделения.* Подставим в схему подстановки формулу вида $A \,\&\, z = x$, где A не содержит z, u, v свободно, но, возможно, содержит x:

$$\forall v \exists u \forall z (z \in u \Leftrightarrow \exists x (x \in v \,\&\, A \,\&\, z = x \,\&\, \forall w (A \,\&\, w = x \Rightarrow z = w))).$$

Покажем, что из этой формулы следует схема ограниченного выделения. Прежде всего «избавимся» от той части формулы, что следует за квантором $\forall w$. Заметим, что $\vdash A \& z = x \Rightarrow (A \& w = x \Rightarrow \Rightarrow z = w)$, т. к. последнее утверждение эквивалентно $A \& w = x \& z = = x \Rightarrow z = w$, что выводимо из транзитивности и симметричности равенства.

Воспользовавшись тем фактом, что если $\vdash A \Rightarrow B$, то $A \,\&\, B \sim \sim A$, и заменой подформулы на эквивалентную, получаем, что исходная формула эквивалентна

$$\forall v \exists u \forall z (z \in u \Leftrightarrow \exists x (x \in v \,\&\, A \,\&\, z = x)).$$

Это уже почти схема ограниченного выделения. Теперь достаточно показать, что

$$\exists x (x \in v \,\&\, A \,\&\, z = x) \sim z \in v \,\&\, (z \mid x) A.$$

Обозначим формулу $x \in v \,\&\, A$ через A'.

В одну сторону: $\vdash z = x \Rightarrow (A' \Rightarrow (z \mid x) A')$ — теорема 29, $\vdash z = x \,\&\, A' \Rightarrow (z \mid x) A'$ — эквивалентно предыдущему, $\vdash \exists x (z = = x \,\&\, A') \Rightarrow (z \mid x) A'$ — $\exists$-правило.

В обратную сторону: $\vdash z = z \,\&\, (z \mid x) A' \Rightarrow \exists x (A' \,\&\, z = x)$ — $\exists$-схема, $\vdash z = z \Rightarrow ((z \mid x) A' \Rightarrow \exists x (A' \,\&\, z = x))$ — эквивалентно предыдущему, $\vdash (z \mid x) A' \Rightarrow \exists x (A' \,\&\, z = x)$ — modus ponens.

2. *Аксиома пустого множества.* Подставим в только что доказанную схему аксиом ограниченного выделения формулу $z \neq z$:

$$\forall x \exists u \forall z (z \in u \Leftrightarrow z \in x \,\&\, z \neq z).$$

Заметим, что $\vdash \forall z(z \in u \Leftrightarrow z \in x \,\&\, z \neq z) \Rightarrow (z \in u \Rightarrow z \neq z)$.

По схеме сведения к противоречию

$$(z \in u \Rightarrow z = z) \Rightarrow ((z \in u \Rightarrow z \neq z) \Rightarrow \neg\, z \in u).$$

Но $z = z$, поэтому $z \in u \Rightarrow z = z$ и

$$(z \in u \Rightarrow z \neq z) \Rightarrow \neg\, z \in u.$$

По правилу $\frac{\exists x A, A \Rightarrow B}{\exists x B}$ имеем

$$\exists u \forall z \neg\, z \in u,$$

что и требовалось. Заметим, что «ограничивающее» множество x при доказательстве «потерялось». Однако если бы мы попытались вместо $z \neq z$ в схему ограниченного выделения подставить формулу $z = z$, то вместо множества всех множеств получили бы всего лишь множество, равное x.

3. *Аксиома пары* таким же прямым образом может быть доказана на основании аксиомы множества-степени и схемы подстановки. Мы не будем останавливаться на её формальном доказательстве, намётки которого будут приведены на с. 94.▷

Упр. 39. Объясните разницу между утверждениями «множество x пусто» и «множество x не существует».

8. Для того чтобы лучше понять смысл аксиомы фундирования, запишем отрицание её отрицания:

$$\neg\exists x(\exists z\ z \in x \,\&\, \forall y(y \in x \Rightarrow \exists u(u \in y \,\&\, u \in x))),$$

что означает следующее: не существует непустого множества x, такого, что для каждого его элемента y найдётся такой $u \in x$, что $u \in y$.

Всякое множество в ZF обязано быть фундированным (т. е. удовлетворять аксиоме фундирования) и, следовательно, не может существовать

- множества, состоящего из единственного элемента x, такого, что $x \in x$,

- множества, состоящего из двух элементов x и y, таких, что $x \in y \,\&\, y \in x$, и вообще такого множества, что его элементы $x_1, \dots x_n$ «закольцованы» по отношению принадлежности условием $x_1 \in x_2 \,\&\, \dots \,\&\, x_{n-1} \in x_n \,\&\, x_n \in x_1$,

- множества, элементы которого образуют бесконечную последовательность $x_1 \ni x_2 \ni x_3 \dots$

Итак, мы ввели аксиоматику ZFC теории множеств и рассмотрели её самые первые следствия. Все теоремы следующих параграфов этой главы будут, по сути, выводимыми утверждениями аксиоматической теории множеств, причём утверждения, зависящие от аксиомы выбора, будут помечаться знаком $^\circ$.

§ 2.2. Операции над термами

1. Термы вида $\{z \mid A\}$. В прошлом параграфе мы на основании аксиом ZF установили, что, например, для любого множества x и произвольной формулы A, не содержащей u свободно, справедливо

$$\exists! u \forall z (z \in u \Leftrightarrow z \in x \,\&\, A).$$

Естественно было бы в дальнейшем ссылаться на существующее и единственное u как на терм, образованный с помощью формулы $z \in x \,\&\, A$. Обозначением для этого терма может служить, к примеру, комбинация знаков $\{z \mid z \in x \,\&\, A\}$ или даже $\{z \in x \mid A\}$ (читается «множество z из x, таких, что A»), где A следует заменить на любую синтаксически корректную формулу с параметром z.

Мы, однако, обязаны действовать в рамках языка, синтаксис которого определён на с. 33 (этот язык называется *языком первого порядка*), поскольку формальный логический вывод опирается на этот синтаксис. Для удобства мы уже расширяли язык первого порядка сокращающими обозначениями (такими, как $\subseteq$, $=$). При

этом указывалось, как можно преобразовать формулу с сокращающим обозначением в формулу языка первого порядка. Так, сокращённая запись $a \subseteq b$ соответствует формуле $\forall x(x \in a \Rightarrow x \in b)$, или, ещё точнее, формуле $(\forall x(\in (x, a) \Rightarrow \in (x, b)))$ языка первого порядка. Чтобы обоснованно пользоваться логическими теоремами и приёмами формального вывода, мы и в дальнейшем не должны потерять «синтаксическую основу» для всех используемых выражений.

Попытавшись ввести в язык термы вида $\{z \mid z \in x \,\&\, A\}$ легко убедиться, что им не могут соответствовать термы языка первого порядка, где термами являются только константы или переменные. Термы, образуемые при помощи формул, являются принципиально новой синтаксической конструкцией. Но мы тем не менее можем корректно внедрить такие термы в нашу систему, если покажем, как преобразовывать формулы с их участием в формулы языка первого порядка.

Итак, расширим синтаксис языка первого порядка теории множеств новым определением: *если* A *— формула, не содержащая переменную* u *в качестве параметра, и* $\mathrm{ZFC} \vdash \exists u \forall z(z \in u \Leftrightarrow A)$, *то* $\{z \mid A\}$ *— терм.* Термы такого вида могут участвовать в логических формулах наряду с переменными и константами, как определено на с. 33. Формулы расширенного языка могут быть переведены в формулы языка первого порядка по следующему алгоритму:

1) все вхождения терма $\{z \mid A\}$ заменяются на переменную u,

2) формула обрамляется конструкцией $\exists u(\forall z(z \in u \Leftrightarrow A) \,\&\, \ldots)$.

При этом, разумеется, имена переменных z и u должны быть выбраны таким образом, чтобы не возникло нежелательных связываний кванторами.

Например, формуле $\{z \mid A\} = \{z \mid B\}$, где A и B не содержат u и v свободно, соответствует в языке первого порядка формула

$$\exists u \exists v \forall z((z \in u \Leftrightarrow A) \,\&\, (z \in v \Leftrightarrow B) \,\&\, u = v).$$

Итак, условием корректности терма $\{z \mid A\}$ мы установили $\mathrm{ZFC} \vdash \exists u \forall z(z \in u \Leftrightarrow A)$. Следуя терминологии Бурбаки [15], будем говорить в таком случае, что A есть формула, *коллективизирующая по* z. Иначе говоря, формула A со свободной переменной z является коллективизирующей в том и только том случае, когда все z, на которых A истинна, образуют множество (как мы уже знаем, в теории ZFC это имеет место не всегда).

Будем говорить, что формула расширенного языка теории множеств *выводима*, если выводима соответствующая ей формула языка первого порядка. Две формулы расширенного языка называются *эквивалентными*, если эквивалентны соответствующие им формулы языка первого порядка.

2. Интуитивно ясно, что формула $t \in \{z \mid A\}$ должна быть эквивалентна $(t \mid z)A$. Действительно, некоторое t принадлежит множеству элементов, обладающих свойством A, тогда и только тогда, когда оно само обладает свойством A. Обоснуем это формально, доказав общую теорему.

Теорема 32. *Если формула* B' *получена из формулы* B *заменой подформул вида* $\xi \in u$ *на* $(\xi \mid z)A$, *то*

$$\exists u(\forall z(z \in u \Leftrightarrow A) \,\&\, B) \sim \exists u(\forall z(z \in u \Leftrightarrow A) \,\&\, B').$$

$\lhd$Докажем индукцией по построению формулы B, что

$$\vdash \forall z(z \in u \Leftrightarrow A) \,\&\, B \Rightarrow B',$$
$$\vdash \forall z(z \in u \Leftrightarrow A) \,\&\, B' \Rightarrow B,$$

из чего уже будет следовать требуемая эквивалентность.

1) Если B имеет вид $\xi \in u$, то

$$\begin{aligned}
&\forall z((z \in u \Leftrightarrow A) \,\&\, \xi \in u) \Rightarrow \\
&\quad \Rightarrow (\xi \mid z)((z \in u \Leftrightarrow A) \,\&\, \xi \in u) \sim \\
&\quad \sim (\xi \in u \Leftrightarrow (\xi \mid z)A) \,\&\, \xi \in u \sim \\
&\quad \sim (\xi \mid z)A \,\&\, \xi \in u \Rightarrow \\
&\quad\quad \Rightarrow (\xi \mid z)A,
\end{aligned}$$

$$\begin{array}{l}\forall z((z \in u \Leftrightarrow A)\ \&\ (\xi \mid z)A) \Rightarrow \\ \quad \Rightarrow (\xi \in u \Leftrightarrow (\xi \mid z)A)\ \&\ (\xi \mid z)A \sim \\ \qquad \sim (\xi \mid z)A\ \&\ \xi \in u \Rightarrow \\ \qquad\quad \Rightarrow \xi \in u.\end{array}$$

2) Если B имеет вид $\neg C$, то по предположению индукции

$$\begin{array}{l}\vdash \forall z(z \in u \Leftrightarrow A)\ \&\ C \Rightarrow C', \\ \vdash \forall z(z \in u \Leftrightarrow A)\ \&\ C' \Rightarrow C.\end{array}$$

Но эти формулы эквивалентны соответственно формулам

$$\begin{array}{l}\forall z(z \in u \Leftrightarrow A)\ \&\ \neg C' \Rightarrow \neg C, \\ \forall z(z \in u \Leftrightarrow A)\ \&\ \neg C \Rightarrow \neg C'.\end{array}$$

3) Если B имеет вид $C\ \&\ D$, то по предположению индукции

$$\begin{array}{l}\vdash \forall z(z \in u \Leftrightarrow A)\ \&\ C \Rightarrow C', \\ \vdash \forall z(z \in u \Leftrightarrow A)\ \&\ D \Rightarrow D',\end{array}$$

откуда

$$\vdash \forall z(z \in u \Leftrightarrow A)\ \&\ C\ \&\ D \Rightarrow C'\ \&\ D'.$$

Аналогично доказывается смежное утверждение (достаточно поменять местами формулы со штрихами и без штрихов).

4) Если B имеет вид $\forall x C$, то

$$\begin{array}{l}\vdash \forall z(z \in u \Leftrightarrow A)\ \&\ \forall x C \Rightarrow \\ \quad \Rightarrow \forall z(z \in u \Leftrightarrow A)\ \&\ (\eta \mid x)C \Rightarrow (\eta \mid x)C',\end{array}$$

где η — некоторая переменная, не используемая в C и A.

Отсюда выводится $\forall z(z \in u \Leftrightarrow A)\ \&\ \forall x C \Rightarrow \forall \eta(\eta \mid x)C'$, и в силу выбора имени переменной η

$$\forall z(z \in u \Leftrightarrow A)\ \&\ \forall x C \Rightarrow \forall x C'.$$

Аналогично доказывается смежное утверждение (достаточно поменять местами C и C').

Рассматривать остальные логические связки нет необходимости, т. к. любая формула может быть сведена к эквивалентной ей со связками $\neg$, $\&$, $\forall$.$\triangleright$

Теорема 32 даёт возможность свободно заменять конструкции вида $t \in \{z \mid A\}$ в формулах расширенного языка на $(t \mid z)A$, что значительно упрощает вид (и, как следствие, вывод) этих формул. Особенно полезно это после раскрытия сокращающих символов $\subseteq$ и $=$, сводящего их к предикатным символам $\in$.

Упр. 40. Проверьте, что для доказательства выводимости $\{z \mid A\} = \{z \mid B\}$ достаточно установить, что $A \sim B$.

3. Введём теперь сокращающие обозначения для некоторых стандартных термов. Для самоконтроля читатель может проверить (на основании аксиом ZF), что образующие их формулы являются коллективизирующими, а также самостоятельно обосновать те свойства, доказательства которых не будут приведены.

- Пустое множество: $\varnothing \rightleftharpoons \{z \mid z \neq z\}$.

  Свойства: $\varnothing \subseteq x$ (пустое множество является подмножеством любого множества), $x \subseteq \varnothing \Leftrightarrow x = \varnothing$.

  Действительно, раскрывая сокращения, получаем из первой формулы эквивалентные ей $\forall z(z \in \varnothing \Rightarrow z \in x)$ и $\forall z(z \neq \neq z \Rightarrow z \in x)$. Но последнее общезначимо в силу противоречия $z = z$ и $z \neq z$. Аналогичным образом доказываются и остальные утверждения о стандартных термах.

- Множество-степень (множество подмножеств x):

  $$\mathfrak{P}(x) \rightleftharpoons \{z \mid z \subseteq x\}.$$

  Свойства: $\varnothing \in \mathfrak{P}(x)$, $x \in \mathfrak{P}(x)$.

- Множество-сумма: $\bigcup x \rightleftharpoons \{z \mid \exists v(z \in v \,\&\, v \in x)\}$.

  Свойства: $x = \bigcup \mathfrak{P}(x)$, $x \subseteq \mathfrak{P}(\bigcup x)$.

  В первом случае доказательство сводится к необходимости доказать $\exists v(z \in v \,\&\, \forall t(t \in v \Rightarrow t \in x)) \sim z \in x$, во втором — к $\vdash z \in x \Rightarrow (u \in z \Rightarrow \exists v(v \in x \,\&\, u \in v))$.

- Множество, определяемое по аксиоме подстановки:

$$\{y \mid \exists x(x \in t \,\&\, A \,\&\, \exists! y A)\}$$

(где t — терм, A — синтаксически корректная формула).

- Множество, заданное ограниченным выделением:

$$\{z \in t \mid A\} \rightleftharpoons \{z \mid z \in t \,\&\, A\}$$

(где t — терм, A — синтаксически корректная формула). Его существование напрямую обусловлено схемой ограниченного выделения, доказанной в теореме 31.

- Множество-пересечение: $\bigcap x \rightleftharpoons \{z \in \bigcup x \mid \forall v(v \in x \Rightarrow z \in v)\}$.

- Одноэлементное множество (синглетон):

$$\{x\} \rightleftharpoons \{z \in \mathfrak{P}(x) \mid z = x\}.$$

Свойства синглетона:

1) $x \in \{x\}$,
2) $x \neq \{x\}$,
3) $u \in \{x\} \sim u = x$,
4) $x = y \sim \{x\} = \{y\}$,
5) $\bigcup\{x\} = x$.

Упр. 41. Проверьте вышеперечисленные свойства.
Упр. 42. Какие из термов $\varnothing$, $\mathfrak{P}(\varnothing)$, $\bigcup\varnothing$, $\bigcap\varnothing$, $\{\varnothing\}$ равны между собой? (Ответ: $\varnothing = \bigcup\varnothing = \bigcap\varnothing$; $\mathfrak{P}(\varnothing) = \{\varnothing\} \neq \varnothing$.)

- Неупорядоченная пара: $\{x, y\} \rightleftharpoons \{z \mid z = x \vee z = y\}$.

Проверка того, что $z = x \vee z = y$ является коллективизирующей формулой, представляет из себя довольно рутинное

упражнение по формальному выводу, завершающее доказательство теоремы 31. За основу берётся схема подстановки, в качестве «ограничивающего» множества v в которую подставляется терм $\mathfrak{P}\mathfrak{P}(\varnothing)$, а в качестве A — формула $(x = \varnothing \,\&\, \&\, z = a) \vee (x = \{\varnothing\} \,\&\, z = b)$. Последовательным упрощением формула приводится к виду $\forall x \forall y \exists u \forall z (z \in u \Leftrightarrow z = x \vee z = y)$.

Свойства неупорядоченной пары:

1) $\{x, y\} = \{y, x\}$,
2) $x \in \{x, y\}$,
3) $\{x, y\} = \{u, v\} \sim (x = u \,\&\, y = v) \vee (x = v \,\&\, y = u)$,
4) $\{x, x\} = \{x\}$,
5) $\{x, y\} = \{u\} \sim x = u \,\&\, y = u$.

Докажем третье свойство неупорядоченной пары.

Справа налево. Как из $x = u \,\&\, y = v$, так и из $x = v \,\&\, y = u$ в силу свойств равенства выводится $\{x, y\} = \{u, v\}$. Следовательно, то же выводится из дизъюнкции $(x = u \,\&\, y = v) \vee (x = v \,\&\, y = u)$.

Слева направо. Из $\{x, y\} = \{u, v\}$ следуют утверждения $x \in \{u, v\}$, $y \in \{u, v\}$, $u \in \{x, y\}$, $v \in \{x, y\}$, откуда выводится формула (обозначим её буквой F)

$$(x = u \vee x = v) \,\&\, (y = u \vee y = v) \,\&\, (x = u \vee y = u) \,\&\, (x = v \vee y = v).$$

Нам необходимо доказать, что $\vdash F \Rightarrow G$, где через G обозначено $(x = u \,\&\, y = v) \vee (x = v \,\&\, y = u)$. Для этого достаточно проверить, что во всех случаях, когда левая часть импликации истинна, правая также истинна. Рассуждаем следующим образом: пусть $x = u$, тогда первый и третий компоненты F становятся истинными. Для того, чтобы второй и четвёртый компоненты стали истинными, остаются следующие два варианта: $y = v$ и $y \neq v \,\&\, x = v \,\&\, y = u$. В обоих этих случаях G будет истинно. Аналогичным образом проводятся рассуждения от $x = v$, $y = u$ и $y = v$.

4. Понятия синглетона $\{x\}$ и неупорядоченной пары $\{x, y\}$ обобщаются на произвольное конечное количество n элементов

с помощью следующего рекурсивного определения:

$$\{x_1, \dots x_n\} \rightleftharpoons \bigcup\{\{x_1, \dots x_{n-1}\}, \{x_n\}\},$$

откуда

$$\{x_1, \dots x_n\} = \{z \mid z = x_1 \vee \dots \vee z = x_n\}.$$

Конструкция $\{x_1, \dots x_n\}$ называется *неупорядоченной n-кой*, или *n-элементным множеством, заданным перечислением*. С её помощью на основании аксиомы фундирования легко доказывается следующая теорема.

Теорема 33. *Не существует*

- *множества x, такого, что $x \in x$,*
- *множеств x, y, таких, что $x \in y \,\&\, y \in x$, и вообще любого набора множеств $x_1, \dots x_n$, «закольцованного» по отношению принадлежности условием $x_1 \in x_2 \,\&\, \dots \,\&\, x_{n-1} \in x_n \,\&\, \& \, x_n \in x_1$.*

$\lhd$Предположим, что такие $x_1, \dots x_n$ существуют. В этом случае существует и множество $\{x_1, \dots x_n\}$. Легко убедиться (см. с. 87), что существование $\{x_1, \dots x_n\}$ противоречит аксиоме фундирования — следовательно, исходное предположение неверно.$\rhd$

Следствие. *Не существует множества всех множеств, т. е.*

$$\neg\exists v \forall x \; x \in v.$$

$\lhd$Если бы такое множество существовало, то, очевидно, было бы $v \in v$.$\rhd$

Этот важный результат можно получить и без использования аксиомы фундирования, см. далее обсуждение теоремы 40.

Упр. 43. Докажите, что не существует 1) x такого, что $\{x\} \in x$, 2) x такого, что $\{x\} \in \bigcup x$.

5. Введём операции объединения, пересечения, дополнения и симметрической разности множеств, связанные с двухместными логическими операциями.

- Объединение множеств: $x \cup y \rightleftharpoons \bigcup\{x, y\}$.

Упрощая определение, имеем $x \cup y = \{z \mid \exists v(z \in v \,\&\, v \in \{t \mid t = x \vee t = y\})\} = \{z \mid \exists v(z \in v \,\&\, (v = x \vee v = y))\} = \{z \mid \exists v(z \in x \vee z \in y)\} = \{z \mid (z \in x \vee z \in y)\}$. Таким образом, объединение x и y представляет из себя множество, каждый элемент которого содержится хотя бы в одном из множеств x, y.

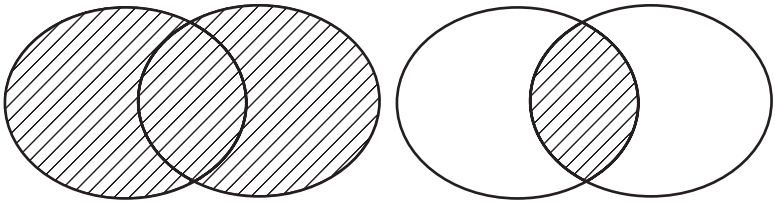


Рис. 2.1. Объединение и пересечение двух множеств

Используя теперь объединение в качестве ограничивающего множества t в терме $\{z \in t \mid A\}$, мы можем ввести следующие операции:

- пересечение (множество из элементов, принадлежащих одновременно x и y) $x \cap y \rightleftharpoons \{z \in x \cup y \mid z \in x \,\&\, z \in y\}$,
- дополнение $x \setminus y \rightleftharpoons \{z \in x \cup y \mid z \in x \,\&\, z \notin y\}$,
- симметрическая разность $x \triangle y \rightleftharpoons \{z \in x \cup y \mid z \in x \oplus z \in y\}$.

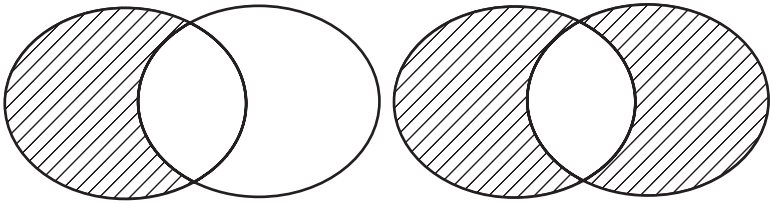


Рис. 2.2. Дополнение и симметрическая разность двух множеств

Ограничивающее условие $z \in x \cup y$ во всех этих трёх случаях можно убрать, т. к. из формул, стоящих справа от вертикальной черты, следует $z \in x \vee z \in y$, что эквивалентно ограничивающему условию.

6. Если формула A, построенная на атомарных подформулах вида $z \in x_1, \ldots z \in x_n$, не содержит кванторов, то определить, является ли она коллективизирующей, можно с помощью простого критерия, а термы вида $\{z \mid A\}$ составляют удобный для изучения класс.

Теорема 34. *Если даны множества $x_1, \ldots x_n$, то не содержащая кванторов формула A, построенная на атомарных подформулах $z \in x_1, \ldots z \in x_n$, будет являться коллективизирующей по z, если и только если*

$$\vdash A \Rightarrow z \in x_1 \vee \ldots \vee z \in x_n.$$

В терминах булевых функций данное требование означает, что функция, задаваемая формулой A, должна принимать значение $\mathfrak{f}$ в случае, когда все её элементарные подформулы принимают значение $\mathfrak{f}$. Такие булевы функции называются *сохраняющими нуль*.

$\lhd$В одну сторону: из условия следует, что

$$A \sim z \in x_1 \vee \ldots \vee z \in x_n \,\&\, A.$$

Это позволяет применить ограниченное выделение и построить множество $\{z \in x_1 \cup \ldots \cup x_n \mid A\}$, равное $\{z \mid A\}$.

В обратную сторону: если условие не выполняется, то подстановка в формулу A пустого множества вместо $x_1, \ldots x_n$ должна давать тождественно истинную относительно z формулу (эквивалентную, например, $z = z$). Получающийся при этом терм $v = \{z \mid z = z\}$ подразумевает существование множества всех множеств, что противоречит следствию теоремы 33.$\rhd$

Легко убедиться, что всего существует 2^{2^n-1} не равных между собой сохраняющих нуль булевых функций n аргументов и, как следствие, столько же не равных между собой термов рассматриваемого вида.

Теорема 35. *Любой терм вида* $\{z \mid A\}$, *где* A — *бескванторная формула, построенная на атомарных подформулах* $z \in x_1, \ldots z \in x_n$, *может быть представлен в виде суперпозиции операций пересечения и симметрической разности над множествами* $x_1, \ldots x_n$.

$\lhd$В силу теоремы 34 формула A задаёт сохраняющую нуль булеву функцию n аргументов. Представим формулу A в виде эквивалентного ей полинома Жегалкина (см. теорему 2). Т. к. A сохраняет нуль, «свободный член» ε_0 соответствующего полинома должен быть равен $\mathfrak{f}$ — иначе полином принимал бы значение $\mathfrak{t}$ в момент, когда все его аргументы равны $\mathfrak{f}$. Таким образом, A может быть представлена в виде суперпозиции одних только операций $\&$ и $\oplus$ над формулами $z \in x_1, \ldots z \in x_n$. Заменив в этом представлении формулы $z \in x_i$ на x_i, знаки $\&$ на $\cap$ и $\oplus$ на $\triangle$, получим искомое представление для терма $\{z \mid A\}$.$\rhd$

Таким образом, по аналогии с базисами логических операций, пара операций $\cap$ и $\triangle$ образует базис в классе термов, построенных с помощью бескванторных формул от $z \in x_1, \ldots z \in x_n$. Естественно, мы можем выбрать в качестве базисного и другой набор операций, коль скоро из него выражаются пересечение и симметрическая разность. Чаще всего за основу берут набор из трёх операций $\cup$, $\cap$ и $\setminus$, имея в виду, что $x \triangle y = (x \cup y) \setminus (x \cap y)$ (проверьте).

Некоторые свойства операций $\cup$, $\cap$ и $\setminus$:

$x \cap x = x$,
$x \cup x = x$,
$x \setminus x = \varnothing$,
$x \cap y = y \cap x$,
$x \cup y = y \cup x$ (коммутативность),
$(x \cap y) \cap z = x \cap (y \cap z)$,
$(x \cup y) \cup z = x \cup (y \cup z)$ (ассоциативность),
$x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$,
$x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$,
$(x \cup y) \setminus z = (x \setminus z) \cup (y \setminus z)$ (дистрибутивность),
$z \setminus (x \cap y) = (z \setminus x) \cup (z \setminus y)$,

$$z \setminus (x \cup y) = (z \setminus x) \cap (z \setminus y),$$
$$z \setminus (y \setminus x) = (x \cap z) \cup (z \setminus y),$$
$$(y \setminus x) \cap z = (y \cap z) \setminus x = y \cap (z \setminus x),$$
$$(y \setminus x) \cup z = (y \cup z) \setminus (x \setminus z),$$
$$x \cap \varnothing = \varnothing, \quad x \cup \varnothing = x,$$
$$\varnothing \setminus x = \varnothing, \quad x \setminus \varnothing = x.$$

Чтобы доказать любое из этих равенств, нужно, как обычно, проверить эквивалентность образующих соответствующие термы формул. Т. к. эти формулы бескванторные, задача упрощается, поскольку для изучения свойств бескванторных формул можно применять таблицы Куайна. Однако бóльшую наглядность при решении подобных задач дают широко известные диаграммы Эйлера–Венна, на которых множества изображаются в виде пересекающихся замкнутых фигур.

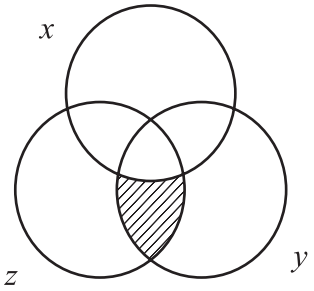


Рис. 2.3. Диаграмма Эйлера, терм $(y \setminus x) \cap z$

Диаграммы Эйлера–Венна для двух и трёх множеств показаны на рис. 2.1–2.3. Диаграмма для n множеств содержит $2^n - 1$ областей пересечения. Закрашивая штриховкой выборки из этих областей, можно проиллюстрировать любой из 2^{2^n-1} термов, образуемых бескванторными формулами над $z \in x_1, \ldots z \in x_n$. На рис. 2.3 штриховкой показан терм $(y \setminus x) \cap z$, равный $(y \cap z) \setminus x$ и $y \cap (z \setminus x)$.

В XX в. Энтони Эдвардсом был предложен изящный способ построения диаграмм Эйлера–Венна для произвольного числа мно-

жеств. Диаграммы Эдвардса для случая двух, трёх, четырёх и пяти множеств показаны на рис. 2.4.

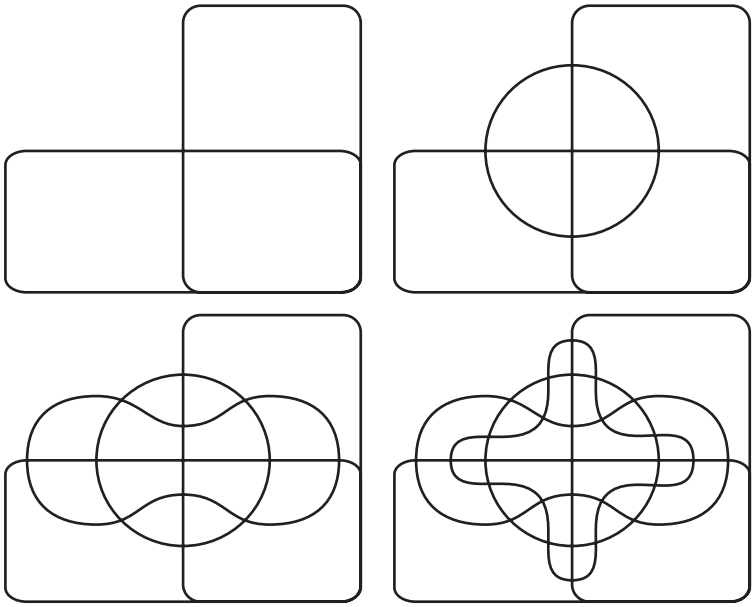


Рис. 2.4. Диаграммы Эдвардса

Упр. 44. Докажите, что любая формула, построенная над множествами $x, x_1, \ldots x_n$ с помощью операций $\cup$, $\cap$, $\triangle$ и $\setminus$, может быть представлена в виде

$$a \triangle (e_1 \cap x) \triangle (e_2 \cap b \cap x),$$

где выражения для a и b не содержат x, а e_1 и e_2 равны либо x, либо $\varnothing$.

Упр. 45. [2]. Докажите, что

$$(x_1 \cap \ldots \cap x_n) \triangle (y_1 \cap \ldots \cap y_n) \subseteq (x_1 \triangle y_1) \cup \ldots \cup (x_n \triangle y_n),$$
$$(x_1 \cup \ldots \cup x_n) \triangle (y_1 \cup \ldots \cup y_n) \subseteq (x_1 \triangle y_1) \cup \ldots \cup (x_n \triangle y_n).$$

Указание: воспользуйтесь индукцией по числу множеств. Для доказательства базы индукции можно воспользоваться диаграммами для четырёх множеств x_1, x_2, y_1, y_2 (см. рис. 2.5 и 2.6).

Упр. 46. Докажите, что в теории ZF $x \cup \{x\} = y \cup \{y\} \sim x = y$.

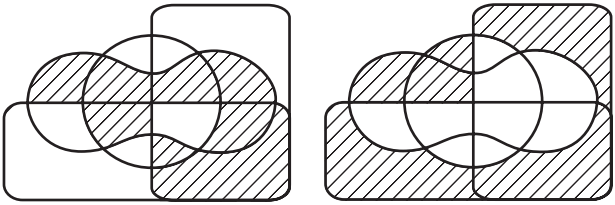


Рис. 2.5. $(x_1 \cap x_2) \triangle (y_1 \cap y_2)$ и $(x_1 \cup x_2) \triangle (y_1 \cup y_2)$

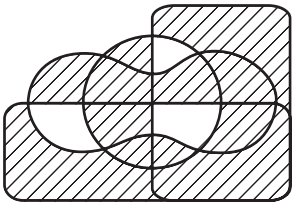


Рис. 2.6. $(x_1 \triangle y_1) \cup (x_2 \triangle y_2)$

Решение. Утверждение $x = y \Rightarrow x \cup \{x\} = y \cup \{y\}$ следует из свойств равенства. Докажем обратное утверждение от противного: пусть $x \cup \{x\} = y \cup \{y\}$, но при этом $x \neq y$. Без ограничения общности можем считать, что существует такой t, что $t \in x$ и $t \notin y$. Отсюда $t \in x \Rightarrow t \in \in x \cup \{x\} \Rightarrow t \in y \cup \{y\} \Rightarrow t \in y \vee t = y$. Из этого и $t \notin y$ следует, что $t = y$ и $y \in x$. Но с другой стороны, $x \in x \cup \{x\} \Rightarrow x \in y \cup \{y\} \Rightarrow x \in y \vee x = y$. В первом случае имеем $y \in x \in y$, во втором — $y \in y$, и оба варианта противоречат аксиоме фундирования (см. теорему 33), значит, $x \neq y$ не имеет места.

7. Легко убедиться, что $\{x, y\} = \{y, x\}$, т. е. в неупорядоченной паре порядок следования элементов не имеет значения. Между тем для дальнейшего нам потребуется объединять пары множеств в конструкцию, в которой различаются *первый* и *второй* компоненты. Иначе говоря, нужен способ построения из x и y такой конструкции (x, y), что

$$(x, y) = (u, v) \sim (x = u) \,\&\, (y = v).$$

При построении теории множеств можно считать упорядочен-

ную пару таким же основным, невыводимым понятием, как и множество, а указанное свойство — аксиомой упорядоченной пары. Но можно и избежать этого, если воспользоваться одним из приёмов введения упорядоченной пары с помощью множеств:

- Упорядоченная пара (по Куратóвскому):

$$(x, y) \rightleftharpoons \{\{x\}, \{x, y\}\}.$$

Основное свойство упорядоченной пары:

$$(x, y) = (u, v) \Leftrightarrow (x = u)\ \&\ (y = v).$$

Справа налево это утверждение следует из свойств равенства.

Слева направо: пусть $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. В силу доказанного выше третьего свойства неупорядоченной пары

$$(\{x\} = \{u\}\ \&\ \{x, y\} = \{u, v\}) \vee (\{x\} = \{u, v\}\ \&\ \{x, y\} = \{u\}).$$

Докажем разбором случаев, что из этого следует то, что требуется доказать.

Первый случай: $\{x\} = \{u\}\ \&\ \{x, y\} = \{u, v\}$. Из первой компоненты конъюнкции следует, что $x = u$. Из второй следует $(x = u\ \&\ y = v) \vee (x = v\ \&\ y = u)$, и нам требуется вывести от этого импликацию к $y = v$. Вновь используем разбор случаев: первая компонента этой дизъюнкции уже содержит то, что нам требуется доказать, конъюнкция правой части с $x = u$ даёт

$$x = v\ \&\ y = u\ \&\ x = u \Rightarrow u = v\ \&\ y = v.$$

Второй случай: $\{x\} = \{u, v\}\ \&\ \{x, y\} = \{u\}$. В силу доказанного выше четвёртого свойства неупорядоченной пары следует, что $x = u\ \&\ x = v\ \&\ y = u$, т. е. все переменные равны между собой, и отсюда же — $(x = u)\ \&\ (y = v)$.

Упр. 47. [7]. Докажите аналогичное утверждение для упорядоченной пары по Винеру: $(x, y) \rightleftharpoons \{\{\varnothing, \{x\}\}, \{\{y\}\}\}$.

Упр. 48. Докажите, что понятие упорядоченной пары можно ввести и так: $(x, y) \rightleftharpoons \{x, \{x, y\}\}$, но в этом случае для доказательства основного свойства надо ссылаться на аксиому фундирования.

Понятие упорядоченной пары обобщается на произвольное конечное количество n элементов с помощью следующего рекурсивного определения:

$$(x_1, \ldots x_n) \rightleftharpoons ((x_1, \ldots x_{n-1}), x_n).$$

Конструкция $(x_1, \ldots x_n)$ называется *упорядоченной n-кой*, или *кортежем*, а $x_1, \ldots x_n$ — *компонентами* кортежа $(x_1, \ldots x_n)$.

8. Множество всех возможных упорядоченных пар (u, v), где $u \in x$, а $v \in y$, называется *прямым*, или *декартовым произведением множеств x и y* и обозначается $x \times y$. Пользуясь определением упорядоченной пары по Куратовскому, мы можем формально записать, что

$$x \times y \rightleftharpoons \{z \in \mathfrak{PP}(x \cup y) \mid \exists u \exists v (u \in x \,\&\, v \in y \,\&\, z = (u, v))\}.$$

Т. к. $\exists u \exists v (u \in x \,\&\, v \in y \,\&\, z = (u, v)) \Rightarrow z \in \mathfrak{PP}(x \cup y)$, ограничивающее условие $z \in \mathfrak{PP}(x \cup y)$ можно убрать из определения.

Пример декартова произведения: если a, b, c, d, e — различные между собой элементы, то $\{a, b, c\} \times \{d, e\} = \{(a, d), (a, e), (b, d), (b, e), (c, d), (c, e)\}$.

Декартову произведению множеств не свойственны коммутативность и ассоциативность (в силу того, что эти свойства отсутствуют у упорядоченных пар, составляющих декартово произведение), но свойственна дистрибутивность относительно операций $\cup$, $\cap$, $\setminus$ и $\triangle$. Например,

$$(x \cup y) \times z = (x \times z) \cup (y \times z),$$
$$x \times (y \cup z) = (x \times y) \cup (x \times z).$$

Докажем первое. $t \in (x \cup y) \times z \sim \exists u \exists v (u \in (x \cup y) \,\&\, v \in z \,\&\, t = (u, v)) \sim \exists u \exists v ((u \in x \vee u \in y) \,\&\, v \in z \,\&\, t = (u, v)) \sim \exists u \exists v ((u \in x \,\&\, v \in z \,\&\, t = (u, v)) \vee (u \in y \,\&\, v \in z \,\&\, t = (u, v))) \sim t \in (x \times z) \cup (y \times z)$.

Аналогичные свойства дистрибутивности доказываются для операций $\cap$, $\setminus$ и $\triangle$.

Упр. 49. [2]. Докажите, что

$$x \times \varnothing = \varnothing \times x = \varnothing,$$
$$x \subseteq u \,\&\, y \subseteq v \sim x \times y \subseteq u \times v,$$
$$x = u \,\&\, y = v \sim x \times y = u \times v,$$
$$(x \cap y) \times (u \cap v) = (x \times u) \cap (y \times v).$$

9. Рассмотрим операции, являющиеся в некотором смысле обратными к операциям образования упорядоченной пары и декартова произведения. Если в качестве определения упорядоченной пары используется упорядоченная пара по Куратовскому, то

- первая и вторая малые проекции:

$$\mathrm{pr}_1(x) \rightleftharpoons \bigcup\{u \in \bigcup x \mid \exists v\ (u, v) = x\},$$
$$\mathrm{pr}_2(x) \rightleftharpoons \bigcup\{v \in \bigcup x \mid \exists u\ (u, v) = x\},$$

- первая и вторая большие проекции:

$$\mathrm{Pr}_1(x) \rightleftharpoons \{u \in \bigcup\bigcup x \mid \exists v\ (u, v) \in x\},$$
$$\mathrm{Pr}_2(x) \rightleftharpoons \{v \in \bigcup\bigcup x \mid \exists u\ (u, v) \in x\}.$$

Основными свойствами проекций, как нетрудно проверить, являются

$$\mathrm{pr}_1((u, v)) = u, \quad \mathrm{pr}_2((u, v)) = v,$$
$$\mathrm{Pr}_1(x \times y) = x, \quad \mathrm{Pr}_2(x \times y) = y,$$
$$r \subseteq x \times y \Rightarrow \mathrm{Pr}_1(r) \subseteq x,$$
$$r \subseteq x \times y \Rightarrow \mathrm{Pr}_2(r) \subseteq y.$$

Для понятий большой и малой проекции имеется наглядная геометрическая интерпретация. Пусть x — множество всех точек оси абсцисс, y — множество всех точек оси ординат. Тогда декартово произведение $x \times y$ является всей координатной плоскостью, элемент $u \in x \times y$ (который есть упорядоченная пара) — точкой

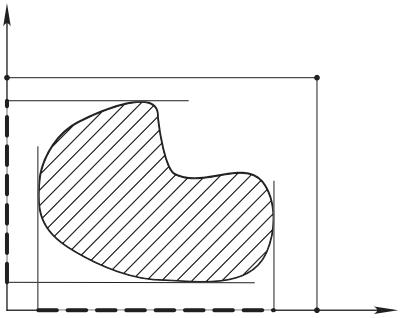


Рис. 2.7. Большая и малая проекции

на плоскости, а множество $v \subseteq x \times y$ (множество пар) — фигурой на этой плоскости. Первая малая проекция является операцией, ставящей в соответствие точке её абсциссу, а первая большая проекция ставит в соответствие области множество абсцисс точек, составляющих область (см. рис. 2.7).

§ 2.3. Натуральные числа

1. В этом параграфе мы применим до сих пор нигде не использованную нами аксиому бесконечности для того, чтобы построить терм, который в дальнейшем будет отождествляться со множеством натуральных чисел.

Теорема 36. *Существует единственное множество ω, удовлетворяющее следующим условиям:*

1) $\varnothing \in \omega$,

2) $\forall x(x \in \omega \Rightarrow x \cup \{x\} \in \omega)$,

3) $\forall x(x \in \omega \Rightarrow (x \neq \varnothing \Rightarrow \exists y(y \in \omega \,\&\, x = y \cup \{y\})))$.

$\lhd$Назовём множества, удовлетворяющие условиям 1 и 2, *прогрессивными* и обозначим формулу $\varnothing \in u \& \forall x(x \in u \Rightarrow x \cup \{x\} \in u)$

через $\mathrm{Prog}(u)$. Аксиома бесконечности, будучи переписана с использованием доступных нам теперь сокращающих обозначений, гласит, что $\exists u\,\mathrm{Prog}(u)$. В качестве ω мы хотим взять такое множество, каждый элемент которого входит во все другие прогрессивные множества. Комбинируя аксиомы бесконечности и ограниченного выделения, имеем

$$\mathrm{ZF} \vdash \exists x(\mathrm{Prog}(x)\ \&\ \exists\omega\forall z(z \in \omega \Leftrightarrow z \in x\ \&\ \forall y(\mathrm{Prog}(y) \Rightarrow z \in y))).$$

Но $\forall y(\mathrm{Prog}(y) \Rightarrow z \in y) \Rightarrow (\mathrm{Prog}(x) \Rightarrow z \in x)$, в результате чего получаем возможность убрать ограничивающее условие $z \in x$ и прийти к

$$\mathrm{ZF} \vdash \exists\omega\forall z(z \in \omega \Leftrightarrow \forall y(\mathrm{Prog}(y) \Rightarrow z \in y)).$$

В силу леммы 30 знак $\exists\omega$ в этом случае можно заменить на $\exists!\omega$, т. е. ω существует и единственно[2].

Осталось показать, что ω прогрессивно и удовлетворяет условию 3.

Используя теорему 32, имеем

$$\begin{aligned}\mathrm{Prog}(\omega) &\sim \varnothing \in \omega\ \&\ \forall t(t \in \omega \Rightarrow t \cup \{t\} \in \omega) \sim\\ &\sim \forall y(\mathrm{Prog}(y) \Rightarrow \varnothing \in y)\&\\ &\quad\&\forall t(\forall y(\mathrm{Prog}(y) \Rightarrow t \in y) \Rightarrow \forall y(\mathrm{Prog}(y) \Rightarrow t \cup \{t\} \in y)).\end{aligned}$$

Первая часть конъюнкции прямо выводима из $\mathrm{Prog}(y)$. Выведем вторую часть.

В силу тавтологии, получаемой из второй схемы аксиом исчисления высказываний,

$$\begin{aligned}\vdash\ &(\mathrm{Prog}(y) \Rightarrow (t \in y \Rightarrow t \cup \{t\} \in y)) \Rightarrow\\ &\Rightarrow ((\mathrm{Prog}(y) \Rightarrow t \in y) \Rightarrow (\mathrm{Prog}(y) \Rightarrow t \cup \{t\} \in y)),\end{aligned}$$

[2] Заметим, что для доказательства этого утверждения не понадобились свойства формулы $\mathrm{Prog}(x)$, что позволяет для любой зависящей от x формулы A утверждать существование множества $\{z \mid \forall x(A \Rightarrow z \in x)\}$ в случае, когда $\exists x A$.

откуда последовательно получаем

$$\vdash (\mathrm{Prog}(y) \Rightarrow t \in y) \Rightarrow (\mathrm{Prog}(y) \Rightarrow t \cup \{t\} \in y)$$

и

$$\vdash \forall y(\mathrm{Prog}(y) \Rightarrow t \in y) \Rightarrow \forall y(\mathrm{Prog}(y) \Rightarrow t \cup \{t\} \in y),$$

в силу чего окончательно $\vdash \mathrm{Prog}(\omega)$.

Докажем, что ω удовлетворяет условию 3.

Выделим множество

$$\omega' = \{x \in \omega \mid x \neq \varnothing \Rightarrow \exists y(y \in \omega \,\&\, x = y \cup \{y\})\}.$$

Ясно, что $\omega' \subseteq \omega$. Докажем $\mathrm{Prog}(\omega')$ таким же образом, как мы только что проделали это для ω:

$$\begin{aligned}\mathrm{Prog}(\omega') \sim \varnothing \in \omega' \,\&\, \forall t(t \in \omega' \Rightarrow t \cup \{t\} \in \omega') \sim \\ \sim (\varnothing \neq \varnothing \Rightarrow \exists y(y \in \omega \,\&\, \varnothing = y \cup \{y\}))\& \\ \&\forall t((t \neq \varnothing \Rightarrow \exists y(y \in \omega \,\&\, t = y \cup \{y\})) \Rightarrow \\ \Rightarrow (t \cup \{t\} \neq \varnothing \Rightarrow \exists y(y \in \omega \,\&\, t \cup \{t\} = y \cup \{y\}))).\end{aligned}$$

В силу того, что $\neg\varnothing \neq \varnothing$, $t \cup \{t\} \neq \varnothing$, $\exists y(y \in \omega \,\&\, t \cup \{t\} = y \cup \{y\}) \sim t \in \omega$ (см. упр. 46),

$$\mathrm{Prog}(\omega') \sim \forall t((t \neq \varnothing \Rightarrow \exists y(y \in \omega \,\&\, t = y \cup \{y\})) \Rightarrow t \in \omega).$$

В силу тавтологии $(A \Rightarrow B) \Rightarrow C \sim (A \Rightarrow (B \Rightarrow C)) \,\&\, (\neg A \Rightarrow C)$ выражение, замкнутое квантором $\forall t$, эквивалентно $(t \neq \varnothing \Rightarrow (\exists y(y \in \omega \,\&\, t = y \cup \{y\}) \Rightarrow t \in \omega)) \,\&\, (t = \varnothing \Rightarrow t \in \omega)$.

Но $\exists y(y \in \omega \,\&\, t = y \cup \{y\}) \Rightarrow \exists y(y \cup \{y\} \in \omega \,\&\, t = y \cup \{y\})$, откуда $\exists y(y \in \omega \,\&\, t = y \cup \{y\}) \Rightarrow t \in \omega$, а вторая часть конъюнкции (утверждение $t = \varnothing \Rightarrow t \in \omega$) следует из $\varnothing \in \omega$.

Таким образом, $\vdash \mathrm{Prog}(\omega')$. Но $\vdash \mathrm{Prog}(\omega') \Rightarrow \omega \subseteq \omega'$, т. к. ω по определению — «минимальное» прогрессивное множество. Значит, $\omega' \subseteq \omega$ и $\omega \subseteq \omega'$, откуда $\omega = \omega'$ и условие 3 выполняется для всех элементов ω.▷

2. Множество ω мы будем называть множеством натуральных чисел (по фон Нейману). Примем, кроме того, следующие обозна-

чения для термов, являющихся элементами ω:

$$\begin{aligned}
&\varnothing \rightleftharpoons 0,\\
&\{\varnothing\} = \{0\} \rightleftharpoons 1,\\
&\{\varnothing, \{\varnothing\}\} = \{0, 1\} \rightleftharpoons 2,\\
&\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\} \rightleftharpoons 3,\\
&\ldots\\
&x \cup \{x\} \rightleftharpoons x + 1.
\end{aligned}$$

Теорема 37. *Множество ω удовлетворяет аксиомам Пеано для натуральных чисел:*

1) $0 \in \omega$ — *нуль является натуральным числом,*

2) $x \in \omega \Rightarrow x + 1 \in \omega$ — *число, следующее за натуральным, также является натуральным числом,*

3) $\neg\exists x(x \in \omega \,\&\, x + 1 = 0)$ — *нуль не следует ни за каким натуральным числом,*

4) $\forall x \forall y(x + 1 = y + 1 \Rightarrow x = y)$ — *всякое натуральное число следует только за одним натуральным числом,*

5) $(0 \mid x)A \,\&\, \forall x(x \in \omega \Rightarrow (A \Rightarrow (x + 1 \mid x)A)) \Rightarrow \forall x(x \in \omega \Rightarrow A)$ — *аксиома индукции: если зависящая от натурального числа формула истинна для нуля, а также для всякого числа, следующего за тем, для которого эта формула истинна, то формула истинна для всех натуральных чисел.*

$\lhd$Утверждения 1–3 тривиально следуют из определений и уже доказанных теоремой 36 свойств, утверждение 4 есть следствие упражнения 46. Для доказательства утверждения 5 достаточно построить терм $\{x \in \omega \mid A\}$ и убедиться в том, что он является прогрессивным множеством в предположении

$$(0 \mid x)A \,\&\, \forall x(x \in \omega \Rightarrow (A \Rightarrow (x + 1 \mid x)A)).\rhd$$

Если x и y — элементы множества ω (т. е., иначе говоря, натуральные числа), то вместо $x \in y$ пишут $x < y$, вместо $x \in y + 1$ — $x \leqslant y$.

Если $u \subseteq \omega$, то элемент x называется *наибольшим в* u (и пишется $x = \sup(u)$), если $x \in u \,\&\, \forall y(y \in u \Rightarrow y \leqslant x)$, и *наименьшим в* u (и пишется $x = \inf(u)$), если $x \in u \,\&\, \forall y(y \in u \Rightarrow x \leqslant y)$.

В общем случае при рассмотрении подмножеств упорядоченных множеств $\sup(u)$ и $\inf(u)$ не есть наибольший и наименьший элементы (см. далее определения, даваемые в § 2.6). Применительно к натуральным числам, однако, понятия «x есть $\sup(u)$» и «x есть наибольший элемент u» совпадают (аналогично inf и «наименьший элемент»), поэтому при рассмотрении подмножеств натуральных чисел удобные обозначения sup и inf будут часто использоваться.

Упр. 50. Докажите, что для любых натуральных чисел m и n выполняется $m < n \Rightarrow m \subset n$. Указание: воспользуйтесь аксиомой индукции, доказанной в теореме 37.

Упр. 51. Докажите, что любое непустое подмножество ω содержит единственный наименьший элемент.

Частичное решение. Предположим, что наименьшего элемента не существует, т. е. $\neg\exists x(x \in u \,\&\, \forall n(n \in u \Rightarrow x \leqslant n))$, что эквивалентно

$$\forall x(x \notin u \vee \neg\forall n(n \in u \Rightarrow x \leqslant n)).$$

Но $\forall n\ 0 \leqslant n$, откуда

$$0 \notin u \,\&\, \forall n(n \in u \Rightarrow 0 \leqslant n).$$

Пусть для некоторого m выполняется $m \notin u \,\&\, \forall n(n \in u \Rightarrow m \leqslant n)$. Тогда $\forall n(n \in u \Rightarrow m < n)$, и

$$\begin{gathered} m + 1 \notin u \vee \neg\forall n(n \in u \Rightarrow m + 1 \leqslant n) \sim \\ \sim m + 1 \notin u \vee \neg\forall n(n \in u \Rightarrow m < n), \end{gathered}$$

из чего следует $m + 1 \notin u$. Но тогда, в силу аксиомы индукции, $\forall n(n \in \in \omega \Rightarrow n \notin u)$, что противоречит исходному предположению о том, что u — непустое.

Заметим также, что этот же результат мы могли бы получить напрямую из аксиомы фундирования.

Упр. 52. Докажите, что любое непустое ограниченное сверху подмножество натуральных чисел (т. е. такое u, что $u \subseteq \omega \,\&\, \exists m \forall n(n \in u \Rightarrow n < m)$) имеет наибольший элемент.

Упр. 53. Пусть $u \subseteq \omega$. Докажите, что если u — непустое множество, то терм $\bigcap u$ есть его наименьший элемент.

Частичное решение. Пусть $u_{\leqslant}(t) = \{x \in u \mid x \leqslant t\}$, $u_{>}(t) = \{x \in u \mid t < x\}$. Тогда

$$\forall n(n \in u_{\leqslant}(t) \Rightarrow \forall m(m \in u_{>}(t) \Rightarrow n \in m)),$$

откуда

$$\bigcap u = \bigcap (u_{\leqslant}(t) \cup u_{>}(t)) = \bigcap u_{\leqslant}(t)$$

для любого $t \in u$.

По доказанному в упр. 51 и только что,

$$\begin{aligned} &\exists t(t = \inf(u) \,\&\, \textstyle\bigcap u = \bigcap u_{\leqslant}(t)) \sim \\ &\quad \sim \exists t(t = \inf(u) \,\&\, \textstyle\bigcap u = \{x \in \omega \mid \forall n(n \in u_{\leqslant}(t) \Rightarrow x \in n)\}). \end{aligned}$$

Но $n \in u_{\leqslant}(t) \sim n \in u \,\&\, n \leqslant t$, а в силу $t = \inf(u)$, $n \in u_{\leqslant}(t) \Rightarrow n = t$ и

$$\exists t(t = \inf(u) \,\&\, \textstyle\bigcap u = \{x \in \omega \mid x \in t\}).$$

По доказанному в упр. 50, $\{x \in \omega \mid x \in t\} = t$, откуда $\inf(u) = \bigcap u$.

Упр. 54. Пусть $u \subseteq \omega$. Докажите, что если наибольший элемент в u существует, то он равен $\bigcup u$.

3. Множество натуральных чисел, индукция и схема аксиом подстановки позволяют доказывать существование множеств, удовлетворяющих некоторым рекурсивным условиям на свои элементы, чем мы в дальнейшем намерены активно пользоваться.

Наметим идею в общих чертах. Предположим, что даны терм x_0 и способ, позволяющий из произвольного терма x_n однозначным образом получать терм x_{n+1} (один такой способ нам уже хорошо известен — это $x_n \cup \{x_n\}$). Тогда существует единственное множество вида

$$\{x_0, x_1, \ldots x_n, \ldots\},$$

каждый последующий элемент которого рекурсивно получается из предыдущего. Формальное определение и доказательство этого факта устанавливает следующая теорема.

Теорема 38 (о рекурсии). *Пусть даны терм x_0 и формула A, такая, что $\forall x \exists! y A$. Тогда существует единственное f, такое, что*

1) $\forall p(p \in f \Rightarrow \exists n \exists x(n \in \omega \,\&\, (n,x) = p))$ — *f является множеством пар, первая компонента каждой из которых — натуральное число,*

2) $\forall n(n \in \omega \Rightarrow \exists! x_n (n, x_n) \in f)$ — *для каждого натурального числа определён единственный элемент, входящий с ним в пару,*

3) $(0, x_0) \in f \& \forall n \forall x((n,x) \in f \Rightarrow \exists! y(A \& (n+1, y) \in f))$ — *первый элемент последовательности задан явно, а каждый следующий может быть рекурсивным образом получен из предыдущего.*

$\lhd$Построим формулу F со свободными переменными n и f_n, выражающую тот факт, что множество f_n является начальным отрезком рекурсивно построенной последовательности, получающимся после n шагов рекурсии:

$$\begin{aligned} F(n, f_n) \rightleftharpoons\ & \forall p(p \in f_n \Rightarrow \exists k \exists x(k \leqslant n \,\&\, (k,x) = p)) \& \\ & \&\forall k(k \leqslant n \Rightarrow \exists! x_k (k, x_k) \in f_n) \& \\ & \&(0, x_0) \in f_n \,\&\, \forall k \forall x(k \leqslant n \,\&\, (k,x) \in f_n \Rightarrow \\ & \quad \Rightarrow \exists! y(A \,\&\, (k+1, y) \in f_n)). \end{aligned}$$

Единственное множество $f_0 = \{(0, x_0)\}$ удовлетворяет этой формуле при $n = 0$, единственное множество $f_1 = \{(0, x_0), (1, x_1)\}$, где $(x_0 \mid x)(x_1 \mid y)A$, удовлетворяет этой формуле при $n = 1$ и т. д.

Таким образом, для всякого *заранее заданного* n мы можем вывести существование и единственность терма f_n, повторив процесс

доказательства нужное количество шагов. Существование бесконечного количества термов f_n само по себе не даёт нам права объединить их *все* в одно множество. Однако индукция и схема аксиом подстановки позволят нам это сделать.

Можно проверить, что условие $F(n, f_n)$ обладает следующими свойствами:

$$\exists! f_0 F(0, f_0),$$
$$\exists! f_n F(n, f_n) \Rightarrow \exists! f_{n+1} F(n+1, f_{n+1}),$$

откуда по индукции имеем

$$\forall n (n \in \omega \Rightarrow \exists! f_n F(n, f_n)).$$

Напомним, что схема аксиом подстановки формулируется следующим образом:

$$\forall v \exists! u \forall z (z \in u \Leftrightarrow \exists x (x \in v \,\&\, A \,\&\, \exists! z A)).$$

Подставив в качестве v множество ω, а в качестве A — формулу $F(n, f_n)$, имеем существование терма

$$u = \{f_n \mid \exists n (n \in \omega \,\&\, F(n, f_n))\}.$$

Терм $\bigcup u$, как нетрудно проверить, удовлетворяет всем трём условиям теоремы.

Докажем единственность. Пусть f' также удовлетворяет условиям теоремы. Тогда $(0, x_0) \in f'$ и $((n, x_n) \in f \Rightarrow (n, x_n) \in f') \Rightarrow$ $\Rightarrow ((n+1, x_{n+1}) \in f \Rightarrow (n+1, x_{n+1}) \in f')$, откуда $f \subseteq f'$. Если $f' \neq$ $\neq f$, то f' может быть только надмножеством f — но последнее невозможно в силу однозначности x_n, входящего в пару с каждым n.$\triangleright$

Использование рекурсии открывает новые возможности для построения операций над термами. Возьмём, например, в качестве x_0 некоторое v, а в качестве формулы A — условие $y = x \times v$. Пусть f — множество, существование и единственность которого обеспечивается в этом случае теоремой 38. Множество $\mathrm{Pr}_2(f) \cup \{\varnothing\}$ называется *звёздочкой Клини* для v и обозначается v^*. Можно сказать, что

$v^* = \{\varnothing\} \cup v \cup (v \times v) \cup (v \times v \times v) \cup \ldots$ и представляет собой множество всех конечных упорядоченных наборов элементов v. Если интерпретировать v как множество символов какого-либо алфавита (включая пробелы и знаки препинания), то v^* есть множество всех возможных строк конечной длины в этом алфавите. Если имеется язык, использующий v в качестве алфавита, то v^* будет являться надмножеством множества всех мыслимых текстов на этом языке.

4. С использованием рекурсии можно ввести операции над натуральными числами. Например, рассмотрим множество, элементы которого определены по следующему рекурсивному правилу:

$$x_0 = \{(x, y, z) \in \omega \times \omega \times \omega \mid x = z \,\&\, y = 0\},$$
$$x_{n+1} = \{(x, y, z) \in \omega \times \omega \times \omega \mid \exists x' \exists y' \exists z' ((x', y', z') \in x_n \,\&$$
$$\&x = x' \,\&\, y = y' + 1 \,\&\, z = z' + 1)\}.$$

Интуитивно понятно, что для каждого x_i, $(x, y, z) \in x_i$ эквивалентно условию $x + y = z$ — но в нашей формальной системе ещё не определена операция сложения натуральных чисел. Рассмотрим множество $s = \bigcup\{x_1, x_2, \ldots x_n, \ldots\}$ и будем говорить, что

$$x + y = z \rightleftharpoons (x, y, z) \in s.$$

Далее рассмотрим множество, элементы которого удовлетворяют условиям

$$x_0 = \{(x, y, z) \in \omega \times \omega \times \omega \mid y = 0 \,\&\, z = 0\},$$
$$x_{n+1} = \{(x, y, z) \in \omega \times \omega \times \omega \mid \exists x' \exists y' \exists z' ((x', y', z') \in x_n \,\&$$
$$\&x = x' \,\&\, y = y' + 1 \,\&\, z = z' + x')\}.$$

Пусть $p = \bigcup\{x_1, x_2, \ldots x_n, \ldots\}$. Ясно, что $xy = z \rightleftharpoons (x, y, z) \in p$.

Аналогичным образом можно получить и другие операции над натуральными числами — например, возведение в степень.

Упр. 55. Постройте множество f, такое, что $(x, y) \in f$ равносильно $x! = y$.

Только что полученные нами термы s, p удовлетворяют по построению аксиомам

$$x + 0 = x,$$
$$x + (y + 1) = (x + y) + 1,$$
$$x0 = 0,$$
$$x(y + 1) = xy + x.$$

Система из этих четырёх аксиом вкупе с аксиомами Пеано для натурального ряда, перечисленными в теореме 37, называется системой аксиом *формальной арифметики*.

5. Как будет показано далее, натуральные числа и множество ω являются представителями класса множеств, именуемых *ординалами*. Теоремами 51 и 57 о трансфинитной индукции и трансфинитной рекурсии математическая индукция и обычная рекурсия будут обобщены для произвольных представителей этого класса.

§ 2.4. Отображения. Сравнение множеств по мощности

1. Одной из характеристик множества в соответствии с интуитивным представлением должно являться количество входящих в него элементов. Эту характеристику называют *мощностью* множества. К примеру, если x, y, z не равны между собой, то мощность множества $\{x, y, z\}$ равна трём. Но для того, чтобы выражения типа «мощность x равна y» обрели строгий формальный смысл, необходимо понять, какие формулы на языке первого порядка аксиоматической теории множеств соответствуют этим выражениям. Ниже мы выполним формальные построения, которые позволят строго рассуждать о мощностях множеств в рамках системы ZFC и даже обобщить понятие мощности на множества, содержащие бесконечное количество элементов. Основополагающей конструкцией для этих построений служит *бинарное отношение*.

2. *Бинарным отношением на множествах x и y* называется такое r, что $r \subseteq x \times y$. Если $(a, b) \in r$ (необходимым, но не достаточным условием чего является $a \in x \,\&\, b \in y$), то говорят, что

элемент a *входит в отношение* r с элементом b. *Областью определения* отношения r называется множество $\mathrm{Pr}_1(r)$, *областью значений* — $\mathrm{Pr}_2(r)$. Частными случаями бинарных отношений являются *пустое отношение* $r = \varnothing$ и *полное отношение* $r = x \times y$.

Бинарное отношение r может обладать, а может и не обладать одним или несколькими из этих свойств:

1) *всюдуопределенность*: $\forall u(u \in x \Rightarrow \exists v((u, v) \in r))$ (каждый элемент первого множества входит в отношение хотя бы с одним из элементов второго множества);

2) *прямая однозначность*: $\forall u(u \in r \Rightarrow \forall v(v \in r \Rightarrow (\mathrm{pr}_1(u) = \mathrm{pr}_1(v) \Rightarrow u = v)))$ (каждый элемент первого множества входит в отношение не более чем с одним из элементов второго множества);

3) *всюдузначность*: $\forall v(v \in y \Rightarrow \exists u((u, v) \in r))$ (каждый элемент второго множества входит в отношение хотя бы с одним из элементов первого множества);

4) *обратная однозначность*: $\forall u(u \in r \Rightarrow \forall v(v \in r \Rightarrow (\mathrm{pr}_2(u) = \mathrm{pr}_2(v) \Rightarrow u = v)))$ (каждый элемент второго множества входит в отношение не более чем с одним из элементов первого множества).

Заметим, что условие всюдуопределённости можно записать как $\mathrm{Pr}_1(r) = x$, а всюдузначности — как $\mathrm{Pr}_2(r) = y$.

Указанные четыре свойства являются логически независимыми (невыводимыми друг из друга). Независимость можно доказать, предоставив шестнадцать примеров бинарных отношений, удовлетворяющих каждой комбинации этих свойств и их отрицаний. Например, если a, b, c, d, e — различные между собой элементы, то $\{(a, d), (b, d), (c, e)\}$ — пример всюдуопределенного, всюдузначного, прямооднозначного, но не обратнооднозначного отношения на множествах $\{a, b, c\}$ и $\{d, e\}$, $\{(a, d), (a, e)\}$ — пример всюдузнач-

ного, обратнооднозначного, но не всюдуопределённого и не прямооднозначного отношения на тех же множествах и т. п.

Упр. 56. Примером простейшего бинарного отношения для случая $x = y$ является тождественное отображение $\mathrm{id}_x = \{t \in x \times x \mid \mathrm{pr}_1(t) = \mathrm{pr}_2(t)\}$, элементами которого являются только такие пары (a, b), что $a = b$. Проверьте, что тождественное отображение id_x удовлетворяет всем условиям 1–4.

3. Варьируя набор из рассмотренных выше четырёх свойств, можно получить шестнадцать видов бинарных отношений, некоторые из которых имеют собственные названия. Бинарное отношение называется

- *функцией*, или *отображением* из x в y, если оно удовлетворяет условиям 1, 2,
- *сюръекцией*, или *наложением* x на y, если выполняются условия 1, 2, 3,
- *инъекцией*, или *вложением* x в y, если выполняются условия 1, 2, 4,
- *биекцией* между x и y, если выполняются все четыре условия.

Условие «f есть функция из x в y» (точнее, выражающая его конъюнкция условий 1 и 2) сокращённо записывается как $f : x \to y$.

Условие «f есть биекция между x и y» сокращённо записывается как $f : x \leftrightarrow y$.

Упр. 57. Пусть $x \neq \varnothing$. Докажите, что: а) $\varnothing : \varnothing \to x$, б) $\varnothing : \varnothing \to \varnothing$, в) $\neg\exists f(f : x \to \varnothing)$. Иначе говоря, требуется доказать, что пустое множество есть отображение из пустого множества в произвольное множество, но не существует никакого отображения из непустого множества в пустое.

Для данной функции $f : x \to y$ и множеств $t \in x$, $u \subseteq x$ вводятся следующие термы:

$$f^{-1} \rightleftharpoons \{t \in \mathrm{Pr}_2(f) \times \mathrm{Pr}_1(f) \mid (\mathrm{pr}_2(t), \mathrm{pr}_1(t)) \in f\},$$
$$f(t) \rightleftharpoons \bigcup\{v \in \mathrm{Pr}_2(f) \mid (t, v) \in f\},$$
$$f[u] \rightleftharpoons \{v \in \mathrm{Pr}_2(f) \mid \exists t(t \in u \,\&\, (t, v) \in f)\}.$$

Терм f^{-1} называется *обратным отображением* к f, $f(t)$ — *значением функции* f для t, $f[u]$ — *образом* множества u. Таким образом, говоря о функциях, мы можем пользоваться традиционным обозначением $f(a) = b$ вместо $(a, b) \in f$.

Ввиду симметричности свойств биекции легко убедиться, что если f — биекция, то f^{-1} также является биекцией.

Упр. 58. [2] Докажите, что если f — функция, то

$$f[x \cup y] = f[x] \cup f[y],$$
$$f[x \cap y] \subseteq f[x] \cap f[y],$$
$$f[x] \setminus f[y] \subseteq f[x \setminus y].$$

Частичное решение: рассмотрим третий пример.

$$f[x] \setminus f[y] = \{z \in \mathrm{Pr}_2(f) \mid \exists t(t \in x \,\&\, (t, z) \in f) \,\&\, \neg\exists t(t \in y \,\&\, (t, z) \in f)\}$$
$$\exists t(t \in x \,\&\, (t, z) \in f) \,\&\, \forall t\neg(t \in y \,\&\, (t, z) \in f) \Rightarrow$$
$$\Rightarrow \exists t(t \in x \,\&\, (t, z) \in f) \,\&\, (t \notin y \vee (t, z) \notin f) \sim$$
$$\sim \exists t(t \in x \,\&\, t \notin y \,\&\, (t, z) \in f),$$

откуда $f[x] \setminus f[y] \subseteq f[x \setminus y]$.

Упр. 59. Докажите, что если f — биекция, то в последних двух примерах упр. 58 можно знаки $\subseteq$ заменить знаками равенства.

Суперпозицией отношений g и f называется отношение $g \circ f$, определяемое следующим образом:

$$g \circ f \rightleftharpoons \{t \in \mathrm{Pr}_1(f) \times \mathrm{Pr}_2(g) \mid \exists u \exists v(u \in f \,\&\, v \in g \,\&$$
$$\&\, \mathrm{pr}_1(t) = \mathrm{pr}_1(u) \,\&\, \mathrm{pr}_2(u) = \mathrm{pr}_1(v) \,\&\, \mathrm{pr}_2(v) = \mathrm{pr}_2(t))\}$$

Упр. 60. Докажите, что если f и g являются функциями, то $g \circ f$ также является функцией и $(g \circ f)(x) = g(f(x))$.

Упр. 61. Докажите, что если f и g одновременно являются биекциями (сюръекциями, инъекциями), то $g \circ f$ также является биекцией (сюръекцией, инъекцией); если g — биекция, а f — сюръекция (инъекция), то $g \circ f$ — сюръекция (инъекция).

4. Важный критерий возможности установления биекции между двумя множествами даёт следующая теорема.

Теорема 39 (Кантора–Шрёдера–Бернштейна). *Необходимым и достаточным условием существования биекции между множествами x и y является существование пары инъекций: из x в y и из y в x.*

$\lhd$Необходимость очевидна: биекция между x и y сама является одновременно инъекцией из x в y и из y в x.

Докажем достаточность. Пусть даны инъекции $f : x \to y$ и $g : y \to x$, «сконструируем» из них искомую биекцию. Обозначим через $\eta(t)$ терм $x \setminus g[y \setminus f[t]]$.

Запишем уравнение

$$u = \eta(u),$$

где $u \subseteq x$, и предположим, что оно имеет корень u_0. Посмотрим, какими свойствами должно обладать множество u_0, если таковое имеется. Пусть $v_0 = y \setminus f[u_0]$. Тогда $x \setminus g[v_0] = u_0$ и

$$\begin{aligned} g[v_0] &= x \setminus u_0, \\ f[u_0] &= y \setminus v_0. \end{aligned}$$

Таким образом, отношение $h' = \{t \in f \mid \mathrm{pr}_1(t) \in u_0\}$ задаёт биекцию между множествами u_0 и $y \setminus v_0$, а отношение $h'' = \{t \in \in g \mid \mathrm{pr}_1(t) \in v_0\}$ — биекцию между множествами $x \setminus u_0$ и v_0. Объединение $h = h' \cup h''^{-1}$ является биекцией между множествами x и y, и доказательство теоремы сводится к поиску корня уравнения $u = \eta(u)$.

Докажем, что решением этого уравнения является терм

$$u = \bigcup \{z \in \mathfrak{P}(x) \mid z \subseteq \eta(z)\}.$$

Действительно, $t \in u \sim \exists z(z \subseteq x \,\&\, z \subseteq \eta(z) \,\&\, t \in z)$. Нетрудно доказать, что «функция» $\eta(z)$ является «монотонной по включению», т. е.

$$z \subseteq z_0 \Rightarrow \eta(z) \subseteq \eta(z_0),$$

откуда

$$\begin{aligned} &z \subseteq \eta(z) \Rightarrow z \subseteq \eta(u) \quad \text{(в силу } z \subseteq u \text{ по определению } u), \\ &t \in z \,\&\, z \subseteq \eta(u) \Rightarrow t \in \eta(u), \end{aligned}$$

откуда $t \in u \Rightarrow t \in \eta(u)$ и $u \subseteq \eta(u)$.

В силу свойства «монотонности» η и только что доказанного соотношения $u \subseteq \eta(u)$ имеем $\eta(u) \subseteq \eta(\eta(u))$. Но всякое z, для которого $z \subseteq \eta(z)$, есть подмножество u по определению u. Значит, $\eta(u) \subseteq u$.

Отсюда $\eta(u) = u$, теорема доказана.▷

Иногда теорему 39 формулируют следующим образом.

Следствие. *Биекция между множествами x и y существует тогда и только тогда, когда существуют биекции между x и некоторым $y_0 \subseteq y$ и между y и некоторым $x_0 \subseteq x$.*

◁Действительно, биекция между x и некоторым $y_0 \subseteq y$ сама непосредственно является инъекцией из x в y, в силу чего утверждение следствия сводится к утверждению теоремы 39.▷

5. На произвольной паре множеств x, y, вообще говоря, можно построить бинарное отношение не любого вида. Так, если $x = \{a, b\}$, а $y = \{c, d, e\}$, то множество $\{(a, c), (b, d)\}$ является инъекцией из x в y, но никакое отношение вида $r \subseteq x \times y$ не будет инъекцией из y в x. Причина в том, что во втором множестве больше различных между собой элементов, чем в первом, и трём элементам второго множества нельзя поставить в соответствие три *различных между собой* элемента первого множества. На этом факте и будут построены наши рассуждения о мощностях множеств.

Пусть даны множества x и y. Рассмотрим четыре возможных случая:

1) Существует инъекция из x в y, но не существует инъекции из y в x.

2) Существует инъекция из y в x, но не существует инъекции из x в y.

3) Существуют обе инъекции: из x в y и из y в x. По теореме Кантора–Шрёдера–Бернштейна это эквивалентно тому, что существует биекция между x и y.

4) Не существует инъекций ни из x в y, ни из y в x.

Мы будем говорить, что

- *мощность x меньше мощности y* и писать $|x| < |y|$ в случае 1,
- $|y| < |x|$ в случае 2,
- множества x и y *равномощны*, или *эквивалентны*, и писать $|x| = |y|$ в случае 3,
- говорить, что множества *несравнимы* в случае 4. Одним из самых фундаментальных следствий аксиомы выбора является следующая теорема: *несравнимых множеств не существует*, т. е. случай 4 никогда не имеет места в ZFC. Доказать это мы сможем только в конце данной главы (см. теорему 61).

Если утверждается только лишь существование инъекции из x в y, но ничего не говорится про инъекцию из y в x, то говорят, что *мощность x меньше или равна мощности y*, и пишут $|x| \leqslant |y|$.

Заметим, что хотя $|x| \leqslant |y| \Rightarrow \neg|y| < |x|$ и $|x| < |y| \Rightarrow \neg|y| \leqslant |x|$, т. е. из *утверждения* отношений $<$, $\leqslant$ следует отрицание отношений $\geqslant$, $>$, из *отрицания* любого из этих отношений не следует никакого утверждения про отношения мощностей. Так, если мы отрицаем $|x| < |y|$, то в этом случае может иметь место как случай $|x| \geqslant |y|$, так и случай, когда x и y несравнимы. Поэтому мы должны проявлять осторожность и понимать, что в действительности среди утверждений «не меньше», «больше или равно», «не меньше или равно», «больше» *нет эквивалентных по определению*.

Эквивалентность $\neg|x| \leqslant |y|$ и $|x| > |y|$ следует из аксиомы выбора, но, во-первых, нами это ещё не доказано. Кроме того, необходимо иметь возможность чётко различать теоремы, зависимые и независимые от аксиомы выбора (например, до сих пор аксиома выбора нигде не использовалась). Поэтому впредь мы намерены придерживаться оговорённых здесь предосторожностей.

Только что введённые знаки $<$, $\leqslant$, $=$ обладают следующими свойствами:

- $x = y \Rightarrow |x| = |y|$,
- $x \subseteq y \Rightarrow |x| \leqslant |y|$,
- транзитивность: $|x| \leqslant |y|$ & $|y| \leqslant |z| \Rightarrow |x| \leqslant |z|$; то же для $<$ и $=$,
- рефлексивность: $|x| \leqslant |x|$, $|x| = |x|$,
- антирефлексивность строгого неравенства: $\neg|x| < |x|$,
- симметричность равенства: $|x| = |y| \sim |y| = |x|$,
- антисимметричность строго неравенства: $|x| < |y| \Rightarrow \neg|y| < |x|$,
- теорема Кантора–Шрёдера–Бернштейна: $|x| \leqslant |y| \& |y| \leqslant |x| \sim |x| = |y|$.

Упр. 62. Докажите приведённые выше утверждения.

До сих пор мы не дали никаких определений, касающихся понятия мощности множества *как таковой*, используя конструкцию $|x|$ лишь в контексте отношений сравнения. Это сделано намеренно: пока что в нашем распоряжении нет аппарата, позволяющего рассматривать запись вида $|x|$ как *терм* (а термами у нас являются множества и только они), но зато вполне ясно, какие *формулы* языка первого порядка соответствуют выражениям вида $|x| < |y|$ или $|x| = |y|$ (выпишите их в качестве упражнения). Может возникнуть желание определить терм $|x|$ как совокупность всех множеств, имеющих ту же мощность, что и x (в этом случае выражение $|x| = |y|$ сводилось бы к $x \in |y|$). Проблема в том, что предположение о существовании множества множеств, равномощных исходному, как и в случае со «множеством Рассела», ведёт к парадоксам. Подобная совокупность не является множеством в ZFC и потому не может быть термом. Поэтому мы должны либо вновь пересмотреть понятие «терм», либо предложить в качестве терма для $|x|$ нечто другое, являющееся множеством. Возможен и ещё

один подход (который мы примем): отказаться от всякого разговора о «природе» мощности как таковой, рассматривая только сравнения множеств по мощностям.

6. Следующая важная теорема указывает на случай, когда множества оказываются неравномощными.

Теорема 40 (Кантора). *Мощность любого множества строго меньше мощности множества всех его подмножеств, т. е. для любого x,*

$$|x| < |\mathfrak{P}(x)|.$$

$\lhd$Прежде всего заметим, что $|x| \leqslant |\mathfrak{P}(x)|$. В самом деле, бинарное отношение

$$\{d \in x \times \mathfrak{P}(x) | \{\mathrm{pr}_1(d)\} = \mathrm{pr}_2(d)\}$$

является инъекцией из x в $\mathfrak{P}(x)$.

Предположим, что существует инъекция $f : \mathfrak{P}(x) \to x$. Выделим множество $a = \{t \in f | \mathrm{pr}_2(t) \notin \mathrm{pr}_1(t)\}$, а также $b = \mathrm{Pr}_2(a)$. Т. к. $b \subseteq x$, то существует единственный y, такой, что $y \in x \,\&\, (b, y) \in f$ (иначе говоря, $y = f(b)$).

Теперь посмотрим, что можно сказать о выводимости утверждения $y \in b$.

Если предположить $y \notin b$, то, по определению множества a, $(b, y) \in a$, откуда $y \in \mathrm{Pr}_2(a)$, откуда $y \in b$ — противоречие. Если предположить $y \in b$, то $(b, y) \notin a$. Но, по условию $b = \mathrm{Pr}_2(a)$, и значит, всё-таки $y \in \mathrm{Pr}_2(a)$, а значит, существует некоторое $c \in \in \mathrm{Pr}_1(a)$, такое, что $c \neq b$ и $(c, y) \in a$. Но последнее нарушает предположение о том, что f — инъекция, т. е. обратнооднозначная функция.

Итак, добавление к посылкам как утверждения $y \in b$, так и его отрицания ведёт к противоречию — следовательно, противоречива исходная посылка о существовании инъекции f.$\rhd$

Обратите внимание на связь доказательства теоремы Кантора с рассуждением на с. 82, приводящим к парадоксу Рассела.

Теорема Кантора вместе с аксиомой существования множества всех подмножеств говорят о том, что, каким бы ни было множество x, при помощи операции $\mathfrak{P}(x)$ мы можем построить множество, превосходящее исходное по мощности. В частности, на этой теореме основывается рассуждение, называемое *парадоксом Кантора*, которое демонстрирует невозможность существования «множества всех множеств» $V = \{x | x = x\}$.

В самом деле, $\forall x \forall t (x \in t \Rightarrow x \in V)$, т. е. всякое множество t должно быть подмножеством V; следовательно, $\forall t\ |t| \leqslant |V|$. Но в силу аксиомы множества всех подмножеств для V, как и любого множества, существует $\mathfrak{P}(V)$ и по теореме Кантора $|\mathfrak{P}(V)| > |V|$, что противоречит предыдущему утверждению. Следовательно, V не может существовать, что вновь вступает в противоречие с «наивной» гипотезой о том, что любое синтаксически корректное логическое условие определяет множество, т. е. что $\exists y \forall z (z \in y \Leftrightarrow A)$ для любой формулы A, не содержащей y свободно.

Упр. 63. Докажите, что

1) не существует множества $e = \{t \mid |t| = |\{\varnothing\}|\}$ всех одноэлементных множеств (указание: чему равнялось бы $\bigcup e$?),

2) для любого непустого множества u не существует множества $\{t \mid |t| = |u|\}$ всех множеств, равномощных u.

7. Конечные и бесконечные множества. Для обозначения мощности натуральных чисел $|\omega|$ применяют символ $\aleph_0$ (читается «а́леф-нуль», алеф — первая буква еврейского алфавита). Таким образом, записи $|x| < \aleph_0$, $|x| \geqslant \aleph_0$ означают $|x| < |\omega|$, $|x| \geqslant |\omega|$ соответственно.

Множество называется *бесконечным*, если $|x| \geqslant \aleph_0$, и *конечным*, если $|x| < \aleph_0$.

Что означают эти условия на содержательном уровне? Условие бесконечности означает существование такой $f : \omega \to x$, с помощью которой можно организовать неограниченный последовательный выбор всё новых элементов интересующего нас множества: сначала выбирается $f(0)$, затем не равный ему $f(1)$, затем не равный

двум предыдущим $f(2)$ и т. д., при этом процесс никогда не закончится исчерпанием элементов x. Если же $|x| < \aleph_0$, то возможно построить биекцию между x и некоторым (как мы сейчас убедимся, имеющим наибольший элемент) подмножеством натуральных чисел, но инъекции из ω в x не существует и бесконечный процесс выбора организовать невозможно.

Множество, несравнимое с ω, с точки зрения данных нами определений должно являться одновременно не бесконечным и не конечным. Первым шагом по направлению к доказательству общей теоремы о сравнимости любых двух множеств является следующая теорема, в которой мы впервые применим аксиому выбора.

°**Теорема 41.** $\mathrm{ZFC} \vdash \neg|x| \geqslant \aleph_0 \sim |x| < \aleph_0$. *Иначе говоря, в системе ZF с аксиомой выбора любое множество либо бесконечно, либо конечно.*

$\lhd$В одну сторону утверждение элементарно. По определению,

$$\begin{aligned} |x| \geqslant \aleph_0 &\sim \exists f\,«f : \omega \to x \text{ — инъекция»},\\ |x| < \aleph_0 &\sim \exists g\,«g : x \to \omega \text{ — инъекция»}\,\&\\ &\&\neg\exists f\,«f : \omega \to x \text{ — инъекция»}, \end{aligned}$$

откуда сразу следует $|x| < \aleph_0 \Rightarrow \neg|x| \geqslant \aleph_0$.

Чтобы доказать, что $\neg|x| \geqslant \aleph_0 \Rightarrow |x| < \aleph_0$, требуется показать наличие инъекции из x в ω при условии отсутствия инъекции из ω в x.

Случай, когда $x = \varnothing = 0$, тривиален, поэтому будем считать множество x не пустым.

Следствием аксиомы выбора, как мы сейчас проверим, является существование такой функции $f : \mathfrak{P}(x) \setminus \{\varnothing\} \to x$, что

$$\forall t(t \neq \varnothing \,\&\, t \subseteq x \Rightarrow f(t) \in t)$$

(иначе говоря, существует функция, которая каждому непустому подмножеству некоторого множества x ставит в соответствие один

элемент этого подмножества). Достроим эту функцию следующим образом:

$$f' = \{(\varnothing, \varnothing)\} \cup \{u \in \mathfrak{P}(x) \times \mathfrak{P}(x) \mid \{f(\mathrm{pr}_1(u))\} = \mathrm{pr}_2(u)\}.$$

Теперь функция определена на всём множестве $\mathfrak{P}(x)$ и обладает свойствами $f'(\varnothing) = \varnothing$, $u \neq \varnothing \,\&\, u \subseteq x \Rightarrow \exists t(\{t\} = f'(u) \,\&\, t \in u)$.

Построим функцию $g : \omega \to \mathfrak{P}(x)$ на основе следующих логических условий:

$$g(0) = x,$$
$$g(n+1) = g(n) \setminus f'(g(n)).$$

Иначе говоря, мы выбираем элемент $x_0 = f(x)$ и «выбрасываем» его из множества x. Если в результате осталось пустое множество, то $g(1)$ и все последующие $g(n)$ получат значение $\varnothing$. Если после удаления одного элемента множество осталось не пустым, то мы выбираем элемент из оставшихся и «выбрасываем» его, и т. д.

Заметим, что выводимы следующие утверждения:

1. $\forall n \forall m(n \neq m \,\&\, g(n) \neq \varnothing \,\&\, g(m) \neq \varnothing \Rightarrow f(g(n)) \neq f(g(m)))$. Иначе говоря, пока $g(n) \neq \varnothing$, из множества x выбираются всё новые элементы. В самом деле, $g(m) \subseteq g(n)$ (можно показать по индукции) и элементы $f(g(m))$ и $f(g(n))$ принадлежат непересекающимся множествам $g(m)$ и $g(n) \setminus g(m)$.

2. $g(n) = \varnothing \Rightarrow (\forall m(m > n \Rightarrow g(m) = \varnothing))$ (можно доказать индукцией).

3. $\exists n\ g(n) = \varnothing$. Если допустить $\forall n\ g(n) \neq \varnothing$, то, в силу п. 1, суперпозиция $f \circ g : \omega \to x$ образует инъекцию, определённую на всём множестве ω, что противоречит условию $\neg|x| \geqslant \aleph_0$.

4. $\forall t(t \in x \Rightarrow \exists n(f(g(n)) = t))$. Пусть существует такое $t \in x$, что $\forall n f(g(n)) \neq t$. Но это значит, что $t \in g(0)$ и $\forall n\ t \in g(n)$, т. е. все множества $g(n)$ — непустые, что противоречит п. 3.

Итак, существует такой n, что функция $\{t \in f \circ g \mid \mathrm{pr}_1(t) < n\}$ является всюдуопределённой, всюдузначной, прямо- и обратнооднозначной, иначе говоря, биекцией между множеством x и подмно-

жеством ω, состоящим из всех чисел, меньших n, а значит, и инъекцией из x в ω, что и требовалось доказать.

Остаётся проверить, что существует $f : \mathfrak{P}(x) \setminus \{\varnothing\} \to x$ такая, что $\forall t(t \neq \varnothing \& t \subseteq x \Rightarrow f(t) \in t)$ (т. е. функция, выбирающая из любого непустого подмножества x один из элементов этого подмножества). Несмотря на «очевидность» этого утверждения, вывести его можно только из аксиомы выбора.

Напомним суть аксиомы выбора: для любого семейства непустых попарно непересекающихся множеств существует множество, содержащее ровно по одному элементу из каждого множества исходного семейства. Для нас это утверждение эквивалентно тому, что существует функция, ставящая в соответствие каждому множеству из семейства непересекающихся множеств его элемент: $\forall x(\forall y \forall z(y \in x \,\&\, z \in x \Rightarrow (y \neq \varnothing \,\&\, (y \cap z \neq \varnothing \Rightarrow z = y))) \Rightarrow \Rightarrow \exists f(f : x \to \bigcup x \,\&\, \forall t(t \in x \Rightarrow f(t) \in t)))$.

Как быть со множеством $\mathfrak{P}(x) \setminus \{\varnothing\}$, некоторые элементы которого попарно пересекаются? К нужному виду, например, его можно привести, помножив каждый элемент $t \subseteq x \,\&\, t \neq \varnothing$ на $\{t\}$, т. к. $t_1 \neq t_2 \Rightarrow t_1 \times \{t_1\} \cap t_2 \times \{t_2\} = \varnothing$.

Итак, множество

$$p = \{u \in \mathfrak{P}(x \times \mathfrak{P}(x)) \mid \exists t(t \in (\mathfrak{P}(x) \setminus \varnothing) \,\&\, u = t \times \{t\})\}$$

удовлетворяет требованиям аксиомы выбора, и функция $f'(x) = \mathrm{pr}_1(f(x \times \{x\}))$, где f — функция выбора для множества p, есть функция выбора для множества $\mathfrak{P}(x) \setminus \{\varnothing\}$.$\triangleright$

Фигурирующее в доказательстве число n, на котором заканчивается процесс выбора элементов x (точнее, $n = \inf\{m \in \omega \mid g(m) = \varnothing\}$), является, очевидно, количеством элементов в конечном множестве x. Следствием (вполне ожидаемым) только что доказанной теоремы является тот факт, что любому конечному множеству соответствует некоторое натуральное число n, получающееся в результате пересчёта его элементов.

Обратим ещё раз внимание на тот факт, что утверждение $|x| < \aleph_0$ является отрицанием утверждения $|x| \geqslant \aleph_0$ только при усло-

вии, что мы принимаем аксиому выбора. В теории множеств, отрицающей аксиому выбора, возможно существование (наряду с конечными и бесконечными) несравнимых с ω множеств, которые, однако, будут «не бесконечными и не конечными» с точки зрения данных нами определений. Если мы желаем до конца быть последовательными в вопросе разделения зависимых и независимых от аксиомы выбора утверждений, то мы должны всегда делать упор на то, что именно — конечность, бесконечность, отрицание одного либо другого — мы утверждаем в том или ином случае.

Теорема 42. *Непустое подмножество натуральных чисел бесконечно тогда и только тогда, когда оно не содержит наибольшего элемента.*

$\lhd$В свете только что сказанного прежде всего заметим, что любое $u \subseteq \omega$ сравнимо с ω и без аксиомы выбора, т. к. $f = \{t \in u \times \omega \mid \mathrm{pr}_1(f) = \mathrm{pr}_2(f)\}$ есть инъекция из u в ω.

В одну сторону. Пусть u непусто и не содержит наибольшего элемента. Построим функцию $f : \omega \to \mathfrak{P}(u)$ на основе следующих логических условий:

$$f(0) = u,$$
$$f(n+1) = f(n) \setminus \{\bigcap(f(n))\}.$$

Таким образом, мы ставим в соответствие нулю всё множество u, а затем на каждом шаге отбрасываем из $f(n)$ либо его наименьший элемент (если $f(n) \neq \varnothing$, см. упр. 53), либо пустое множество, если $f(n) = \varnothing$ (см. упр. 42). Используя тот факт, что u — непустое множество без наибольшего элемента, при помощи индукции нетрудно убедиться, что

$$\forall n(n \in \omega \Rightarrow f(n) \neq \varnothing),$$

т. е. процесс «извлечения» элементов никогда не прекратится, и что

$$\forall m \forall n(m \in \omega \,\&\, n \in \omega \,\&\, m < n \Rightarrow \inf(f(m)) < \inf(f(n))),$$

т. е. наименьшие элементы всех $f(n)$ различны между собой и образуют возрастающую последовательность ($f(0) \neq \varnothing$ по условию,

и если предположить $\exists n f(n) \neq \varnothing \,\&\, f(n+1) = \varnothing$, то $f(n)$ окажется равным $\{\sup(u)\}$). Отсюда уже ясно, что функция $g : \omega \to u$, определённая условием $g(n) = \inf(f(n))$, есть искомая инъекция, обеспечивающая бесконечность множества u.

В обратную сторону. Пусть дана инъекция $f : \omega \to u$ и $\exists m\ \sup(u) = m$. По условию $\exists! n\ f(n) = m$ и

$$f \setminus \{(n, m)\} : \omega \setminus \{n\} \to u \setminus \{m\}$$

есть инъекция из множества ω без элемента n в множество u без своего наибольшего элемента. Но для любого n существует биекция между ω и $\omega \setminus \{n\}$: поставим в соответствие каждому элементу $x \in \in \omega \,\&\, x < n$ самого себя и каждому элементу $x \in \omega \,\&\, x \geqslant n$ элемент $x + 1$. Отсюда следует, что существует также инъекция из ω в $u \setminus \{\sup(u)\}$.

Теперь воспользуемся индукцией по величине $\sup(u)$ для того, чтобы доказать, что какой бы она ни была, все множества, имеющие наибольший элемент, конечны.

Если $\sup(u) = 0$, то $u = \{\varnothing\}$, $u \setminus \{\sup(u)\} = \varnothing$ и не может существовать никакой функции (не говоря уже об инъекции) из ω в $\varnothing$, т. к. нарушается условие всюдуопределённости. Значит, множество $\{\varnothing\}$ конечно. Предположим теперь, что $\sup(u) = m + 1$ и любое подмножество ω, чей наибольший элемент равен m, конечно. Но если бы имелось бесконечное u с наибольшим элементом $m+1$, то существовала бы инъекция $g : \omega \to u \setminus \{\sup(u)\}$. Множество $u \setminus \{\sup(u)\}$ непусто и ограничено сверху элементом $\sup(u)$, и с учётом $\sup(u \setminus \{\sup(u)\}) < \sup(u)$ имеем противоречие с предположением индукции.$\triangleright$

При доказательстве этой теоремы обнаружилось, что «отбрасывание» одного элемента из бесконечного множества оставляет его бесконечным. Но в действительности мы можем отбросить и бесконечное число элементов. Из приведённой ниже таблицы, в которой числа, выписанные в одном столбце, поставлены в биективное соответствие друг другу, ясно, что мощность $\aleph_0$ имеет не только множество ω, но также его строгие подмножества: множество нечётных

чисел, множество простых чисел, квадратов натуральных чисел, множество степеней двойки и т. д.:

$$
\begin{array}{lllllll}
1 & 2 & 3 & 4 & 5 & \cdots & n \\
1 & 3 & 5 & 7 & 9 & \cdots & 2n-1 \\
2 & 3 & 5 & 7 & 11 & \cdots & p_n \\
1 & 4 & 9 & 16 & 25 & \cdots & n^2 \\
2 & 4 & 8 & 16 & 32 & \cdots & 2^n \\
1 & 2 & 6 & 24 & 120 & \cdots & n!
\end{array}
$$

Можно привести примеры последовательностей натуральных чисел с ещё более быстрым ростом, которые, как бы редко они ни были распределены в ω, имеют мощность не меньшую, чем всё множество натуральных чисел[3]. Такое нарушение принципа «часть меньше целого» есть характерная черта бесконечных множеств.

Теорема 43 (критерий Дедекинда). *Множество является бесконечным, если и только если оно равномощно некоторому своему строгому подмножеству.*

$\lhd$*В одну сторону.* Пусть $u_1 \subset u$ и $f : u \leftrightarrow u_1$ — биекция, докажем существование инъекции $g : \omega \to u$.

[3] Б. Рассел в книге «Misticism and Logic» указывает следующее остроумное «применение» данному свойству бесконечности. В романе Л. Стерна «Жизнь и мнения Тристрама Шенди, джентльмена» герой обнаруживает, что ему потребовался целый год, чтобы изложить события первого дня его жизни, и ещё один год понадобился, чтобы описать второй день. В связи с этим герой сетует, что материал его биографии будет накапливаться быстрее, чем он сможет его обработать, и он никогда не сможет её завершить. «Теперь я утверждаю, — возражает на это Рассел, — что если бы он жил вечно и его работа не стала бы ему в тягость, даже если бы его жизнь продолжала быть столь же богатой событиями, как вначале, то ни одна из частей его биографии не осталась бы ненаписанной». Действительно, события n-го дня своей жизни Шенди мог бы описать за n-й год и, таким образом, в его автобиографии каждый день оказался бы запечатлён: иначе говоря, если бы жизнь длилась бесконечно, то она насчитывала бы столько же лет, сколько дней.

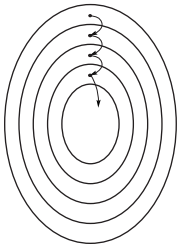


Рис. 2.8. К доказательству теоремы 43

По условию $\exists x_0(x_0 \in u \setminus f[u])$. Определим $g : \omega \to u$ на основе следующих логических условий:

$$g(0) = x_0,$$
$$g(n+1) = f(g(n)).$$

Иначе говоря, мы выбираем некоторый элемент $x_0 \in u \setminus f[u]$, а затем последовательно применяем к нему функцию $f : u \to u_1$: $x_1 = f(x_0)$, $x_2 = f(x_1)$ и т. д.

Индукцией можно показать, что в силу биективного характера f

$$u \supset f[u] \supset f[f[u]] \supset f[f[f[u]]] \supset \ldots,$$

$$x_0 \in u \setminus f[u],\ x_1 \in f[u] \setminus f[f[u]],\ x_2 \in f[f[u]] \setminus f[f[f[u]]], \ldots,$$

из чего следует, что все x_i различны между собой, т. е. построенная нами $g : \omega \to u$ — инъекция.

В обратную сторону. Пусть множество u бесконечно. Тогда существует инъекция $f : \omega \to u$. «Выбросим» из u элемент $f(0)$ и построим биекцию $g : f[\omega] \leftrightarrow f[\omega] \setminus \{f(0)\}$ по условию $g(f(n)) = f(n+1)$.$\triangleright$

§ 2.5. Операции над мощностями

1. Пусть множества x и y конечны и содержат соответственно n и m элементов. Легко убедиться, что если $x \cap y = \varnothing$, то

- множество $x \cup y$ содержит $n + m$ элементов,
- множество $x \times y$ содержит nm элементов,
- множество $\mathfrak{P}(x)$ содержит 2^n элементов.

Говоря о мощности множеств $x \cup y$, $x \times y$, $\mathfrak{P}(x)$ для произвольных x, y, применяют следующие сокращающие обозначения:

$$|x \cup y| \rightleftharpoons |x| + |y|,$$
$$|x \times y| \rightleftharpoons |x||y|,$$
$$|\mathfrak{P}(x)| \rightleftharpoons 2^{|x|}.$$

В частности, теорема Кантора может быть записана как

$$\forall x\ (2^{|x|} > |x|).$$

Заметим, что все эти обозначения — чистый формализм, т. к. мы не определили, что за объекты представляют собой $|x|$ и $|y|$. Однако эти конструкции удобно применять, т. к. их свойства хорошо согласуются со свойствами соответствующих арифметических операций.

Теорема 44. *Выводимы следующие утверждения:*

$$|x| = |u| \,\&\, |y| = |v| \Rightarrow |x| + |y| = |u| + |v|,$$
$$|x| = |u| \,\&\, |y| = |v| \Rightarrow |x||y| = |u||v|,$$
$$|x| = |u| \Rightarrow 2^{|x|} = 2^{|u|},$$
$$|x| + |y| = |y| + |x|, \quad |x||y| = |y||x|,$$
$$(|x| + |y|) + |z| = |x| + (|y| + |z|), \quad (|x||y|)|z| = |x|(|y||z|),$$
$$|x|(|y| + |z|) = |x||y| + |x||z|,$$
$$2^{|x|+|y|} = 2^{|x|}2^{|y|}.$$

$\lhd$1. Пусть даны биекции $f : x \leftrightarrow u$ и $g : y \leftrightarrow v$. Тогда

$$f \cup g : x \cup y \leftrightarrow u \cup v$$

(здесь используется условие, что $x \cap y = \varnothing$), а бинарное отношение

$$\{((a, b), (c, d)) \in (x \times y) \times (u \times v) \mid (a, c) \in f \,\&\, (b, d) \in g\}$$

есть биекция[4] между $x \times y$ и $u \times v$.

2. Докажем $|x| = |u| \Rightarrow 2^{|x|} = 2^{|u|}$. Пусть $f : x \leftrightarrow u$, тогда

$$\{t \in \mathfrak{P}(x) \times \mathfrak{P}(u) \mid f[\mathrm{pr}_1(t)] = \mathrm{pr}_2(t)\}$$

является биекцией между множествами $\mathfrak{P}(x)$ и $\mathfrak{P}(u)$.

3. Утверждение $|x| + |y| = |y| + |x|$ следует из $x \cup y = y \cup x$. Бинарное отношение

$$\{(a, (b, c)) \in (x \times y) \times (y \times x) \mid a = (c, b)\}$$

есть биекция между $x \times y$ и $y \times x$.

4. Утверждение $(|x| + |y|) + |z| = |x| + (|y| + |z|)$ следует из $(x \cup y) \cup z = x \cup (y \cup z)$. Бинарное отношение

$$\{(a, (b, (c, d))) \in ((x \times y) \times z) \times (x \times (y \times z)) \mid a = ((b, c), d)\}$$

есть биекция между $(x \times y) \times z$ и $x \times (y \times z)$.

5. Утверждение $|x|(|y|+|z|) = |x||y|+|x||z|$ следует из $x \times (y \cup z) = x \times y \cup x \times z$.

6. Утверждение $2^{|x|+|y|} = 2^{|x|}2^{|y|}$ несколько сложнее: здесь вновь необходимо использовать тот факт, что x и y — непересекающиеся множества. Каждый элемент $t \in \mathfrak{P}(x \cup y)$ состоит из элементов, принадлежащих x, и элементов, принадлежащих y, т. е. $t = t' \cup t''$, где $t' = t \cap x$ и $t'' = t \cap y$. Т. к. $x \cap y = \varnothing$, то разложение t на $t' \cup t''$ возможно единственным образом, и бинарное отношение

$$\{(a, (b, c)) \in \mathfrak{P}(x \cup y) \times (\mathfrak{P}(x) \times \mathfrak{P}(y)) \mid a = b \cup c\}$$

является биекцией между $\mathfrak{P}(x \cup y)$ и $\mathfrak{P}(x) \times \mathfrak{P}(y)$.$\triangleright$

2. Введём обозначение

$$x^y \rightleftharpoons \{f \in \mathfrak{P}(y \times x) \mid f :\ y \to x\},$$

[4] Разумеется, требуется ещё доказать, что все приводимые здесь термы в действительности являются биекциями. В каждом случае такое доказательство представляет собой нетрудное, но громоздкое упражнение по формальному выводу, поэтому мы не будем на этом останавливаться.

т. е. результат теоретико-множественного возведения в степень представляет собой набор всех возможных функций из y в x.

Упр. 64. [7]. Чему равно а) $x^{\varnothing}$, т. е. x^0 для произвольного x? б) $\varnothing^x$, т. е. 0^x для $x \neq \varnothing$? (Указание: см. упр. 57. Ответ: а) $\{\varnothing\}$, т. е. 1, б) $\varnothing$, т. е. 0).

Пользуясь комбинаторным рассуждением, легко доказать, что если множества x и y конечны и содержат соответственно n и m элементов, то множество x^y содержит n^m элементов. Говоря о мощности множества x^y для произвольных x, y, применяют следующее сокращающее обозначение:

$$|x^y| \rightleftharpoons |x|^{|y|}.$$

Теорема 45. *Выводимы следующие утверждения:*

$$\begin{aligned}
&|x| = |u| \,\&\, |y| = |v| \Rightarrow |x|^{|y|} = |u|^{|v|},\\
&|x|^{|y|+|z|} = |x|^{|y|}|x|^{|z|},\\
&(|x||y|)^{|z|} = |x|^{|z|}|y|^{|z|},\\
&\left(|x|^{|y|}\right)^{|z|} = |x|^{|y||z|}.
\end{aligned}$$

◁Как и при доказательстве теоремы 44, доказательство каждого из этих утверждений сводится к указанию соответствующей биекции. Формальные выражения для этих биекций достаточно громоздки, поэтому для экономии места и наглядности мы только наметим принципы, по которым их можно построить.

1. Пусть даны биекции $f : x \leftrightarrow u$ и $g : y \leftrightarrow v$. Тогда взаимно однозначное отношение между функциями $h \in x^y$ и $h' \in u^v$ будет определяться условием $\forall t(t \in y \Rightarrow f(h(t)) = h'(g(t)))$.

2. Элемент $h \in x^{y \cup z}$ является функцией со значениями в x, определённой на $y \cup z$. Каждая из этих функций состоит из двух частей: той, что определена на y, и той, что определена на z:

$$\begin{aligned}
&h' = \{t \in h \mid \mathrm{pr}_1(t) \in y\},\\
&h'' = \{t \in h \mid \mathrm{pr}_1(t) \in z\},\\
&h = h' \cup h'', \quad h' \cap h'' = \varnothing.
\end{aligned}$$

Нетрудно убедиться, что отношение между $h \in x^{y \cup z}$ и парой элементов $h' \in x^y$, $h'' \in x^z$ — взаимно однозначное, что позволяет построить биекцию между $x^{y \cup z}$ и $x^y \times x^z$.

3. Посмотрим, как конструируется биекция между $(x \times y)^z$ и $x^z \times \times y^z$. Элемент $h \in (x \times y)^z$ есть функция, ставящая в соответствие элементу z пару элементов из $x \times y$. Но ей взаимно однозначно соответствует пара функций из z в x и из z в y: так, кривая на плоскости, заданная функцией $\mathbf{r}(t)$, ставящей в соответствие переменной $t \in \mathbb{R}$ радиус-вектор $\mathbf{r} \in \mathbb{R} \times \mathbb{R}$, однозначно определяется парой функций $(x(t), y(t))$, задающих соответственно абсциссу и ординату радиуса-вектора.

4. Наконец, элемент $h \in x^{y \times z}$ представляет собой функцию из $y \times z$ в x, т. е. функцию двух аргументов. Если фиксировать второй аргумент (из множества z), то получится функция $f_z = \{t \in \in y \times x \mid (\mathrm{pr}_1(t), (\mathrm{pr}_2(t), z)) \in h\}$ из y в x, т. е. $f_z \in x^y$. Но тогда $(x^y)^z$ есть множество всех функций из y в x, зависящих от параметра z, что, конечно, является всего лишь другим взглядом на множество функций двух аргументов.$\triangleright$

В частности, если x состоит всего из двух элементов (допустим, является неупорядоченной парой $\{0, 1\}$), то терм x^y представляет собой множество всех возможных способов поставить в соответствие каждому элементу y нуль или единицу. Этих способов столько же, сколько существует подмножеств у y (выберем некоторое подмножество y и поставим в соответствие его элементам единицы, остальным элементам y — нули), поэтому для двухэлементного множества x значение $|x|^{|y|}$ равно $2^{|y|}$. Если же $y = \{0, 1\} = 2$, то терм x^y представляет собой множество всех возможных способов поставить в соответствие нулю один из элементов множества x, а единице — другой или тот же самый элемент. Таким образом, в этом случае терм x^y равномощен множеству всевозможных упорядоченных пар элементов x, т. е. $|x|^{|y|} = |x||x| = |x|^2$. По индукции уже нетрудно показать, что для любого $n \in \omega$

$$|x|^n = |\underbrace{x \times x \times \ldots \times x}_{n \text{ раз}}|.$$

Как видим, введённые нами операции над мощностями согласуются по своим свойствам с соответствующими арифметическими операциями и в случае конечных множеств соответствуют таковым над количествами элементов в множествах.

3. Следующая теорема показывает, что основные операции над термами оставляют конечные множества конечными.

Теорема 46. *Если x и y — не бесконечные множества, то множества $x \cup y$, $\mathfrak{P}(x)$, $x \times y$, x^y также не являются бесконечными.*

$\lhd$1. Пусть дана инъекция $f : \omega \to x \cup y$. Рассмотрим множества $u = \{t \in \omega \mid f(t) \in x\}$ и $v = \{t \in \omega \mid f(t) \in y\}$. Оба этих множества не должны быть бесконечными (если бы существовала, скажем, инъекция $g : \omega \to u$, то существование инъекции $f \circ g : \omega \to x$ противоречило бы условию). В силу теоремы 42 у множеств u и v существуют наибольшие элементы. Можно показать, что в этом случае наибольший элемент (равный большему из чисел $\sup(u)$, $\sup(v)$) имеется и у множества $u \cup v$. Но $u \cup v = \omega$ — без наибольшего элемента, противоречие.

2. Если множество x — пустое, то $\mathfrak{P}(x) = \{\varnothing\} = \{0\}$ — ограниченное множество, являющееся конечным по теореме 42. Если множество x непустое, то $\exists t(t \in x)$. Представим терм $\mathfrak{P}(x)$ в виде непересекающихся множеств

$$\begin{gathered} v_1 = \{u \in \mathfrak{P}(x) \mid t \in u\}, \\ v_2 = \{u \in \mathfrak{P}(x) \mid t \notin u\}, \\ \mathfrak{P}(x) = v_1 \cup v_2,\ v_1 \cap v_2 = \varnothing. \end{gathered}$$

Докажем, что $|v_1| = |v_2| = |\mathfrak{P}(x \setminus \{t\})|$. Отношение

$$\{z \in v_1 \times \mathfrak{P}(x \setminus \{t\}) \mid \mathrm{pr}_1(t) = \mathrm{pr}_2(t) \setminus \{t\}\}$$

есть биекция между $|v_1|$ и $\mathfrak{P}(x \setminus \{t\})$,

$$\{z \in v_2 \times \mathfrak{P}(x \setminus \{t\}) \mid \mathrm{pr}_1(t) = \mathrm{pr}_2(t)\}$$

есть биекция между $|v_2|$ и $\mathfrak{P}(x \setminus \{t\})$.

По доказанному в п. 1 настоящей теоремы в предположении небесконечности множеств v_1 и v_2 множество $v_1 \cup v_2$ также должно быть не бесконечным. Если же предположить $|\mathfrak{P}(x)| = |v_1 \cup v_2| \geqslant \aleph_0$, то $|v_1| \geqslant \aleph_0 \vee |v_2| \geqslant \aleph_0$. Отсюда выводится $|\mathfrak{P}(x \setminus \{t\})| \geqslant \aleph_0$, откуда

$$|\mathfrak{P}(x)| \geqslant \aleph_0 \Rightarrow (x \setminus \{t\} \neq \varnothing) \,\&\, (|\mathfrak{P}(x \setminus \{t\})| \geqslant \aleph_0),$$

и мы можем бесконечно удалять по одному элементу из x, тем самым организовав инъекцию из ω в x.

3. Если x и y — не бесконечные множества, то $x \times y$ — не бесконечное, т. к. является подмножеством не бесконечного множества $\mathfrak{P}\mathfrak{P}(x \cup y)$.

4. Если x и y — не бесконечные множества, то x^y — не бесконечное, т. к. является подмножеством не бесконечного множества $\mathfrak{P}\mathfrak{P}(x \times y)$.$\triangleright$

Мы намеренно использовали термин «не бесконечное множество» вместо «конечное множество», чтобы сделать эту, не зависящую от аксиомы выбора, теорему пригодной и для аксиоматических систем, отвергающих аксиому выбора.

Следствие. *Если* $|x| < \aleph_0$ *и* $|y| < \aleph_0$, *то* $|x| + |y| < \aleph_0$, $2^{|x|} < \aleph_0$, $|x||y| < \aleph_0$ *и* $|x|^{|y|} < \aleph_0$.

°**Следствие.** *Не существует такого* x, *что* $2^{|x|} = \aleph_0$.

4. Счётные множества. Множества, мощность которых равна $\aleph_0$ (т. е. такие, что каждому элементу исходного множества можно поставить в соответствие уникальное натуральное число и каждому натуральному числу — уникальный элемент исходного множества), называются *счётными*.

Рассмотрим несколько примеров счётных множеств и их свойств.

- Если x и y — счётные, $x \cap y = \varnothing$, то $x \cup y$ — также счётное, т. е. $\aleph_0 + \aleph_0 = \aleph_0$.

Пусть элементы x и y занумерованы. Тогда элементы множества $x \cup y$ можно занумеровать, расположив их следующим образом:

$$x_0,\ y_0,\ x_1,\ y_1, \ldots$$

При этом каждый n-й элемент x получит номер $2n$, каждый n-й элемент y — номер $2n+1$. (Коль скоро мы ввели арифметические операции над натуральными числами, построить соответствующий терм-биекцию не составит труда.)

- Если $|x| \leqslant \aleph_0$, $|y| = \aleph_0$, $x \cap y = \varnothing$, то $|x \cup y| = \aleph_0$. Иначе говоря, $|x| \leqslant \aleph_0 \Rightarrow |x| + \aleph_0 = \aleph_0$.

  Действительно, биекция между y и ω будет инъекцией из ω в $x \cup y$, откуда $|x| + \aleph_0 \geqslant \aleph_0$. С другой стороны, т. к. существует инъекция из x в ω, то существует и инъекция из $x \cup y$ в $\omega \cup y$ (без ограничения общности считаем, что $y \cap \omega = \varnothing$). Отсюда $|x| + \aleph_0 \leqslant \aleph_0$ и окончательно $|x| + \aleph_0 = \aleph_0$.

- Если $|x| \geqslant \aleph_0$, то $|x| + \aleph_0 = |x|$. Вместе с предыдущим утверждением это даёт

  $$|x| + \aleph_0 = \max(|x|, \aleph_0)$$

  для произвольного x, сравнимого по мощности с $\aleph_0$. (Далее мы увидим, что это утверждение — лишь частный случай некоторой общей формулы.)

  Упр. 65. Докажите, что если $|x| \geqslant \aleph_0$, то $|x| + \aleph_0 = |x|$.

- Если x и y — счётные, то $x \times y$ — также счётное, т. е. ${\aleph_0}^2 = \aleph_0$. Действительно, пусть элементы x и y занумерованы. Тогда пары элементов счётных множеств можно занумеровать, например, по диагональной схеме:

1	3	6	10	$\cdots$
2	5	9	$\cdots$	
4	8	$\cdots$		
7	$\cdots$			
$\cdots$				

При этом пара элементов с индексами (i, j) получит уникальный номер по нумерующей функции Кантора:

$$\frac{(i+j-1)(i+j-2)}{2} + j,$$

откуда $|x| = |y| = \aleph_0 \Rightarrow |x \times y| = \aleph_0$.

- Счётными также являются множества троек, четвёрок и любых конечных кортежей элементов счётных множеств, иначе говоря, ${\aleph_0}^n = \aleph_0$ для любого натурального $n \geqslant 1$: по индукции ${\aleph_0}^2 = \aleph_0$, ${\aleph_0}^{n+1} = {\aleph_0}^n \aleph_0 = \aleph_0 \aleph_0 = \aleph_0$.

- Если $x \neq \varnothing$ и $|x| \leqslant \aleph_0$, то $|x|\aleph_0 = \aleph_0$ (если одно из множеств конечно или счётно, а другое — счётно, то их декартово произведение является счётным множеством). Действительно, $x \neq \neq \varnothing \Rightarrow \exists a(a \in x \,\&\, \{a\} \times y \subseteq x \times y)$, откуда $\aleph_0 \leqslant |x|\aleph_0$. Но т. к. $|x| \leqslant \aleph_0$, то существуют инъекции из x в ω и из $x \times \omega$ в $\omega \times \omega$, т. е. $|x|\aleph_0 \leqslant \aleph_0$, откуда по теореме 39 $|x|\aleph_0 = \aleph_0$.

- Каждый элемент множества $\mathbb{Z}$ целых чисел взаимно однозначно соответствует элементу множества $\{0, 1\} \times \omega$, т. е. множества пар вида «знак, абсолютное значение», где нуль в качестве первого компонента пары означает знак «+», а единица — знак «−». По доказанному $|\mathbb{Z}| = \aleph_0$.

- Каждый элемент множества $\mathbb{Q}$ рациональных чисел взаимно однозначно соответствует элементу множества

$$\{t \in \mathbb{Z} \times \omega \mid \text{«}\tfrac{\mathrm{pr}_1(t)}{\mathrm{pr}_2(t)} \text{ — несократимая дробь»}\}.$$

(Выражение в кавычках следует, конечно, заменить на соответствующую формулу. Введённых нами конструкций уже достаточно для того, чтобы эту формулу построить.) Это — подмножество $\mathbb{Z} \times \omega$, откуда $|\mathbb{Q}| \leqslant \aleph_0$. С другой стороны, множество целых рациональных чисел (дробей с единицей в знаменателе) является подмножеством $\mathbb{Q}$ и счётно, откуда $|\mathbb{Q}| \geqslant \aleph_0$ и окончательно $|\mathbb{Q}| = \aleph_0$.

- Рассмотрим операцию «звёздочка Клини», определённую на с. 112. Если $|x| = \aleph_0$, то $|x^*| = \aleph_0$, т. е.

$$\aleph_0 + {\aleph_0}^2 + \ldots + {\aleph_0}^n + \ldots = \aleph_0.$$

Каждое слагаемое этой суммы счётно, и мы имеем счётное количество счётных множеств, элементы которых можно занумеровать по диагональной схеме.

Заметим, что конечность каждого упорядоченного набора, входящего в терм x^*, существенна. Множество всех конечных и бесконечных наборов натуральных чисел имеет мощность, не меньшую $\mathfrak{P}(\omega)$, т. е. несчётно.

Упр. 66. Пусть $|x| \leqslant \aleph_0$. Докажите, что $|x^*| = \aleph_0$. (Результат упражнения говорит о том, что, коль скоро мы используем не более чем счётные алфавиты, множества всех мыслимых книг, компьютерных программ, логических формул и т. п. являются не более чем счётными множествами.)

Упр. 67. Докажите, что множество алгебраических чисел $\mathbb{A}$, определяемое как множество корней многочленов с рациональными коэффициентами, счётно.

Упр. 68. [7]. Докажите, что любое семейство непересекающихся интервалов на прямой конечно или счётно. Указание: каждый интервал содержит по крайней мере одну рациональную точку.

Упр. 69. [7]. Докажите, что множество точек строгого локального максимума любой функции действительного аргумента конечно или счётно.

Упр. 70. [7]. Докажите, что множество точек разрыва любой монотонной функции конечно или счётно.

5. Мощность континуума. Рассмотрим множество бесконеч-

ных двоичных дробей вида

$$d_0\left(\frac{1}{2}\right)^1 + d_1\left(\frac{1}{2}\right)^2 + d_2\left(\frac{1}{2}\right)^3 + \ldots \quad (d_i \in \{0,1\}).$$

Любое действительное число из полуинтервала $[0,1)$ можно представить в виде такой бесконечной двоичной дроби, причём числа вида $m/2^n$ представимы неоднозначно: например, число $1/2$ может быть представлено двоичной дробью как $0,1$, а может — как $0,01111\ldots$ Если число представимо двоичной дробью неоднозначно, то примем в качестве канонического такое представление, которое не содержит единицу в периоде дроби.

Каждая двоичная дробь рассматриваемого вида однозначно соответствует подмножеству натуральных чисел, для которых $d_i = 1$, а всё множество действительных чисел на полуинтервале $[0,1)$ однозначно соответствует множеству своих канонических представлений

$$c = \{x \in \mathfrak{P}(\omega) \mid \forall u(u \in x \Rightarrow \exists v(v \notin x \,\&\, v > u))\}.$$

Упр. 71. Представьте число $1/3$ в виде двоичной дроби и в виде подмножества натуральных чисел. Ответ: $0,01010101\ldots$, $\{1,3,5,7\ldots\}$.

Множество c представляет собой подмножество $\mathfrak{P}(\omega)$, из которого отброшены «неправильные» двоичные представления чисел вида $m/2^n$, которых счётное множество. С учётом доказанного выше (см. упр. 65) имеем

$$|c| + \aleph_0 = |\mathfrak{P}(\omega)| = \max(|c|, \aleph_0).$$

Т. к. по теореме Кантора $|\mathfrak{P}(\omega)| = 2^{\aleph_0} > \aleph_0$, окончательно получаем $|c| = 2^{\aleph_0}$. Про множество, равномощное определённому нами множеству c, говорят, что оно *имеет мощность континуума*, и пишут $|x| = \mathfrak{c}$, где $\mathfrak{c}$ есть традиционное сокращающее обозначение для $2^{\aleph_0}$.

Выведем несколько свойств $\mathfrak{c}$.

Легко проверить, что делению на два в двоичном представлении соответствует сдвиг всех цифр двоичного представления вправо на один разряд. Иначе говоря, бинарное отношение

$$\{t \in \mathfrak{P}(\omega) \times \mathfrak{P}(\omega) \mid \forall n(n \in \mathrm{pr}_1(t) \Leftrightarrow n+1 \in \mathrm{pr}_2(t))\}$$

задаёт функцию $f(x) = x/2$. Если число x принадлежит полуинтервалу $[0, 1/2)$, то первая цифра в его двоичном представлении всегда равна нулю и существует единственный y из полуинтервала $[0, 1)$ такой, что $y/2 = x$. Таким образом, деление на 2 устанавливает биекцию между полуинтервалами $[0, 1)$ и $[0, 1/2)$, каждый из которых имеет мощность $\mathfrak{c}$.

Если $x < 1/2^n$, то добавление к x числа $\left(\frac{1}{2}\right)^n$ есть попросту выставление единицы в $(n-1)$-м разряде двоичного представления, т. е. $x + \left(\frac{1}{2}\right)^n \rightleftharpoons x \cup \{n-1\}$. Операция прибавления $1/2$ устанавливает биекцию между полуинтервалами $[0, 1/2)$ и $[1/2, 1)$, каждый из которых имеет мощность континуума, откуда

$$\mathfrak{c} + \mathfrak{c} = \mathfrak{c}.$$

С точки зрения двоичных представлений доказательство этого факта выглядит следующим образом: возьмём две копии полуинтервала $[0, 1)$, сдвинем двоичные представления всех чисел обоих полуинтервалов вправо на один разряд, добавив в начало представлений всех чисел из первой копии нуль, всех чисел из второй копии — единицу, тем самым получим биекцию с полуинтервалом $[0, 1)$.

Рассуждая схожим образом, мы можем разбить c на три континуальных множества

$$\left[0, \frac{1}{2}\right), \ \left[\frac{1}{2}, \frac{3}{4}\right), \ \left[\frac{3}{4}, 1\right),$$

а также на любое конечное и даже счётное множество континуальных множеств

$$\left[0, \frac{1}{2}\right), \ \left[\frac{1}{2}, \frac{3}{4}\right), \ \left[\frac{3}{4}, \frac{7}{8}\right), \ldots, \ \left[\frac{2^n-1}{2^n}, \frac{2^{n+1}-1}{2^{n+1}}\right) \ldots,$$

откуда имеем

$$|x| \leqslant \aleph_0 \Rightarrow |x|\mathfrak{c} = \mathfrak{c}.$$

Упр. 72. Как выглядят эти разбиения с точки зрения представления чисел в виде бесконечных двоичных дробей?

Теперь определим множество действительных чисел как

$$\mathbb{R} = \{0,1\} \times \omega \times c,$$

т. е. как множество троек вида «знак, целое значение, дробная часть». По доказанному

$$|\mathbb{R}| = |\{0,1\} \times \omega||c| = \aleph_0\mathfrak{c} = \mathfrak{c}.$$

Итак, мощность множества $\mathbb{R}$ всех действительных чисел равна мощности множества действительных чисел на полуинтервале $[0,1)$ и равна $2^{\aleph_0}$.

Определив множество $\mathbb{R}$, мы достигли той точки в изложении, с которой обычно начинается содержание учебников по математическому анализу (традиционные учебники, впрочем, определяют действительные числа в виде бесконечных десятичных, а не бесконечных двоичных дробей, но это не меняет сути). Дальнейшие задачи заключаются в определении порядка на действительных числах (предиката $<$), арифметических операций, изучении свойств различных подмножеств $\mathbb{R}$ и функций действительного переменного.

Упр. 73. Не ссылаясь на теорему 39, докажите, что отрезок $\{x \in \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\}$ равномощен полуинтервалу $\{x \in \mathbb{R} \mid 0 \leqslant x < 1\}$.

Решение: выделим на отрезке $r = \{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\}$ счётное подмножество

$$c = \{x \in r \mid \exists n(n \in \omega \,\&\, x = 1/2^n)\}.$$

Искомая биекция может быть представлена в виде $h \cup h'$, где

$$h = \{t \in r \times r \mid \mathrm{pr}_1(t) \in r \setminus c \,\&\, \mathrm{pr}_1(t) = \mathrm{pr}_2(t)\},$$
$$h' = \{t \in r \times r \mid \exists n(n \in \omega \,\&\, \mathrm{pr}_1(t) = 1/2^n \,\&\, \mathrm{pr}_2(t) = 1/2^{n+1})\}.$$

Упр. 74. Докажите, что любое подмножество $\mathbb{R}$, содержащее интервал, имеет мощность $\mathfrak{c}$.

Как мы уже убедились, числовой интервал равномощен всей числовой прямой. Несколько более неожиданным может показаться тот факт, что, на самом деле, плоскость, а также трёхмерное и даже $\aleph_0$-мерное пространство имеют мощность, равную $\mathfrak{c}$.

Теорема 47. $\forall x(|x| \leqslant \aleph_0 \Rightarrow \mathfrak{c}^{|x|} = \mathfrak{c})$.

$\lhd$Начнём с доказательства утверждения $\mathfrak{c}^2 = \mathfrak{c}\mathfrak{c} = \mathfrak{c}$.

Действительно: каждой паре двоичных представлений чисел из полуинтервала $[0, 1)$

$$\begin{array}{ll} x_0, x_1, x_2 \ldots & (x_i \in \{0, 1\}) \\ y_0, y_1, y_2 \ldots & (y_i \in \{0, 1\}) \end{array}$$

можно поставить в соответствие уникальную для данной пары последовательность

$$x_0, y_0, x_1, y_1, x_2, y_2 \ldots,$$

чётные цифры которой берутся из цифр числа x, нечётные — из цифр числа y. Указанное отношение определяет инъекцию $f : [0, 1) \times [0, 1) \to \mathfrak{P}(\omega)$, что вместе с $\mathfrak{c}^2 \geqslant \mathfrak{c}$ доказывает утверждение $\mathfrak{c}^2 = \mathfrak{c}$.

Аналогичным образом в одну двоичную последовательность можно «упаковать» тройки и любые конечные кортежи действительных чисел из $[0, 1)$, в случае же, когда чисел — счётное множество, следует воспользоваться диагональной схемой

$$\begin{array}{l} z_0, z_2, z_5, z_9 \ldots \\ z_1, z_4, z_8, z_{13} \ldots \\ z_3, z_7, z_{12} \ldots \\ z_6, z_{11} \ldots \\ \ldots \rhd \end{array}$$

Мы могли бы вывести «арифметические» свойства $\mathfrak{c}$, аналогичные тем, что мы вывели для $\aleph_0$, но не будем этого делать, т. к.

далее получим некоторые общие формулы, касающиеся бесконечных мощностей.

Упр. 75. [7]. Докажите, что любая пространственная фигура, содержащая отрезок кривой, имеет мощность континуума.

Упр. 76. [7]. Докажите, что множество всех непрерывных функций $f : \mathbb{R} \to \mathbb{R}$ имеет мощность континуума. Указание: непрерывная функция полностью задаётся своими значениями в рациональных точках.

Упр. 77. [7]. Докажите, что множество всех монотонных функций имеет мощность континуума. Указание: см. упр. 70.

6. Сформулируем и докажем ещё одну, зависящую от аксиомы выбора, теорему, касающуюся свойств операций над мощностями.

°**Теорема 48** (Кёнига). $|x| + |y| = |u||v| \Rightarrow |x| \geqslant |u| \vee |y| \geqslant |v|$.

$\lhd$Действительно: пусть $x \cap y = \varnothing$, $\neg|x| \geqslant |u| \& \neg|y| \geqslant |v|$, и существует биекция $f : u \times v \leftrightarrow x \cup y$. Разобьём f на две части f_x и f_y, такие, что $\mathrm{Pr}_2(f_x) = x$ и $\mathrm{Pr}_2(f_y) = y$ ($f_x \cup f_y = f$, $f_x \cap f_y = \varnothing$). Из условий следует, что существует $u_0 \in u$, такой, что $\forall t(u_0, t) \notin \mathrm{Pr}_1(f_x)$. Предположив обратное, замечаем, что бинарное отношение

$$r_x = \{(a, b) \in u \times x \mid \exists t(((a, t), b) \in f_x)\}$$

является всюдуопределённым на u. Но в таком случае, если $f_c : \mathfrak{P}(u) \to u$ — функция выбора такая, что $f_c(h) \in h$, то

$$r'_x = \{(a, b) \in u \times x \mid b = f_c(\{t \mid (a, t) \in r_x\})\}$$

есть инъекция из u в x, т. е. $|u| \leqslant |x|$, что противоречит условию. Аналогичным образом, существует $v_0 \in v$, такой, что $\forall t(t, v_0) \notin \mathrm{Pr}_1(f_y)$. Но это значит, что $(u_0, v_0) \notin \mathrm{Pr}_1(f_x)$ & & $(u_0, v_0) \notin \mathrm{Pr}_1(f_y)$, откуда $(u_0, v_0) \notin \mathrm{Pr}_1(f)$. Но f — биекция между $u \times v$ и $x \cup y$, и должна быть определена для любых пар элементов множеств $u \times v$. Противоречие.$\rhd$

Упр. 78. Докажите, что если а) квадрат, б) отрезок разбит на две части, то по крайней мере одна из них имеет мощность континуума.

7. Континуум-гипотеза. Ещё в начале своих исследований (1877) Кантор высказал предположение (получившее в дальнейшем название *континуум-гипотезы*, сокращённо CH) о том, что $\mathfrak{c}$

есть ближайшая к $\aleph_0$ бесконечная мощность, т. е. не существует x такого, что $\aleph_0 < |x| < \mathfrak{c}$, но доказательство этого предположения Кантор предоставить не смог. Длительное время поиск доказательства или опровержения континуум-гипотезы оставался нерешённой проблемой для математиков. Эта задача стала первой из двадцати трёх знаменитых математических проблем, о которых Д. Гильберт доложил на II Международном Конгрессе математиков в Париже в 1900 году, поэтому континуум-гипотеза известна также как «первая проблема Гильберта».

В 1940 году Курт Гёдель доказал в предположении непротиворечивости системы аксиом ZF, что, исходя из аксиом теории множеств вместе с аксиомой выбора, континуум-гипотезу нельзя опровергнуть (т. е. если система аксиом ZFC имеет модель, то модель имеет также система утверждений ZFC + CH). Почти четверть века спустя, в 1963 году, Пол Коэн доказал (также в предположении непротиворечивости ZF), что континуум-гипотезу из тех же аксиом нельзя вывести (т. е. если система аксиом ZFC имеет модель, то модель имеет также система утверждений ZFC + $\neg$CH). Таким образом, континуум-гипотеза не зависит от аксиом ZF.

Обобщённая континуум-гипотеза утверждает, что для любого бесконечного множества x не существует такого z, что $|x| < |z| < |\mathfrak{P}(x)|$. Обобщённая континуум-гипотеза также не противоречит аксиоматике Цермело–Френкеля, и, кроме того, из неё следует аксиома выбора.

Доказательства этих утверждений изложены, например, в [9] и [12].

8. Парадокс Сколема. С теоремой 40 Кантора связано рассуждение, именуемое «парадоксом Сколема». В отличие от уже изученных нами парадоксов Рассела (см. с. 82) и Кантора (см. с. 123), где при помощи логически верных выводов мы обнаруживали противоречие, «замаскированное» в исходных посылках, «противоречие» парадокса Сколема возникает от ошибки в рассуждениях, и аккуратное рассмотрение вопроса показывает, что

собственно никакого парадокса нет. Тем не менее рассмотрение парадокса Сколема имеет большую дидактическую ценность.

Если система аксиом любой аксиоматической теории множеств непротиворечива, то она (см. теоремы 24 Гёделя и 25 Лёвенгейма–Сколема) имеет модель, и, более того, эта модель может быть построена на натуральных числах. Т. е. всего лишь счётное множество M объектов (каждый из которых будет соответствовать уникальному множеству) требуется для того, чтобы подобрать значение предиката $x \in y$ для каждой пары объектов x, y, полностью удовлетворяющее системам аксиом ZF или ZFC. В такой ситуации для каждого объекта модели y лишь конечное или счётное количество объектов (больше просто нет в предметной области) могут входить в отношение $\ldots \in y$. Фиксируем такую модель $\mathfrak{M}$ со счётным M в качестве предметной области.

В силу доказанных теорем вне зависимости от принятой модели в ZF выводимо, например, существование терма $\mathfrak{P}(\omega)$, мощность которого несчётна. Но в счётной модели любое множество вынуждено быть не более чем счётным — противоречие?

Проведём рассуждение аккуратно. Факт $\mathrm{ZF} \vdash \exists x(x = \mathfrak{P}(\omega))$ означает, что существует такой объект $c \in M$, что формула первого порядка, соответствующая выражению $x = \mathfrak{P}(\omega)$, истинна в модели $\mathfrak{M}$ на оценке, при которой индивидной переменной x поставлен в соответствие объект c. Теорема Кантора утверждает, что x — несчётно, что по определению значит

$$\mathrm{ZF} \vdash \neg\exists f(f : \mathfrak{P}(\omega) \leftrightarrow \omega)$$

(все сокращающие обозначения, напомним, заменяют вполне определённую формулу на языке первого порядка, которую не приводим полностью лишь в силу её громоздкости). Но это значит лишь то, что *среди элементов* M нет такого f, что в модели $\mathfrak{M}$ оно удовлетворяло бы четырём свойствам биекции между $\mathfrak{P}(\omega)$ и ω. При этом не важно, что в отношение принадлежности с объектом из M, соответствующим терму $\mathfrak{P}(\omega)$, может входить не более чем счётное

число объектов *из* M, — важно то, что *среди объектов* M не существует f, осуществляющего необходимую биекцию.

Рассуждение «если модель счётна, то в отношение $\in$ с любым объектом может входить не более чем счётное число объектов» есть рассуждение *внешнее* по отношению к изучаемой аксиоматической теории и никакой формуле в этой теории не соответствует. С внешней точки зрения на теорию ZF «множество всех *множеств*» (второй раз слово «множество» здесь обозначает лишь некоторый объект предметной области ZF) может существовать и даже быть счётным, что никак не связано (и потому не может противоречить) с выводимыми в ZF формулами.

§ 2.6. Упорядоченные множества

1. *Бинарным отношением на множестве* x называется такое r, что $r \subseteq x \times x$. Помимо уже рассмотренных в § 2.4 четырёх стандартных свойств бинарного отношения на множествах x и y, для отношения на одном множестве рассматривают, в частности, следующие:

1) *транзитивность*: $\forall a \forall b \forall c((a,b) \in r \,\&\, (b,c) \in r \Rightarrow (a,c) \in r)$ (если пары (a,b) и (b,c) входят в отношение r, то пара (a,c) также входит в отношение r);

2) *симметричность*: $\forall a \forall b((a,b) \in r \Rightarrow (b,a) \in r)$ (если пара (a,b) входит в отношение r, то пара (b,a) тоже обязана входить в отношение r);

3) *антисимметричность*: $\forall a \forall b((a,b) \in r \,\&\, (b,a) \in r \Rightarrow a = b)$, или, что эквивалентно, $\forall a \forall b(a \neq b \,\&\, (a,b) \in r \Rightarrow (b,a) \notin r)$ (если $a \neq b$ и в r имеется пара (a,b), то в r не может быть пары (b,a));

4) *рефлексивность*: $\forall a(a \in x \Rightarrow (a,a) \in r)$ (для любого элемента a из x пара (a,a) должна входить в r);

5) *антирефлексивность*: $\forall a(a,a) \notin r$ (в r не существует пар вида (a,a));

6) *линейность*: $\forall a \forall b(a \in x \,\&\, b \in x \,\&\, a \neq b \Rightarrow (a,b) \in r \vee (b,a) \in r)$ (любая пара нетождественных элементов a и b из множества x должна входить в отношение — либо как (a,b), либо как (b,a)).

2. Бинарное отношение, удовлетворяющее условиям рефлексивности, симметричности и транзитивности, называется *отношением эквивалентности*. Если r — отношение эквивалентности, то часто вместо $(a,b) \in r$ пишут $a \underset{r}{\simeq} b$ или просто $a \simeq b$, полагая множество r заданным. *Классом эквивалентности* $[a]_r$ (или просто $[a]$) элемента a по отношению эквивалентности r называют множество, состоящее из тех и только тех элементов, которые входят с a в отношение эквивалентности, т. е.

$$[a]_r \rightleftharpoons \{b \in x \mid (b,a) \in r\}.$$

Таким образом, формулы $b \simeq a$ и $b \in [a]$ эквивалентны.

Пусть дано множество x с введённым на нём отношением эквивалентности r. *Фактормножеством* для x по отношению r (обозначается x/r) называется множество всех классов эквивалентности на x, т. е.

$$x/r \rightleftharpoons \{u \in \mathfrak{P}(x) \mid \exists a(a \in x \,\&\, u = [a]_r)\}.$$

Теорема 49. *Справедливы следующие утверждения:*

1) *Если множество x разбито в объединение непересекающихся множеств, т. е. если дано множество $u \subseteq \mathfrak{P}(x)$, такое, что а) $\bigcup u = x$ и б) $\forall a \forall b(a \in u \,\&\, b \in u \Rightarrow a \cap b = \varnothing \vee a = b)$, то отношение «лежать в одном множестве» $\exists v(v \in u \,\&\, a \in v \,\&\, b \in v)$ является отношением эквивалентности.*

2) *Если дано отношение эквивалентности r на множестве x, то фактормножество x/r является разбиением множества x (т. е. удовлетворяет условиям а) и б)).*

◁Первое утверждение доказывается тривиально. Например, если дано разбиение u и $\exists v(v \in u \,\&\, (a \in v \,\&\, b \in v) \,\&\, (b \in v \,\&\, c \in v))$, то из этого сразу следует $\exists v(v \in u \,\&\, a \in v \,\&\, c \in v)$, что доказывает выполнение условия транзитивности. Рефлексивность и симметричность доказываются аналогично.

Докажем второе утверждение теоремы.

Условие а) $\bigcup(x/r) = x$ эквивалентно утверждению $\forall a(a \in x \Rightarrow \Rightarrow \exists e(e \in x/r \,\&\, a \in e))$, которое мы и будем доказывать. В силу рефлексивности $\forall a(a \in x \Rightarrow (a \in [a]))$, откуда

$$\forall a(a \in x \Rightarrow \exists e(e = [a] \,\&\, e \in x/r \,\&\, a \in e)),$$

откуда следует требуемое.

Условие б) эквивалентно утверждению

$$\forall a \forall b(a \in x \,\&\, b \in x \Rightarrow [a] \cap [b] = \varnothing \vee [a] = [b]),$$

что в свою очередь эквивалентно

$$\forall a \forall b(a \in x \,\&\, b \in x \,\&\, [a] \cap [b] \neq \varnothing \Rightarrow [a] = [b]).$$

Докажем последнее утверждение. $[a] \cap [b] \neq \varnothing \sim \exists z(z \simeq a \,\&\, \&\, z \simeq b)$. В силу симметричности и транзитивности имеем $[a] \cap [b] \neq \neq \varnothing \Rightarrow a \simeq b$. Отсюда $\forall t(t \in [a] \Rightarrow t \in [b])$ (в силу $t \simeq a \,\&\, a \simeq b \Rightarrow \Rightarrow t \simeq b$), и наоборот, $\forall t(t \in [b] \Rightarrow t \in [a])$, откуда $[a] = [b]$.▷

Упр. 79. [7]. Пусть r_1 и r_2 задают на множестве x отношение эквивалентности. Будут ли множества 1) $r_1 \cup r_2$, 2) $r_1 \cap r_2$, 3) $r_1 \setminus r_2$ задавать отношения эквивалентности на множестве x?

3. Множество называется *(частично) (нестрого) упорядоченным*, если для его элементов введено бинарное отношение, обладающее свойствами транзитивности, рефлексивности и антисимметричности. Слова «частично» и «нестрого» часто для краткости опускают. Само бинарное отношение при этом называют *(частичным) (нестрогим) порядком*. Если вместо свойства рефлексивности бинарное отношение обладает свойством антирефлексивности,

то говорят, что оно задаёт *(частичный) строгий* порядок. Если бинарное отношение строгого или нестрогого порядка обладает также свойством линейности, то такой порядок называют *линейным* (в отличие от частичного).

Если r — отношение нестрогого порядка, то часто вместо $(a,b) \in \in r$ пишут $a \leqslant b$, полагая множество r заданным; для строгого порядка применяют обозначение $a < b$. Записи $a \geqslant b$ и $a > b$ обозначают соответственно случаи $b \leqslant a$ и $b < a$. Для всякого отношения нестрогого порядка r можно построить соответствующее ему отношение строгого порядка $r \setminus \mathrm{id}_x$ (где, напомним, $\mathrm{id}_x = \{(u,v) \in \in x \times x \mid u = v\}$), такое, что $a < b \sim a \leqslant b \,\&\, a \neq b$. Аналогичным образом для всякого строгого порядка r' можно получить соответствующий ему нестрогий порядок $r' \cup \mathrm{id}_x$, удовлетворяющий условию $a \leqslant b \sim a < b \vee a = b$. По этой причине не имеет смысла изучать свойства строгих и нестрогих порядков по отдельности: в дальнейшем все упорядочения будут по умолчанию считаться нестрогими, и для порядка, обозначаемого знаком $\leqslant$, знак $<$ будет рассматриваться как соответствующий ему строгий порядок (иначе говоря, запись $a < b$ будет рассматриваться как сокращающее обозначение для $a \leqslant b \,\&\, a \neq b$, или, что то же, $(a,b) \in r \setminus \mathrm{id}_x$).

Когда порядок на x не является линейным (не выполняется условие линейности), в x не исключается существование пар *несравнимых* элементов a, b, таких, что ни $a \leqslant b$, ни $b \leqslant a$ не имеет места. Заметим, что в этом случае, хотя $a \leqslant b \Rightarrow \neg b < a$ и $b < \\ < a \Rightarrow \neg a \leqslant b$, т. е. из *утверждения* отношений $<$, $\leqslant$ следует отрицание отношений $\geqslant$, $>$, из *отрицания* любого из этих отношений не следует никакого утверждения. Так, если отрицается $a < b$, то может иметь место как случай $a \geqslant b$, так и случай, когда a и b несравнимы. Поэтому следует проявлять осторожность и понимать, что в случае частичного порядка среди утверждений «не меньше», «больше или равно», «не меньше или равно», «больше» *нет эквивалентных по определению*.

Рассмотрим примеры.

- Всякое множество x можно частично упорядочить отноше-

нием id_x: бинарное отношение тождества представляет собой частичный порядок, в котором любые два неравных элемента несравнимы.

- Множества натуральных, целых, рациональных, действительных чисел линейно упорядочены обычным отношением $\leqslant$.

- На множестве функций с действительными аргументами и значениями, определённых на $v \subseteq \mathbb{R}$, можно ввести частичный (не линейный) порядок условием «$f \leqslant g$, если и только если $\forall x(x \in v \Rightarrow f(x) \leqslant g(x))$».

- На множестве натуральных чисел можно ввести частичный порядок по условию «$a \leqslant b$, если и только если b делится без остатка на a» (проверьте транзитивность, антисимметричность и рефлексивность).

- Множество $\mathfrak{P}(x)$ всех подмножеств некоторого данного множества может быть частично упорядочено по условию «$a \leqslant b$ тогда и только тогда, когда $a \subseteq b$» (соответствующий строгий порядок задаётся соотношением $a \subset b$).

- Если на множестве x определён порядок r и $s \subseteq x$, то множество $(s \times s) \cap r$ будет порядком на s (будем называть этот порядок *индуцированным*).

- Если на непересекающихся множествах x и y определены частичные порядки, то на множестве $x \cup y$ частичный порядок может быть введён, например, следующими способами:

  – элементы внутри множеств x и y сравниваются как раньше, любой элемент множества x не сравним с любым элементом множества y (такой порядок, если множества x и y непустые, будет необходимо частичным);

– элементы внутри множеств x и y сравниваются как раньше, любой элемент множества x считается меньшим любого из элементов множества y. Если на x и y введены линейные порядки, то такой порядок также будет линейным. Множество $x \cup y$, упорядоченное таким образом, будет называться *суммой упорядоченных множеств x и y* (заметим, что эта сумма некоммутативна: $x + y \neq y + x$).

- Если на множествах x и y определены частичные порядки, то на множестве $x \times y$ частичный порядок может быть введён, например, следующими способами:

  – $(a, b) \leqslant (c, d)$ тогда и только тогда, когда $a \leqslant c \,\&\, b \leqslant d$, такой порядок называется *покоординатным сравнением* и, если множества x и y непустые, является необходимо частичным;

  – $(a, b) \leqslant (c, d)$ тогда и только тогда, когда $b \leqslant d \vee (b = d \,\&\, a \leqslant c)$. Иначе говоря, сначала сравниваются вторые компоненты пар, и, если, например, $b \leqslant d$, то считается $(a, b) \leqslant (c, d)$. Если же вторые компоненты пар совпадают, то сравниваются первые компоненты. Если на x и y введены линейные порядки, то такой порядок также будет линейным. Множество $x \times y$, упорядоченное таким образом, будет называться *произведением упорядоченных множеств x и y*.

- Пусть x — непустое множество с линейным порядком. Назовём это множество *алфавитом*, его элементы — *символами*, а линейный порядок на этих элементах — *алфавитным порядком* (например, на буквах русского алфавита установлен порядок а $\leqslant$ б $\leqslant$ в $\leqslant \ldots \leqslant$ я). Тогда элементами терма x^* (звёздочки Клини, см. определение на с. 112) являются упорядоченные наборы символов (строки). Для любого линейно упорядоченного множества x множество x^* может быть линейно упорядочено, например, такими способами:

– 1) Если строка a является началом строки b, считаем $a \leqslant b$ (например, если x — кириллический алфавит, то абажур $\leqslant$ абажуродержатель). 2) Если ни одна из строк не является началом другой, то отношение между строками определяется первой буквой, в которой строки различаются (ракета $\leqslant$ рама, т. к. к $\leqslant$ м). Этот (разумеется, знакомый читателю) линейный порядок на множестве x^* называется *словарным*, или *лексикографическим*.

– Если множество x — конечное и содержит p элементов, то можно интерпретировать строки из x^* как натуральные числа в p-ичной системе счисления, с обычным для натуральных чисел линейным порядком.

4. Пусть x — частично упорядоченное множество с отношением порядка $\leqslant$. Тогда элемент $a \in x$ называется

- минимальным, если $\forall b(b \in x \Rightarrow \neg a > b)$;
- наименьшим, если $\forall b(b \in x \Rightarrow a \leqslant b)$;
- максимальным, если $\forall b(b \in x \Rightarrow \neg b > a)$;
- наибольшим, если $\forall b(b \in x \Rightarrow b \leqslant a)$.

Сказанное выше о разнице между утверждениями $a \leqslant b$ и $\neg a > b$ поясняет различие между понятиями минимального и наименьшего, максимального и наибольшего элементов. Следующее упражнение предлагает доказать несколько простых утверждений, связанных с этими понятиями.

Упр. 80. Докажите следующие утверждения: 1) всякий наименьший элемент является минимальным, а наибольший — максимальным; 2) если в множестве существует наименьший элемент, то он единствен, то же справедливо для наибольшего элемента; 3) не исключается случай, когда множество имеет несколько минимальных и/или несколько максимальных элементов; 4) если в множестве имеется несколько минимальных элементов, то в нём не существует наименьшего элемента, если несколько максимальных — не существует наибольшего; 5) любые

два минимальных элемента несравнимы, и то же справедливо для двух максимальных элементов; 6) если порядок на множестве линеен, то его минимальный элемент, если существует, является наименьшим, а максимальный, если существует, — наибольшим.

Рассмотрим примеры.

- В полуинтервале $[0, 1)$ минимальный, он же наименьший, элемент — 0, максимального элемента не существует.

- В множестве натуральных чисел, больших единицы, упорядоченных отношением делимости, имеется счётно-бесконечное множество минимальных элементов (простые числа) и нет наименьшего и максимальных элементов.

- В множестве $\mathfrak{P}(x)$, частично упорядоченном по включению, не всякая пара элементов сравнима. Тем не менее $\varnothing$ — наименьший, а x — наибольший элемент этого множества.

- Пусть конечное множество x состоит из n элементов. Тогда в множестве $\mathfrak{P}(x) \setminus \{x\} \setminus \{\varnothing\}$, частично упорядоченном по включению, имеется n минимальных элементов (все элементы $\{t\}$, $t \in x$) и столько же максимальных (все элементы $x \setminus \{t\}$, где $t \in x$).

5. Пусть x — частично упорядоченное множество с отношением порядка $\leqslant$, s — подмножество x с индуцированным на нём порядком, a — элемент x. Тогда a называют

- *нижней гранью* s, если $\forall b(b \in s \Rightarrow a \leqslant b)$;

- *наибольшей нижней гранью*, или *infimum* s, и пишут $a = \inf(s)$, если a есть наибольший элемент множества нижних граней s;

- *максимальной нижней гранью* s, если a есть максимальный элемент множества нижних граней s.

Аналогичным образом определяются понятия *верхней грани*, *наименьшей верхней грани* (*supremum*, $\sup(s)$) и *минимальной верхней грани* множества.

- Наименьшей верхней гранью (supremum) полуинтервала $[0,1)$ в множестве $\mathbb{R}$ является 1.

- Рассмотрим множество конечных подмножеств натуральных чисел, к элементам которого добавлено также множество целых чисел $\mathbb{Z}$ и множество положительных действительных чисел $\mathbb{R}_+$. Упорядочим это множество по включению. В этом множестве как $\mathbb{Z}$, так и $\mathbb{R}_+$ являются минимальными верхними гранями множества конечных подмножеств натуральных чисел, но ни одно из них не является наименьшей верхней гранью, т. к. $\mathbb{Z}$ и $\mathbb{R}_+$ не сравнимы по включению.

6. Изоморфизмы порядков. Два частично упорядоченных множества x и y называются *изоморфными*, если существует такая биекция $f : x \leftrightarrow y$, что

$$f(a) < f(b) \Leftrightarrow a < b.$$

Разумеется, для того чтобы множества x и y были изоморфными, необходимо (но не достаточно), чтобы их мощности были равны.

Приведём несколько примеров.

- Множества всех действительных чисел и действительных чисел на интервале $(0,1)$ изоморфны. Изоморфизм $f : (0,1) \leftrightarrow \mathbb{R}$ задаёт, например, отображение

$$f(x) = \begin{cases} 1 - \frac{1}{2x}, \text{ если } 0 < x \leqslant \frac{1}{2}, \\ \frac{1}{2(1-x)} - 1, \text{ если } \frac{1}{2} \leqslant x < 1. \end{cases}$$

  Эта же функция задаёт изоморфизм между рациональными числами интервала $(0,1)$ и множеством $\mathbb{Q}$ всех рациональных чисел (т. к. переводит рациональные числа в рациональные).

- Отрезок $[0,1]$ не изоморфен числовой прямой, т. к. у отрезка есть наибольший и наименьший элементы, а у числовой прямой они отсутствуют (изоморфизм должен переводить наибольшие элементы в наибольшие).

- Счётные множества ω, $\mathbb{Z}$ и $\mathbb{Q}$ (порядки обычные) попарно неизоморфны. Действительно, у ω есть наименьший элемент, а у $\mathbb{Z}$ и $\mathbb{Q}$ его нет. Предположим, что имеется изоморфизм f между $\mathbb{Z}$ и $\mathbb{Q}$. Рассмотрим два соседних целых числа n и $n+1$, которые переводятся с помощью f в рациональные $f(n) < < f(n+1)$. Тогда любому рациональному числу между $f(n)$ и $f(n+1)$ должно соответствовать целое число $n < z < n+1$, но таких нет.

- Конечные линейно упорядоченные множества из одинакового числа элементов изоморфны. Действительно, последовательно выбирая по минимальному элементу из этих множеств, с помощью рекурсии можно установить изоморфизм между каждым из них и множеством $n = \{0, 1, \dots n-1\}$, где n — количество элементов в каждом из множеств.

Функция f называется *монотонной*, если удовлетворяет свойству $a \leqslant b \Rightarrow f(a) \leqslant f(b)$. Если x и y — частично упорядоченные множества, то наличие монотонной биекции $f : x \leftrightarrow y$ ещё не означает изоморфизма x и y. Пусть x — множество натуральных чисел, упорядоченное отношением делимости, y — множество натуральных чисел с обычным отношением порядка, $f = \mathrm{id}_x$. Если a делит b, то $a \leqslant b$, но не обязательно наоборот, и множества x и y действительно неизоморфны: множество элементов x, непосредственно следующих за единицей, бесконечно и равно множеству простых чисел, в то время как в y непосредственно за единицей следует только двойка.

Однако если x — линейно упорядоченное множество, то наличия монотонной биекции $f : x \leftrightarrow y$ достаточно для установления изоморфизма между x и y.

Упр. 81. Проверьте последнее утверждение.

Упр. 82. Назовём множество x *плотным*, если для любых его элементов a, b, $a < b$, существует элемент $c \in x$, такой, что $a < c < b$. Докажите, что любые два счётных плотных линейно упорядоченных множества без наибольшего и наименьшего элементов изоморфны. Указание: постройте изоморфизм с помощью рекурсии.

Легко видеть, что отношение изоморфизма транзитивно, рефлексивно и симметрично. Таким образом, всякое множество упорядоченных множеств разбивается отношением изоморфизма на классы эквивалентности. Про множества, лежащие в одном классе эквивалентности по изоморфизму, говорят, что они имеют одинаковый порядковый тип (разумеется, это лишь ещё один способ сказать, что множества изоморфны).

7. Частично упорядоченное множество называется *фундированным*, если любое его непустое подмножество имеет минимальный элемент. Формально x — фундированное множество, если и только если

$$\forall u(u \subseteq x \,\&\, u \neq \varnothing \Rightarrow \exists m(m \in u \,\&\, \forall b(b \in u \Rightarrow \neg m > b))).$$

Фундированное линейно упорядоченное множество называется *вполне упорядоченным*, а соответствующий порядок — *полным*. Примеры:

- множество натуральных чисел вполне упорядочено (см. упр. 51);
- множество натуральных чисел, упорядоченное отношением делимости, является фундированным, но не вполне упорядоченным (т. к. оно не упорядочено линейно);
- множество целых чисел, упорядоченное обычным отношением $\leqslant$, не является фундированным (например, у множества

всех отрицательных целых чисел нет минимального элемента), также и множество неотрицательных действительных чисел, упорядоченное обычным отношением $\leqslant$, не является фундированным (например, у подмножества $(0,1)$ нет минимального элемента);

- множество действительных чисел $\{x \in \mathbb{R} \mid x = 1 \vee \exists n(n \in \in \omega \,\&\, x = 1 - 2^{-n})\}$, упорядоченное обычным отношением $<$, является вполне упорядоченным (проверьте).

Следующее упражнение определяет некоторые способы конструирования новых вполне упорядоченных множеств из уже имеющихся.

Упр. 83. Докажите, что если x и y — вполне упорядоченные множества, то их сумма и произведение (в смысле, определённом выше) являются вполне упорядоченными множествами.

Упр. 84. Используя аксиому выбора, докажите, что линейно упорядоченное множество x является вполне упорядоченным тогда и только тогда, когда в нём нельзя построить бесконечной убывающей последовательности элементов (т. е. такой инъекции $h : \omega \to x$, что $h(n+1) < h(n)$ для любого натурального n).

Вполне упорядоченные множества обладают многими интересными свойствами и играют важную роль в доказательстве ряда фундаментальных теорем. Несколько удобнее, однако, изучать свойства не упорядоченных множеств вообще, а некоторых «канонических представителей» класса упорядоченных множеств, именуемых *ординалами*.

8. Ординалы. Назовём множество *транзитивным*, если каждый его элемент является также и его подмножеством:

$$\mathrm{Trans}(x) \rightleftharpoons \forall t(t \in x \Rightarrow t \subseteq x).$$

Ординалом (или *трансфинитным числом*, или *порядковым числом*) называется такое множество, что оно само и все его элементы транзитивны:

$$\mathrm{Ord}(x) \rightleftharpoons \mathrm{Trans}(x) \,\&\, \forall t(t \in x \Rightarrow \mathrm{Trans}(t)).$$

Свойства, непосредственно вытекающие из этого определения, сформулированы в следующей теореме.

Теорема 50. *Справедливы следующие утверждения:*

1) $\varnothing$ — *ординал;*

2) *если* x — *ординал, то* $x+1$ — *ординал*[5]*;*

3) $\vdash \mathrm{Ord}(x) \Rightarrow \forall t(t \in x \Rightarrow \mathrm{Ord}(t))$ — *все элементы ординала являются ординалами;*

4) *если* u — *множество ординалов, т. е.* $\forall t(t \in u \Rightarrow \mathrm{Ord}(t))$, *то* $\bigcup u$ — *ординал.*

◁Первые два утверждения теоремы тривиальны. Третье тоже доказывается просто: всякий элемент ординала x — транзитивен и является подмножеством x, значит, элементы элементов ординала x сами являются элементами x и транзитивны.

Докажем четвёртое утверждение. Докажем, что $\bigcup x$ — транзитивно, что эквивалентно $z \in \bigcup x \Rightarrow \forall y(y \in z \Rightarrow y \in \bigcup x)$. Имея в виду $\forall$-правило вывода, достаточно доказать, что

$$z \in \bigcup x \Rightarrow (y \in z \Rightarrow y \in \bigcup x),$$

что эквивалентно

$$y \in z \,\&\, z \in \bigcup x \Rightarrow y \in \bigcup x.$$

Но $y \in z \,\&\, z \in \bigcup x \Rightarrow y \in z \,\&\, \exists t(t \in x \,\&\, z \in t)$, откуда в силу транзитивности каждого $t \in x$, $y \in z \,\&\, z \in \bigcup x \Rightarrow y \in z \,\&\, \exists t(t \in x \,\&\, \&\, z \subseteq t)$, из чего окончательно следует $y \in z \,\&\, z \in \bigcup x \Rightarrow \exists t(t \in x \,\&\, \&\, y \in t)$, что и будет эквивалентно требуемому $y \in z \,\&\, z \in \bigcup x \Rightarrow \Rightarrow y \in \bigcup x$.

[5] Напомним, что $x+1 \rightleftharpoons x \cup \{x\}$.

Докажем, что каждый элемент $\bigcup x$ транзитивен. Напомним, что каждый элемент x — ординал, а значит, $z \in \bigcup x \Rightarrow \exists t(t \in \in x \,\&\, \mathrm{Ord}(t) \,\&\, z \in t)$. Т. к. каждый элемент ординала является ординалом, то $\mathrm{Ord}(t) \& z \in t \Rightarrow \mathrm{Ord}(z)$, откуда $z \in \bigcup x \Rightarrow \mathrm{Ord}(z)$, и все элементы $\bigcup x$ являются ординалами (а значит, транзитивны).$\triangleright$

Чтобы лучше понять, что собой представляют ординалы, рассмотрим некоторые примеры, учитывая, что только что доказанная теорема позволяет двумя способами конструировать новые ординалы из уже имеющихся: добавлением единицы и суммированием произвольного множества ординалов.

Прежде всего заметим, что нуль и все натуральные числа 1, 2, 3... — ординалы, что легко доказывается на основе первых двух утверждений теоремы по математической индукции. Множество всех натуральных чисел ω — ординал. Действительно, все его элементы — ординалы, а значит, транзитивны, кроме того, любое натуральное число есть множество чисел, строго меньших n (см. упр. 50), следовательно, $n \in \omega \Rightarrow n \subseteq \omega$. Но коль скоро ω — ординал, то $\omega \cup \{\omega\} = \omega + 1$ — ординал, и то же справедливо для $\omega + 1 + 1 = \omega + 2$, $\omega + 3$ и т. д. (Свойства ординалов позволяют, образно говоря, «продолжать счёт за пределами бесконечности» — поэтому они и называются также *трансфинитными числами*).

Объединение множества ординалов вида $\omega + n$, где n — натуральное число, даёт ординал $\omega + \omega = \omega \cdot 2$, за которым можно построить $\omega \cdot 2 + 1$, $\omega \cdot 2 + 2$,... и т. д., а затем $\omega \cdot 3$, $\omega \cdot 4$...

Объединение множества ординалов вида $\omega \cdot k$ само является ординалом, обозначим его как ω^2. За ним следуют $\omega^2 + 1$, $\omega^2 + 2$,... $\omega^2 + \omega$, $\omega^2 + \omega + 1$,... $\omega^2 + \omega \cdot 2$,... $\omega^2 \cdot 2$,..., ω^3,... ω^4 и т. д., объединение ординалов вида ω^n даёт ω^ω. Далее возможно определить $\omega^{(\omega^2)}$ и т. д., в какой-то момент получим $\varepsilon_0 = \bigcup\{\omega, \omega^\omega, \omega^{(\omega^\omega)}, \ldots\}$... Процесс конструирования новых ординалов можно продолжать сколько угодно, но всё бóльшие ординалы становится всё труднее описать.

9. Пусть x — некоторое множество ординалов, т. е. $\forall t(t \in x \Rightarrow$

$\Rightarrow \mathrm{Ord}(t)$). Нетрудно установить следующие два свойства такого множества.

1) x строго упорядочено отношением $\in$. Антирефлексивность и антисимметричность отношения $\in$ следуют из аксиомы фундирования (см. теорему 33 на с. 95). Докажем транзитивность. Пусть $a \in b$ и $b \in c$. Т. к. c — транзитивное множество, то $b \subseteq c$, откуда $a \in c$.

2) Если x — непустое множество ординалов, строго упорядоченное отношением $\in$, то для любого $a \in x$ имеется $b \leqslant a$, минимальное в x. Предположим, что это не так, т. е. $\forall y(y \in x \Rightarrow \Rightarrow \exists u(u \in y))$. В силу транзитивности каждого элемента x следствием этого предположения должно быть $\forall y(y \in x \Rightarrow \Rightarrow \exists u(u \in y \,\&\, u \in x))$, т. е. для любого $y \in x$ имеется элемент, общий с x и y. Но это — прямое отрицание аксиомы фундирования.

Таким образом, всякое множество ординалов является фундированным упорядоченным множеством (далее будет показано, что любые два ординала сравнимы и всякое множество ординалов является вполне упорядоченным множеством).

Фундированность любого множества ординалов позволяет без труда доказать теорему, являющуюся сильным обобщением принципа математической индукции, доказанного в § 2.3, со множества натуральных чисел на произвольное множество ординалов (мы не говорим «множество всех ординалов» по причине, которая вскоре станет ясна). С этого момента будем считать, что обозначения $x < y$ и $x \in y$, когда речь идёт об ординалах, взаимозаменяемы.

Теорема 51 (о трансфинитной индукции)**.** *Если имеется такое соотношение A со свободной переменной x, что*

$$\forall x(\forall x'(\mathrm{Ord}(x) \,\&\, x' < x \Rightarrow (x' \mid x)A) \Rightarrow A),$$

то $\forall x(\mathrm{Ord}(x) \Rightarrow A)$. Иначе говоря, если для произвольного ординала x установлено, что из того факта, что если формула A истинна на любом ординале, меньшем x, следует, что формула A

истинна на x, то формула A должна быть истинна на любом ординале x.

$\lhd$Предположим, что $\exists x(\mathrm{Ord}(x)\ \&\ \neg A)$. Рассмотрим множество ординалов меньших x и таких, что $\neg A$: $\{u \in x \mid \neg(u \mid x)A\}$. Если это множество пусто, то $\forall x'(x' \in x \Rightarrow (x' \mid x)A)$, из чего должно следовать A на x, но мы предположили обратное — противоречие. Следовательно, это множество не должно быть пусто и у него должен иметься минимальный элемент u_0, такой, что любой элемент множества $\{u \in x \mid \neg(u \mid x)A\}$ не будет меньше этого минимального элемента. Сам минимальный элемент u_0 принадлежит этому множеству, поэтому $\neg(u_0 \mid x)A$ — на u_0 формула ложна. Но для всех ординалов, меньших u_0, формула истинна. Следовательно, она должна быть истинна и на u_0 — противоречие. Следовательно, такого x, что $\mathrm{Ord}(x)\ \&\ \neg A$, не существует.$\rhd$

Упр. 85. Пусть A зависит от x и y. Докажите, что если

$$\forall x\forall y(\forall x'\forall y(x' < x\ \&\ \mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow (x' \mid x)A)\&\\ \&\forall y'(y' < y\ \&\ \mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow (y' \mid y)A) \Rightarrow A),$$

то $\forall x\forall y(\mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow A)$. (Указание. Предположим, что A ложна для каких-то x и y. Построим множество $\{(u,v) \in x\times y \mid \neg(u \mid x)(v \mid y)A\}$. Должен существовать минимальный u_0, такой, что при любом $u < u_0$ и любом v A выполняется. Должен далее существовать минимальный v_0, что для всех $v < v_0$ формула $(u_0 \mid x)A$ выполняется, и т. д.)

Теорема 52. *Любые два ординала сравнимы по $\in$. Иначе говоря,* $\mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow x < y \vee x = y \vee y < x$.

$\lhd$Обозначим через A формулу $x < y \vee x = y \vee y < x$. Чтобы доказать $\mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow A$, воспользуемся обобщением трансфинитной индукции на случай двух переменных (см. упр. 85). Для этого достаточно доказать

$$\forall x\forall y(\forall x'\forall y(x' \in x\ \&\ \mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow (x' \mid x)A)\&\\ \&\forall y'(y' \in y\ \&\ \mathrm{Ord}(x)\ \&\ \mathrm{Ord}(y) \Rightarrow (y' \mid y)A) \Rightarrow A),$$

что содержательно означает: если для ординала x истинно, что каждый его элемент x' сравним с любым ординалом y и он сам

сравним с любым элементом y' ординала y, то ординал x сравним с ординалом y.

Докажем это утверждение разбором случаев. Для произвольных x, y выполняется по крайней мере один из трёх случаев: $x = y$, $x \setminus y \neq \varnothing$, $y \setminus x \neq \varnothing$.

Если $x = y$, ординалы сравнимы (и равны).

Пусть $x \setminus y \neq \varnothing$. Тогда имеется элемент u, такой, что $u \in x$ & $\& u \notin y$, сравнимый с y. Если $u = y$, то $y \in x$, и ординалы сравнимы. Если $y \in u$, то, т. к. $u \subseteq x$ в силу транзитивности x, имеет место $y \in x$, и ординалы сравнимы. Случай $u \in y$ исключается выбором u.

Пусть, наконец, $y \setminus x \neq \varnothing$. Тогда имеется элемент u, такой, что $u \in y$ & $u \notin x$, сравнимый с x. Если $u = x$, то $x \in y$, и ординалы сравнимы. Если $x \in u$, то, т. к. $u \subseteq y$ в силу транзитивности y, имеет место $x \in y$, и ординалы сравнимы. Случай $u \in x$ исключается выбором u.▷

Из этой теоремы сразу выводятся следующие важные следствия:

1) если x и y — ординалы, то $\neg(x < y) \Rightarrow x \geqslant y$;

2) если x и y — ординалы, то $x \subset y \vee x = y \vee y \subset x$, причём $x \subset y$ тогда и только тогда, когда $x \in y$;

3) любое множество ординалов строго линейно вполне упорядочено отношением $\in$ (и отношением $\subset$).

Следующая теорема показывает, что всякий ординал задаёт отношением $\in$ уникальный (с точностью до изоморфизма) полный порядок.

Теорема 53. *Два ординала изоморфны тогда и только тогда, когда они равны.*

◁Пусть a, b — ординалы. Если они равны, то они изоморфны. Пусть они не равны. В силу следствий из теоремы 52 без ограничения общности можно считать, что $a \subset b$. Предположим, что

изоморфизм $f : a \leftrightarrow b$ существует. В силу критерия Дедекинда (см. теорему 43) такая биекция может существовать, только если b — бесконечное множество. Будем рассуждать так же, как при доказательстве теоремы 43. По условию $\exists x_0(x_0 \in b \setminus f[b])$. Определим рекурсией $g : \omega \to b$ на основе условий

$$g(0) = x_0,$$
$$g(n+1) = f(g(n)).$$

Индукцией можно показать, что в силу биективности функции f

$$b \supset f[b] \supset f[f[b]] \supset f[f[f[b]]] \supset \ldots,$$

$$g(0) \ni g(1) \ni g(2) \ni \ldots,$$

из чего следует, что $g[\omega]$ — множество ординалов без минимального элемента. Но таких множеств не существует — противоречие. Следовательно, a и b не изоморфны.▷

Заметим, что бесконечные ординалы могут быть равномощны, но не изоморфны: таковы, например, счётные ординалы ω и $\omega + 1$.

Теорема 54 («парадокс Бурали–Форти»). *Не существует множества всех ординалов. Иначе говоря, формула* $\mathrm{Ord}(x)$ *не является коллективизирующей по* x.

◁Пусть $\Omega = \{x \mid \mathrm{Ord}(x)\}$ — множество всех ординалов. Оно должно быть транзитивно: по теореме 50 элементы любого ординала являются ординалами, а значит, элементами Ω. Каждый элемент Ω — ординал, а значит, транзитивен. Отсюда следует, что Ω само должно быть ординалом и $\Omega \in \Omega$, что запрещено аксиомой фундирования.▷

Утверждение только что доказанной теоремы, разумеется, противоречит схеме аксиом неограниченного выделения наивной теории множеств, в соответствии с которой при помощи любой формулы A со свободной переменной x можно образовать множество всех x, таких, что A. Более простые примеры противоречий, выводимых из принципа $\exists y \forall z(z \in y \Leftrightarrow A)$, уже были рассмотрены ранее:

это парадоксы Рассела и Кантора, связанные с тем, что формулы $x \notin x$ и $x = x$ не являются коллективизирующими. Интересно, что, несмотря на свою относительную сложность, факт несуществования множества всех ординалов исторически был установлен ранее и носит название *парадокса Бурали–Форти* по фамилии открывшего его математика.

10. Ординал x называется *последующим*, если имеется ординал x', такой, что $x = x' + 1$. Не равный пустому множеству не последующий ординал называется *предельным*. Нетрудно проверить, что если x', фигурирующее в определении последующего ординала, существует, то оно единственно (см. упр. 46). Следующая теорема устанавливает критерий, определяющий тип произвольного ординала.

Теорема 55. *Для любого ординала $x \neq \varnothing$ имеет место один и только один из следующих случаев:*

1) $\bigcup x + 1 = x$, *и x — последующий ординал;*

2) $\bigcup x = x$, *и x — предельный ординал.*

$\lhd$Из транзитивности нетрудно установить, что для любого ординала x имеет место $\bigcup x \subseteq x$, а значит, $\bigcup x \leqslant x$.

Докажем, что утверждения A: «x — последующий ординал», B: $\bigcup x \subset x$ и C: $x = \bigcup x + 1$ эквивалентны.

$A \Rightarrow B$. Пусть x — последующий ординал, т. е. $x = x' \cup \{x'\}$. Тогда $\bigcup x = (\bigcup x') \cup (\bigcup\{x'\}) = x'$ (на последнем шаге использован тот факт, что $\bigcup x' \subseteq x'$). Но тогда $\bigcup x = x' < x$.

$B \Rightarrow C$. Пусть $\bigcup x \subset x$, а значит, $\bigcup x < x$. Сравним ординалы $\bigcup x{+}1$ и x. $\bigcup x{+}1$ не может быть строго меньше x, т. к. это означало бы существование такого t, что $\bigcup x < t < x$, однако $\forall t(t \in x \Rightarrow$ $\Rightarrow t \leqslant \bigcup x)$ (предположив обратное, выводим $\bigcup x < \bigcup x$). С другой стороны, $\bigcup x{+}1$ не может быть строго больше x, т. к. это означало бы $x + 1 \leqslant \bigcup x + 1$ и $x \subseteq \bigcup x$, а мы предполагаем $\bigcup x \subset x$. В силу теоремы 52 остаётся единственный вариант — $x = \bigcup x + 1$.

$C \Rightarrow A$. Если $x = \bigcup x + 1$, то ясно, что он последующий.

Если ординал не равен $\varnothing$ и не последующий, то он предельный. С учётом того, что $\bigcup x \subseteq x$ для любых ординалов, для предельных остаётся случай $\bigcup x = x$.$\triangleright$

Теорема 56. *Любой ординал $x > \omega$ однозначным образом представим в виде суммы $z + n$, где z — предельный ординал, n — натуральное число, сумма $z+n$ понимается в смысле $z+\underbrace{1+1+\ldots+1}_{n\ раз}$.*

$\triangleleft$Определим рекурсивно функцию $f : \omega \to x + 1$, такую, что

$$f(0) = x,$$
$$f(n+1) = \begin{cases} \bigcup f(n), \text{ если } f(n) \text{ — последующий,} \\ \varnothing, \text{ если } f(n) \text{ — предельный или } \varnothing. \end{cases}$$

Начиная с какого-то момента все элементы $f(n)$ должны обратиться в $\varnothing$, иначе получим убывающую последовательность ординалов без минимального элемента (а у всякого множества ординалов, напомним, имеется минимальный элемент). Если n_0 — минимальное число, при котором $f(n_0 + 1) = \varnothing$, то $f(n_0)$ — предельный ординал, из которого можно получить x путём n_0-кратного прибавления единицы. Однозначность разложения следует из однозначности на каждом шаге.$\triangleright$

11. Вслед за математической индукцией (и с её помощью) в § 2.3 была доказана теорема 38 о рекурсивных определениях, позволяющая построить функцию на множестве ω, располагая только значением этой функции в точке 0 и способом получения значения $f(n + 1)$ на основе значения $f(n)$. Рекурсивные построения использовались далее при доказательстве многих теорем, включая доказанную только что теорему 56. И подобно тому, как теорема о трансфинитной индукции расширяет принцип математической индукции, распространяя его со множества ω на произвольные ординалы, теорема о трансфинитной рекурсии, которая сейчас будет доказана, позволит рекурсивно строить функции, определённые на любом ординале, из которых ω является только лишь частным случаем.

В обычной рекурсии (на множестве ω) значение функции определяется на основе её предыдущего значения. Но если функция определена на некотором ординале x, какой-то из $x' < x$ может оказаться предельным и не иметь непосредственного предшественника. Поэтому при определении функции по трансфинитной рекурсии её значение для текущего аргумента определяется на основе множества сразу всех её предыдущих значений.

Теорема 57 (о трансфинитной рекурсии). *Пусть $\xi(u)$ — произвольное выражение терма со свободной переменной u. Тогда справедливо*

$$\forall x(\mathrm{Ord}(x) \Rightarrow \exists! h(\exists y(h : x \to y) \,\&\, \forall x'(x' < x \Rightarrow h(x') = \xi(h[x'])))).$$

Иначе говоря, для любого ординала x может быть определена единственная функция h, действующая на всём x и такая, что при любом аргументе $x' \in x$ её значение определяется с помощью терма ξ от множества значений h от всех предыдущих аргументов: $h(x') = \xi(h[x'])$ — здесь используется тот факт, что любой ординал x' есть множество ординалов, меньших себя.

◁Естественно при доказательстве этого утверждения прибегнуть к трансфинитной индукции. Для краткости обозначим через $A(x, h)$ условие

$$\exists y(h : x \to y) \,\&\, \forall x'(x' < x \Rightarrow h(x') = \xi(h[x'])),$$

и пусть F означает формулу

$$\forall t(t < x \,\&\, \mathrm{Ord}(x) \Rightarrow \exists! h A(t, h)).$$

Для трансфинитной индукции достаточно доказать, что $F \Rightarrow$ $\Rightarrow \exists! h A(x, h)$.

Заметим, что $A(x, h)$ истинна при

- $x = \varnothing$, $h = \varnothing$;
- $x = \{\varnothing\}$, $h = \{(\varnothing, \xi(\varnothing))\}$;

- $x = \{\varnothing, \{\varnothing\}\}$, $h = \{(\varnothing, \xi(\varnothing)), (\{\varnothing\}, \xi(\{\xi(\varnothing)\}))\}$ и т. д.

В силу аксиомы подстановки для любого ординала x

$$\exists e(e = \{h \mid \exists t(t < x \,\&\, \mathrm{Ord}(x) \,\&\, A(t,h) \,\&\, \exists! h A(t,h))\}),$$

откуда выводим

$$F \Rightarrow \exists e(e = \{h \mid \exists t(t < x \,\&\, \mathrm{Ord}(x) \,\&\, A(t,h))\}).$$

Фигурирующее здесь множество e есть множество всех тех h, существование и единственность которых предполагается для каждого $t \in x$.

Рассмотрим терм $\bigcup e$ и убедимся, что $F \Rightarrow A(\bigcup x, \bigcup e)$.

Докажем, что $\bigcup e$ — функция на $\bigcup x$. Для любого $z \in \bigcup x$ существует ординал t, такой, что $z < t < x$, а ему по предположению индукции F соответствует функция $h_t \in e$, определённая на всём t (а значит, и в точке z), такая, что $A(t, h_t)$. Поэтому для любого $z \in \bigcup x$ в $\bigcup e$ найдётся элемент, первая проекция которого равна z. Но он же будет и единственным: покажем, что для любых t, таких, что $z < t < x$, значения всех h_t в точке z совпадают. В самом деле: $x' < x \Rightarrow (A(x,h) \Rightarrow A(x',h))$, и если предположить, что имеются t и t' такие, что $t' < t$ и $h_t(z) \neq h_{t'}(z)$, то это нарушит заложенное в F условие на единственность $h_{t'}$ для ординала t' (так как выполняются $A(t', h_{t'})$ и $A(t', h_t)$).

Проверим теперь, что $\forall x'(x' \in \bigcup x \Rightarrow \bigcup e(x') = \xi(\bigcup e[x']))$. Действительно: для каждого $x' < \bigcup x$ имеются ординал t такой, что $x' < t < x$ и функция $h_t \in e$, для которой данное условие выполняется. Значит, оно выполняется и для $\bigcup e$.

Мы только что доказали $F \Rightarrow \exists h A(\bigcup x, h)$. Докажем, что $F \Rightarrow$ $\Rightarrow \exists! h A(\bigcup x, h)$. Пусть F и для некоторого x существуют h, h' такие, что $A(\bigcup x, h)$ и $A(\bigcup x, h')$. Найдём минимальный аргумент $t \in$ $\in \bigcup x$, на котором $h'(t) \neq h(t)$, а на всех предыдущих аргументах их значения совпадают. Но тогда $h'(t) = \xi(h'[t]) = \xi(h[t]) = h(t)$ — противоречие.

Итак, $F \Rightarrow \exists! h A(\bigcup x, h)$. Если x — предельный ординал или $\varnothing$, то это эквивалентно $F \Rightarrow \exists! h A(x, h)$. Если x — последующий ординал, то $x = \bigcup x \cup \{\bigcup x\}$. Доопределим функцию h «в точке» $\bigcup x$ единственным возможным способом: $h(\bigcup x) = \xi(h[\bigcup x])$.▷

Трансфинитную рекурсию мы будем всегда использовать в паре со следующей леммой, выводимой из парадокса Бурали–Форти.

Лемма 58. *Пусть даны множество x, терм $\xi(u)$ такой, что его значением может быть только $\varnothing$ или одноэлементное множество $\{e\} \subseteq x$ и для любого ординала t трансфинитной рекурсией определена единственная функция $h_t : t \to \mathfrak{P}(x)$ такая, что*

$$\forall t' \left(t' < t \Rightarrow h_t(t') = \left(\bigcup h_t[t'] \right) \cup \xi(h_t[t']) \right).$$

Тогда имеется ординал t_0 такой, что для любого $t' > t_0$ $h_{t'}(t_0) = \bigcup h_{t'}[t_0]$.

Иначе говоря, если определённые по трансфинитной рекурсии функции задают расширяющиеся последовательности подмножеств x, к которым на каждом шаге добавляется не более одного элемента, то обязательно существует такой ординал t_0, на котором расширения не будет.

◁Определённые по трансфинитной рекурсии функции обладают тем свойством, что если $t < t'$, то значения функции h_t совпадают со значениями $h_{t'}$ для всех ординалов, меньших t. Рассмотрим следующее логическое условие, которое для краткости обозначим как $A(t, a)$:

$$\exists t' \left(t < t' \,\&\, a \in h_{t'}(t) \setminus \bigcup h_{t'}[t] \right).$$

Иначе говоря, $A(t, a)$, если a есть в точности элемент x, добавляемый на ординале t. В силу того, что на каждом шаге рекурсии добавляется не более одного элемента, имеем $\forall t(\mathrm{Ord}(t) \,\&\, \& \exists a A(t, a) \Rightarrow \exists! a A(t, a))$, откуда, в силу аксиомы подстановки, существует множество ординалов

$$\{t \mid \exists a (a \in x \,\&\, \mathrm{Ord}(t) \,\&\, A(t, a))\}$$

таких, что на каждом из них добавляется некоторый элемент из x.

В силу теоремы 54, это множество не может быть множеством всех ординалов, откуда $\exists t_0 \forall a(a \in x \,\&\, \mathrm{Ord}(t_0) \Rightarrow \neg A(t_0, a))$. $\triangleright$

Теорема 59. *Любое вполне упорядоченное множество x изоморфно единственному ординалу.*

$\triangleleft$Определим для всякого $u \subseteq x$ терм $\eta(u)$ следующим образом: $\{y \in u \mid \forall y'(y' \in u \Rightarrow y \leqslant y')\}$. В силу того, что x вполне упорядочено, $\eta(u)$ является либо одноэлементным множеством, содержащим наименьший элемент u, либо пустым множеством, если $u = \varnothing$.

В силу теоремы о трансфинитной рекурсии, для любого ординала t существует единственная функция $h_t : t \to \mathfrak{P}(x)$ такая, что

$$\forall t' \left(t' < t \Rightarrow h_t(t') = \left(\bigcup h_t[t']\right) \cup \eta\left(x \setminus \bigcup h_t[t']\right)\right).$$

Иначе говоря, каждая из функций h_t на каждом «шаге» трансфинитной рекурсии равна множеству выбранных ранее из x элементов плюс минимальный элемент x из числа оставшихся, если элементы остались.

В силу леммы 58, существует по крайней мере один (а значит, существует и наименьший) ординал t' такой, что $h_t(t') = \bigcup h_t[t']$. Но это возможно только если $x = \bigcup h_t[t']$ (иначе $\eta(x \setminus \bigcup h_t[t']) \neq \varnothing$). Нетрудно проверить, что функция $f(t) = \bigcup(h_{t'}(t) \setminus \bigcup h_{t'}[t])$, равная элементу x, выбираемому на шаге t, сюръективна и обратнооднозначна, т. е. является биекцией между ординалом t' и x.

Но эта биекция монотонна. На любом «шаге» t_1 выбирается наименьший из оставшихся элементов x, а на любом «шаге» $t_2 > t_1$ будет выбираться один из элементов, остававшихся к «шагу» t_1, кроме наименьшего, т. е. $t_2 > t_1 \Rightarrow f(t_2) > f(t_1)$. В силу линейной упорядоченности t' существования монотонной биекции между множествами t' и x достаточно для установления изоморфизма между этими множествами.

Таким образом, мы доказали, что любое вполне упорядоченное множество изоморфно некоторому ординалу. Но в силу транзитивности изоморфизма и теоремы 53 этот ординал — единственный.▷

12. Использование трансфинитной рекурсии совместно с аксиомой выбора позволяет доказать ряд важных результатов, к которым относится теорема Цермело (из которой сразу следует вывод о сравнимости любых двух множеств по мощности) и лемма Цорна.

°**Теорема 60** (Цермело)**.** *Любое множество x может быть вполне упорядочено.*

◁Достаточно доказать, что можно установить биекцию между x и некоторым ординалом. Общий подход к установлению этого факта подобен тому, что применялся в доказательстве теоремы 41 на с. 124.

Прежде всего с помощью аксиомы выбора обеспечим себя функцией выбора $f_c : \mathfrak{P}(x) \to \mathfrak{P}(x)$, такой, что $f_c(\varnothing) = \varnothing$ и $u \neq \varnothing \,\&\, u \subseteq x \Rightarrow \exists t(\{t\} = f_c(u) \& t \in u)$, т. е. если аргумент этой функции есть непустое подмножество u, то результат — одноэлементное множество из одного из элементов u.

Далее в доказательстве теоремы 41 с помощью обычной рекурсии определялась счётная последовательность сжимающихся множеств, получающаяся «отбрасыванием» из x по одному элементу, так что если какой-то из членов этой последовательности обращается в $\varnothing$, то все следующие также должны были быть пустыми. Потом выводилось, что такой член обязан существовать, иначе имелась бы инъекция из x в ω, наличие которой отрицается по условию теоремы 41.

Примерно то же самое мы проделаем и теперь, но вместо обычной рекурсии для получения последовательности сжимающихся множеств применим трансфинитную, после чего необходимо будет доказать, что в какой-то момент процедура «трансфинитного выбора» исчерпает все элементы произвольного множества x.

В силу теоремы о трансфинитной рекурсии для любого ординала t существует единственная функция $h_t : t \to \mathfrak{P}(x)$, такая, что

$$\forall t' \left(t' < t \Rightarrow h_t(t') = \left(\bigcup h_t[t'] \right) \cup f_c \left(x \setminus \bigcup h_t[t'] \right) \right).$$

Иначе говоря, каждая из функций h_t на каждом «шаге» трансфинитной рекурсии равна множеству выбранных ранее из x элементов плюс ещё один элемент x из числа оставшихся, если элементы остались.

В силу леммы 58 существует по крайней мере один (а значит, существует и наименьший) ординал t', такой, что $h_t(t') = \bigcup h_t[t']$. Но это возможно, только если $x = \bigcup h_t[t']$ (иначе $f_c(x \setminus \bigcup h_t[t']) \neq \neq \varnothing$). Нетрудно проверить, что функция $f(t) = \bigcup (h_{t'}(t) \setminus \bigcup h_{t'}[t])$, равная элементу x, выбираемому на шаге t, сюръективна и обратнооднозначна, т. е. является биекцией между ординалом t' и x. Полный порядок на x переносится с ординала t'.▷

°**Теорема 61.** *В ZFC любые два множества x, y сравнимы по мощности.*

◁В силу теоремы Цермело 60 существуют ординалы u и v, такие, что существуют биекции $f_x : x \leftrightarrow u$ и $f_y : y \leftrightarrow v$. Но в силу следствия теоремы 52 для любых ординалов u и v должно быть $u \subseteq v$ или $v \subseteq u$. В первом случае $f_y^{-1} \circ f_x$ есть инъекция из x в y и $|x| \leqslant |y|$, во втором — $f_x^{-1} \circ f_y$ есть инъекция из y в x и $|y| \leqslant |x|$. Таким образом случай, когда не существует инъекций ни из x в y, ни из y в x, не может иметь места.▷

Пусть x — частично упорядоченное множество. Подмножество $u \subseteq x$ называется *цепью*, если индуцированный на u порядок линеен.

°**Лемма 62** (Цорна)**.** *Если x — частично упорядоченное множество, в котором каждая цепь имеет верхнюю грань, то для любого элемента $x_0 \in x$ существует $x_0' \geqslant x_0$, являющийся максимальным в x.*

◁Обозначим для краткости через $C(u)$ условие «u есть цепь в x», формально записываемое как

$$u \subseteq x \,\&\, \forall a \forall b (a \in u \,\&\, b \in u \,\&\, a \neq b \Rightarrow a < b \vee b < a).$$

Определим далее терм $\eta(u)$, задающий множество верхних граней для всякого $u \subseteq x$. Формально,

$$\eta(u) = \{y \in x \mid \forall t (t \in u \Rightarrow t \leqslant y)\}.$$

Если $t \in u \cap \eta(u)$, то t — максимальный (и даже наибольший) элемент в u. Пусть теперь $\eta'(u) = \eta(u) \setminus u$ — множество верхних граней u, не являющихся элементами u.

Пусть $f_c : \mathfrak{P}(x) \to \mathfrak{P}(x)$ — функция выбора, как в доказательствах теорем 41 и 60. Переопределим её так, чтобы $f_c(x) = \{x_0\}$, т. е. при подстановке в неё всего x в качестве выбираемого элемента выступал заданный в условии теоремы начальный x_0. В силу теоремы о трансфинитной рекурсии для любого ординала t существует единственная функция $h_t : t \to \mathfrak{P}(x)$, такая, что

$$\forall t' \left(t' < t \Rightarrow h_t(t') = \left(\bigcup h_t[t']\right) \cup f_c\left(\eta'\left(\bigcup h_t[t']\right)\right)\right).$$

Как видим, ситуация почти такая же, как в доказательстве теоремы Цермело. Каждая из функций h_t на каждом «шаге» трансфинитной рекурсии равна множеству выбранных ранее из x элементов плюс ещё один элемент x — но не просто из числа оставшихся, как мы брали в теореме Цермело, а из числа верхних граней уже выбранного множества элементов, не входящих в множество уже выбранных элементов (если такие верхние грани имеются).

В силу леммы 58 существует по крайней мере один (а значит, существует и наименьший) ординал t, такой, что $h_k(t) = \bigcup h_k[t]$ для $k > t$. Но тогда множество $\bigcup h_k[t] \subseteq x$ — цепь. Действительно, пусть $t' < t$ — минимальный ординал такой, что во множестве $h_k(t')$ имеются несравнимые элементы. Но $h_k(t')$ есть объединение всех выбранных ранее (сравнимых) элементов и одноэлементного множества, состоящего из какой-то верхней грани (сравнимой со всеми

элементами) — противоречие, множество $\bigcup h_k[t]$ — действительно цепь.

Но если $\bigcup h_k[t]$ — цепь, то у неё, по условию, существует верхняя грань b. Раз все лежащие вне этой цепи верхние грани «исчерпаны» на ординале t, то b должен лежать внутри цепи и быть её максимальным, и даже наибольшим, элементом. Из сравнимых с b элементов x нет элементов, больших b, значит, мы имеем дело с максимальным в x элементом.$\triangleright$

Мы не будем здесь останавливаться на арифметических операциях, которые можно ввести над ординалами (об этом можно прочитать, например, в [11], [13]), а только выведем некоторые важные, на наш взгляд, следствия, касающиеся операций над мощностями.

13. Операции над мощностями (дальнейшее развитие). Теперь с помощью леммы Цорна мы готовы получить некоторые существенные обобщения формул, выведенных в § 2.5.

Первое из них обобщает формулу $|x| + \aleph_0 = \max(|x|, \aleph_0)$.

°**Теорема 63.** *Если хотя бы одно из множеств x, y бесконечно, то*

$$|x| + |y| = \max(|x|, |y|).$$

$\triangleleft$Первый шаг: докажем сначала, что для бесконечного x имеет место $|x| + |x| = |2 \times x| = |x|$.

Условие $|x| \geqslant \aleph_0$ означает, что в x можно выделить счётное подмножество $d \subseteq x$, для которого существует биекция $f_d : d \leftrightarrow 2 \times d$ (как нам уже известно, $2\aleph_0 = \aleph_0$).

Пусть m — множество пар (a, f_a), таких, что: 1) $d \subseteq a \subseteq x - a$ есть надмножество d и подмножество x, 2) $f_a : a \leftrightarrow 2 \times a - f_a$ есть биекция между a и $2 \times a$, 3) $f_d \subseteq f_a$ — значения f_a на d совпадают с f_d.

Упорядочим элементы множества m отношением $(a, f_a) \leqslant (b, f_b) \ \sim \ a \subseteq b \ \& \ f_a \subseteq f_b$. Тогда любая цепь c в множестве m имеет верхнюю грань $\bigcup c$, и в силу леммы Цорна 62 существует элемент $(e, f_e) \geqslant (d, f_d)$, максимальный в m. Устано-

вим, что e имеет ту же мощность, что и x, чем теорема будет доказана (по построению, существует биекция между e и $2 \times e$).

Т. к. $e \subseteq x$, $|e| \leqslant |x|$, так что могут иметь место всего два случая: $|e| < |x|$ и $|e| = |x|$. Предположим, что $|e| < |x|$ и $y = x \setminus e$. Докажем, что y — бесконечное множество.

Если бы e и y были конечными, то их сумма, равная x, также была бы конечной, что противоречит тому, что x — бесконечное множество. Если же e бесконечно, а y — конечно, то, т. к. добавление конечного числа элементов к бесконечному множеству не меняет его мощности, $|x| = |e + y| = |e| < |x|$ — вновь противоречие. Отсюда следует, что y — бесконечно.

Но это значит, что в y можно выделить счётное подмножество y' и построить биекцию $f_{y'} : y' \leftrightarrow 2 \times y'$. В таком случае терм $(e \cup y', f_e \cup f_{y'})$ будет, очевидно, элементом m, превышающим (e, f_e), что противоречит тому, что (e, f_e) — максимальный в m элемент. Значит, исходное предположение о том, что $|e| < |x|$, неверно и $|e| = |x| = |2 \times e| = |2 \times x| = |x| + |x|$.

Второй шаг. В силу теоремы 61 возможны только случаи $|x| \leqslant |y|$ и $|y| \leqslant |x|$. Пусть, например, $|x| \leqslant |y|$. Тогда $|y| \leqslant |x| + |y|$ и $|x| + |y| \leqslant |y| + |y| \leqslant |y|$, откуда по теореме Кантора–Шрёдера–Бернштейна имеем $|x| + |y| = |y|$. Аналогичным образом в предположении $|x| \geqslant |y|$ доказывается $|x| + |y| = |x|$, откуда $|x| + |y| = \max(|x|, |y|)$, что и требовалось.▷

В § 2.5 было установлено, что $\aleph_0 \aleph_0 = \aleph_0$ и $\mathfrak{c}\mathfrak{c} = \mathfrak{c}$. Обобщим этот результат на любую бесконечную мощность.

°**Теорема 64** (о квадрате). $\mathrm{ZFC} \vdash |x| \geqslant \aleph_0 \Rightarrow |x|^2 = |x|$.

◁Действуем так же, как и при доказательстве теоремы 63. Условие $|x| \geqslant \aleph_0$ означает, что в x можно выделить счётное подмножество $d \subseteq x$, для которого, например, нумерующая функция Кантора f_d устанавливает биекцию между d и $d \times d$.

Пусть m — множество пар (a, f_a), таких, что: 1) $d \subseteq a \subseteq x - a$ есть надмножество d и подмножество x, 2) $f_a : a \leftrightarrow a \times a - f_a$ есть биекция между a и $a \times a$, 3) $f_d \subseteq f_a$ — значения f_a на d совпадают с f_d.

Упорядочим элементы множества m отношением $(a, f_a) \leqslant (b, f_b) \sim a \subseteq b \;\&\; f_a \subseteq f_b$. Тогда любая цепь c в множестве m имеет верхнюю грань $\bigcup c$, и в силу леммы Цорна 62 существует элемент $(e, f_e) \geqslant (d, f_d)$, максимальный в m. Установим, что e имеет ту же мощность, что и x, чем теорема будет доказана (по построению, существует биекция между e и $e \times e$).

Т. к. $e \subseteq x$, $|e| \leqslant |x|$, так что могут иметь место всего два случая: $|e| < |x|$ и $|e| = |x|$. Предположим, что $|e| < |x|$ и $y = x \setminus e$. До сих пор мы почти дословно воспроизводили доказательство теоремы 63, и в этом месте выводилось, что y — бесконечное множество. Но теперь можно утверждать большее: т. к. $x = y \cup e$, $|x| = \max(|e|, |y|)$ и т. к. $|e| < |x|$ по предположению, $|y| = |x| > |e|$.

Это значит, что имеется $y' \subseteq x \setminus e$, такой, что $|y'| = |e|$. Положим $z = e \cup y'$ и покажем, что существует биекция между z и $z \times z$, продолжающая биекцию f_e. Действительно,

$$z \times z = (e \cup y') \times (e \cup y') = \\ = (e \times e) \cup (e \times y') \cup (y' \times e) \cup (y' \times y').$$

Т. к. $|e| = |y'| = |y'|^2 = |e|^2$ и четыре множества, входящих в объединение, не пересекаются

$$|(e \times y') \cup (y' \times e) \cup (y' \times y')| = 3|y'| = |y'|.$$

Отсюда следует, что существует биекция между y' и $(e \cup y') \times (e \cup y') \setminus e \times e$, объединив её с биекцией f_e, получим биекцию между $e \cup y'$ и $(e \cup y') \times (e \cup y')$, продолжающую f_e. Но это значит, что $(e \cup y', f_{e \cup y'}) \geqslant (e, f_e)$, а это противоречит предположению о максимальности (e, f_e).$\triangleright$

Можно доказать, что в системе ZF аксиома выбора, теорема 60 Цермело о вполне упорядочении, лемма 62 Цорна и теорема 64

о квадрате *эквивалентны*, т. е. за аксиому можно принять любое из этих утверждений, и остальные будут выводиться из него.

Упр. 86. Используя идеи доказательств теорем 63 и 64, покажите, что из леммы Цорна в ZF следует теорема Цермело о вполне упорядочении.

Упр. 87. Докажите, что из теоремы Цермело о вполне упорядочении в ZF следует аксиома выбора. Указание: в любом подмножестве вполне упорядоченного множества имеется единственный наименьший элемент.

Результат выполнения двух последних упражнений доказывает эквивалентность в ZF теоремы Цермело, леммы Цорна и аксиомы выбора. Сложнее вывести, например, теорему Цермело из теоремы о квадрате. Соответствующее доказательство приведено, например, в [1].

°**Теорема 65.** *Если одно из множеств x, y бесконечно, а другое — непусто, то*

$$|x||y| = \max(|x|, |y|).$$

◁Доказательство аналогично доказательству теоремы 63, только вместо $|x|+|x| = |x|$ используется доказанное в теореме 64 утверждение $|x|^2 = |x|$.▷

Объединив результаты теорем 63 и 65, получим, что для непустых множеств x и y, одно из которых бесконечно,

$$|x| + |y| = |x||y| = \max(|x|, |y|).$$

Упр. 88. Пусть x — бесконечно. Докажите, что $|x^*| = |x|$.

Упр. 89. Пусть множество y бесконечно. Докажите, что

$$|x|^{|y|} = 2^{|y|}, \text{ если } 2 \leqslant |x| \leqslant 2^{|y|};$$
$$|x| \leqslant |x|^{|y|} < 2^{|x|}, \text{ если } |x| > 2^{|y|}.$$

14. Понятие класса. Напомним, что такие формулы A, что в теории множеств выводимо $\exists u \forall z (z \in u \Leftrightarrow A)$, мы называли *коллективизирующими*. Если рассматриваемая нами теория множеств непротиворечива, то не все формулы являются коллективизирующими: так, например, мы выяснили, что формулы $z \notin z$, $z = z$, $\mathrm{Ord}(z)$ и т. п. не могут являться коллективизирующими, т. к.

предположение о существовании соответствующих множеств ведёт к противоречиям.

Рассмотренные примеры неколлективизирующих формул наводят на мысль, что, образно говоря, для некоторых формул A совокупность «всех x, таких, что A» оказывается «слишком велика» для того, чтобы являться множеством. Тем не менее представляется удобным рассуждать о таких совокупностях как о самостоятельных объектах. Делать это, не впадая в противоречия, позволяет концепция *класса*.

Мы будем говорить, что произвольная формула A, возможно, содержащая x в качестве параметра, задаёт *класс* $\{x \mid A\}$ множеств, для которых A истинно. Например, формула $\mathrm{Ord}(x)$ задаёт класс ординальных чисел, формула $x = x$ — класс всех множеств, $x \neq x$ — пустой класс и т. д.

Если $\{x \mid A\}$ — класс, то запись $t \in \{x \mid A\}$ означает, по определению, $(t \mid x)A$. Отношения $t \subseteq \{x \mid A\}$ и $t = \{x \mid A\}$ вводятся обычным образом.

Всякое множество является классом (если A — коллективизирующая формула, то $\{x \mid A\}$ — множество), но не всякий класс является множеством. Классы, не являющиеся множествами, мы назовём *собственно классами*.

Т. к. собственно классы не есть множества, они находятся вне предметной области теории множеств. Иначе говоря, если мы рассматриваем некоторую формулу A со свободной переменной x, то для нас x «пробегает» все множества, но не собственно классы. Если теперь мы захотим построить класс $\{x \mid A\}$, то в качестве элементов в него попадут только множества, но ни один собственно класс в него не попадёт.

Отсюда следует основное свойство собственно классов: *никакой собственно класс не может являться элементом другого класса* (и, следовательно, другого множества). Говорить о «классе всех классов, таких, что...» попросту синтаксически некорректно: правильно говорить лишь о «классе всех множеств, таких, что...» Образно говоря, собственно класс является «настолько большой»

совокупностью, что сам уже не может быть элементом никакой другой совокупности.

Это свойство и позволяет применять неколлективизирующие формулы в выражениях вида $\{x \mid A\}$, не впадая в противоречия. Так, мы можем говорить о классе всех множеств, не содержащих себя в качестве элемента, не впадая при этом в парадокс Рассела. Т. к. $x \notin x$ — неколлективизирующая формула, то рассматриваемый класс будет собственно классом и своим элементом не будет. Это, однако, не нарушает «всеобщности», поскольку в логическом условии идёт речь только о множествах.

Таким образом, понятие класса сохраняет непротиворечивую теорию множеств непротиворечивой: оно добавляет новые возможности формальной записи, но не увеличивает количества выводимых формул.

ГЛАВА 3

РОДЫ СТРУКТУР

§ 3.1. Типизации и биективная переносимость

1. *Схема конструкции ступени* (по Павловскому [16, 17]) есть выражение, определяемое следующим образом:

1) индекс[1] есть схема конструкции ступени;

2) если S — схема конструкции ступени, то $\mathfrak{P}(S)$ — схема конструкции ступени;

3) если S и S' — схемы конструкции ступени, то $(S \times S')$ — схема конструкции ступени;

4) других схем конструкции ступени не существует.

Иногда вместо «схема конструкции ступени» говорят просто «схема», если из контекста ясно, что речь идёт о схеме конструкции ступени. Если S — схема, а n — максимальный индекс, использованный при её построении, то S называется *схемой конструкции ступени над n множествами*.

Примеры: 1 — схема над одним множеством; 2, (1×2), $\mathfrak{P}(\mathfrak{P}(2))$ и $\mathfrak{P}(1 \times \mathfrak{P}(2))$ — схемы над двумя множествами; $\mathfrak{P}(3 \times 5)$ — схема над пятью множествами.

[1] *Индексом* мы называем строку вида ||| ... | (n палочек), для краткости всюду заменяемую соответствующим натуральным числом n. Важно понимать, однако, что числа, изображающие индексы, не имеют отношения к натуральным числам, определённым в §2.3, и являются всего лишь сокращающими знаками для строк из соответствующего числа вертикальных палочек. Для определения индекса (в отличие от определения натурального числа) не требуется никакой теории, что позволяет использовать их в схемах конструкций ступеней (и в именах индексированных переменных типа x_2, d_4) ещё прежде разговора о любой теории.

Как и в случае с пропозициональными формулами (см. с. 12), внешние скобки на каждом шаге построения схемы нужны для того, чтобы однозначным образом определять последовательность вычислений. Для удобства будем экономить скобки в тех случаях, когда последовательность очевидна: прежде всего откажемся от внешних скобок на последнем шаге построения схемы (например, схему (1×2) будем записывать как 1×2). Во-вторых, будем считать, что операция $\times$ выполняется последовательно слева направо, т. е. схемы вида $(1 \times 2) \times 3$ (но не $1 \times (2 \times 3)$) будем записывать как $1 \times 2 \times 3$.

2. Пусть дана схема S над n множествами и не менее чем n переменных $\xi_1, \ldots \xi_{n'}$, $n' \geqslant n$. Тогда терм, полученный заменой индексов в схеме S на буквы $\xi_1, \ldots \xi_{n'}$ с соответствующими индексами, мы будем называть *ступенью, построенной по схеме S над множествами* $\xi_1, \ldots \xi_{n'}$ и обозначать как $S[\xi_1, \ldots \xi_{n'}]$. Пример: если S — схема $\mathfrak{P}(1 \times \mathfrak{P}(2))$, то $S[x_1, x_2] = \mathfrak{P}(x_1 \times \mathfrak{P}(x_2))$ и $S[y_1, y_2] = \mathfrak{P}(y_1 \times \mathfrak{P}(y_2))$.

Шкалой над множествами $x_1, \ldots x_n$ называется совокупность всех ступеней, которые можно построить по какой-либо схеме над множествами $x_1, \ldots x_n$. Иначе говоря, шкала над $x_1, \ldots x_n$ — это совокупность всех множеств, которые можно построить из исходных множеств при помощи операций декартова произведения и множества-степени. Шкала сама является множеством (причём счётным), т. к. все её элементы можно перечислить при помощи рекурсии.

3. Наглядную иллюстрацию для понятий шкалы и ступеней дают так называемые *М-графы*. М-граф представляет собой геометрическую фигуру, состоящую из вершин, соединённых дугами (рёбрами), причём для каждой дуги задано направление, пара вершин может быть соединена одной или более чем одной дугой, и если последнее имеет место, то дуги нумеруются.

Построим граф по следующему алгоритму: изобразим множества $x_1, \ldots x_k$ в виде вершин; если A — вершина, соответствующая ступени m, то для ступени $\mathfrak{P}(m)$ достроим новую вершину М-

графа, соединяя её дугой с вершиной A; если A_1, A_2 — вершины, соответствующие ступеням m_1, m_2 (возможно, какие-то из них — совпадающие), то для ступени $m_1 \times m_2$ достроим новую вершину М-графа, соединяя её нумерованными дугами с вершинами A_1, A_2, причём номер каждой дуги соответствует позиции m_i в декартовом произведении. Пример М-графа см. на рис. 3.1, где вершина A соответствует ступени $\mathfrak{P}(x_1)$, вершина B — ступени $x_1 \times x_2$ и т. д.

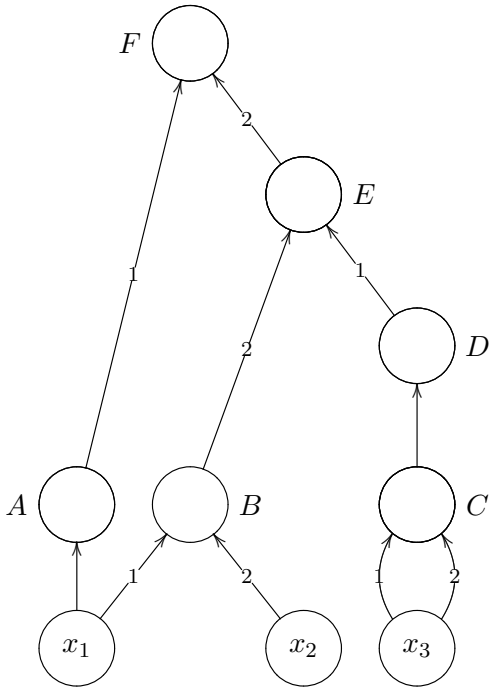


Рис. 3.1. Пример М-графа

Упр. 90. Каким ступеням соответствуют вершины C, D, E, F М-графа на рис. 3.1?

Упр. 91. Постройте М-графы ступеней, соответствующих следую-

щим формулам:

$$\mathfrak{P}(x_1 \times \mathfrak{P}\mathfrak{P}(x_1 \times x_1)),$$
$$\mathfrak{P}(x_2 \times x_1) \times \mathfrak{P}(x_2 \times x_1),$$
$$\mathfrak{P}\mathfrak{P}(x_2) \times \mathfrak{P}(x_1) \times x_1,$$
$$x_1 \times \mathfrak{P}(x_3) \times \mathfrak{P}\mathfrak{P}(x_2),$$
$$x_3 \times \mathfrak{P}(\mathfrak{P}(x_3) \times x_2) \times x_1.$$

4. Формула вида $\xi \in S[x_1, \ldots x_n]$, где ξ — произвольная переменная или терм, называется *соотношением типизации* для переменной (терма) ξ. Если для ξ выполняется соотношение типизации, то говорят также, что множество (переменная, терм) ξ *типизировано ступенью* $S[x_1, \ldots x_n]$ или *имеет тип* $S[x_1, \ldots x_n]$.

Характерной особенностью типизированных множеств является наличие некоторой предсказуемой структуры их элементов. Индукцией по построению схемы легко показать, что типизированными множествами могут быть только

- элементы множеств $x_1, \ldots x_n$ (если соотношение типизации имеет вид $\xi \in x_i$), в этом случае говорят, что ξ *имеет характер элемента*;

- кортежи, каждый компонент которых типизирован (если соотношение типизации имеет вид $\xi \in S_1[x_1, \ldots x_n] \times \ldots \times \times S_k[x_1, \ldots x_n]$), в этом случае говорят, что ξ *имеет характер кортежа*;

- множества, каждый элемент которых типизирован (если соотношение типизации имеет вид $\xi \in \mathfrak{P}(S[x_1, \ldots x_n])$), в этом случае говорят, что ξ *имеет характер множества*.

Например, если $d \in x_1 \times x_2$, то d — это пара элементов: $(\ldots, \ldots)$. Если $d \in \mathfrak{P}(x_1 \times x_2)$, то d — это некоторое множество пар: $\{(\ldots, \ldots), (\ldots, \ldots), \ldots\}$. Если $d \in \mathfrak{P}\mathfrak{P}(x_1 \times x_2)$, то d — это множество множеств пар: $\{\{(\ldots, \ldots), (\ldots, \ldots) \ldots\}, \{(\ldots, \ldots), (\ldots, \ldots) \ldots\}, \ldots\}$. Если $d \in \mathfrak{P}(x_1) \times \mathfrak{P}(x_2)$, то d — это пара множеств: $(\{\ldots\}, \{\ldots\})$. Если $d \in \mathfrak{P}(\mathfrak{P}(x_1) \times x_2)$, то d — это множество пар вида «множество, элемент»: $\{(\{\ldots\}, \ldots), (\{\ldots\}, \ldots), \ldots\}$, и т. д.

Таким образом, типизированное множество не допускает, например, существования среди своих элементов «вперемешку» множеств и кортежей или кортежей с разным количеством компонент. Условие $\xi \in S[x_1, \dots x_n]$ кажется существенным ограничением для ξ, но, как показывает практика, одних только типизированных множеств вполне достаточно для описания средствами теории множеств математических объектов и построения прикладных моделей.

5. Другой важной особенностью типизированного множества является тот факт, что в ситуации, когда множества $x_1, \dots x_n$ подвергаются преобразованиям, типизированное множество $\xi \in S[x_1, \dots x_n]$ может быть преобразовано вместе с $x_1, \dots x_n$ некоторым согласованным образом.

Пусть даны множества x и x', а также функция $f : x \to x'$. Функция $\hat{\mathfrak{P}}(f) : \mathfrak{P}(x) \to \mathfrak{P}(x')$, определённая по формуле $\hat{\mathfrak{P}}(f) = \{(u, v) \in \mathfrak{P}(x) \times \mathfrak{P}(x') \mid f[u] = v\}$, называется *каноническим распространением f на множество частей.*

Пусть даны множества x_1, x_2, x'_1, x'_2, а также функции $f_1 : x_1 \to x'_1$ и $f_2 : x_2 \to x'_2$. Функция $f_1 \hat{\times} f_2 : x_1 \times x_2 \to x'_1 \times x'_2$, определённая по формуле $f_1 \hat{\times} f_2 = \{((u, v), (u', v')) \in (x_1 \times x_2) \times (x'_1 \times x'_2) \mid f_1(u) = u' \,\&\, f_2(v) = v'\}$, называется *каноническим распространением f_1, f_2 на декартово произведение.*

Пусть имеются множества $x_1, \dots x_n$, $x'_1, \dots x'_n$ и функции $f_1, \dots f_n$, такие, что $f_i : x_i \to x'_i$, как показано на диаграмме:

$$\begin{array}{ccccc} x_1 & x_2 & \dots & x_n \\ \big\downarrow{\scriptstyle f_1} & \big\downarrow{\scriptstyle f_2} & & \big\downarrow{\scriptstyle f_n} \\ x'_1 & x'_2 & \dots & x'_n \end{array}$$

Пусть также дана схема S над не более чем n множествами.

Функция, получаемая из схемы S заменой индексов $1, 2, 3 \dots$ на буквы f_i с соответствующими индексами, знаков $\mathfrak{P}$ на $\hat{\mathfrak{P}}$ и знаков $\times$ на $\hat{\times}$, называется *каноническим распространением* $f_1, \dots f_n$

по схеме S, обозначается $\langle f_1, \dots f_n\rangle^S$ и обладает свойством

$$\langle f_1, \dots f_n\rangle^S : S[x_1, \dots x_n] \to S[x'_1, \dots x'_n].$$

Например, если даны $f_1 : x_1 \to x'_1$ и $f_2 : x_2 \to x'_2$, а также схема $\mathfrak{P}(1 \times 2)$, то можно построить по этой схеме функцию $\hat{\mathfrak{P}}(f_1 \hat{\times} \times f_2) : \mathfrak{P}(x_1 \times x_2) \to \mathfrak{P}(x'_1 \times x'_2)$.

Применение функции $\langle f_1, \dots f_n\rangle^S$ к типизированному множеству $d \in S[x_1, \dots x_n]$ называется *переносом* множества d с помощью функций $f_1, \dots f_n$. В соответствии с данными нами определениями результат переноса будет являться типизированным множеством, причём

$$\langle f_1, \dots f_n\rangle^S(d) \in S[x'_1, \dots x'_n].$$

Например, если $d \in \mathfrak{P}(x_1 \times x_2)$ и даны $f_1 : x_1 \to x'_1$ и $f_2 : x_2 \to x'_2$, то мы можем получить $d' = \hat{\mathfrak{P}}(f_1 \hat{\times} f_2)(d)$, такую, что $d' \in \in \mathfrak{P}(x'_1 \times x'_2)$, при этом каждой паре $(u, v) \in d$ соответствует пара $(u', v') \in d'$, такая, что $u' = f_1(u)$ и $v' = f_2(v)$.

Теорема 66. *Справедливы следующие утверждения:*

1) *если* $f_i : x_i \to x'_i$, $f'_i : x'_i \to x''_i$ *для* $i = 1, \dots n$, *то*

$$\langle f'_1 \circ f_1, \dots f'_n \circ f_n\rangle^S = \langle f'_1, \dots f'_n\rangle^S \circ \langle f_1, \dots f_n\rangle^S;$$

2) *если все* $f_i : x_i \to x'_i$ — *сюръекции (инъекции, биекции) для* $i = 1, \dots n$, *то* $\langle f_1, \dots f_n\rangle^S$ — *сюръекция (инъекция, биекция);*

3) *если* $f_i : x_i \leftrightarrow x'_i$ *для* $i = 1, \dots n$, *то*

$$\left(\langle f_1, \dots f_n\rangle^S\right)^{-1} = \langle f_1^{-1}, \dots f_n^{-1}\rangle^S.$$

⊲Докажем первые два утверждения теоремы индукцией по построению схемы S.

Если S представляет собой индекс k, то $\langle f'_1 \circ f_1, \dots f'_n \circ f_n\rangle^S = \langle f'_1, \dots f'_n\rangle^S \circ \langle f_1, \dots f_n\rangle^S = f'_k \circ f_k$. При этом $\langle f_1, \dots f_n\rangle^S = f_k$, сюръективность (инъективность, биективность) сохраняется.

Пусть S имеет вид $S_1 \times S_2$. Используя предположение индукции, заключаем, что $\langle f'_1 \circ f_1, \dots f'_n \circ f_n\rangle^{S_1\times S_2} = (\langle f'_1, \dots f'_n\rangle^{S_1} \circ \circ \langle f_1, \dots f_n\rangle^{S_1})\hat{\times}(\langle f'_1, \dots f'_n\rangle^{S_2} \circ \langle f_1, \dots f_n\rangle^{S_2})$. Но $(g_1 \circ h_1)\hat{\times}(g_2 \circ \circ h_2) = (g_1\hat{\times}g_2) \circ (h_1\hat{\times}h_2)$, т. к. $(g_1 \circ h_1)\hat{\times}(g_2 \circ h_2)((u,v)) = = (g_1(h_1(u)), g_2(h_2(v)))$, откуда $\langle f'_1 \circ f_1, \dots f'_n \circ f_n\rangle^{S_1\times S_2} = = \langle f'_1, \dots f'_n\rangle^{S_1\times S_2} \circ \langle f_1, \dots f_n\rangle^{S_1\times S_2}$. По предположению индукции, $\langle f_1, \dots f_n\rangle^{S_1}$ и $\langle f_1, \dots f_n\rangle^{S_2}$ — сюръекция (инъекция, биекция). Т. к. $g\hat{\times}h$ сохраняет одновременную сюръективность (инъективность, биективность) g и h, функция $\langle f_1, \dots f_n\rangle^{S_1\times S_2} = \langle f_1, \dots f_n\rangle^{S_1}\hat{\times} \times\langle f_1, \dots f_n\rangle^{S_2}$ сюръективна (инъективна, биективна).

Пусть, наконец, S имеет вид $\mathfrak{P}(S')$ и $\langle f'_1 \circ f_1, \dots f'_n \circ f_n\rangle^{\mathfrak{P}(S')} = = \hat{\mathfrak{P}}(\langle f'_1, \dots f'_n\rangle^{S'} \circ \langle f_1, \dots f_n\rangle^{S'})$. Но $\hat{\mathfrak{P}}(g \circ h) = \hat{\mathfrak{P}}g \circ \circ \hat{\mathfrak{P}}h$, т. к. $\hat{\mathfrak{P}}(g \circ h)(u) = (g \circ h)[u] = g[h[u]]$, откуда $\langle f'_1 \circ f_1, \dots f'_n \circ f_n\rangle^{\mathfrak{P}(S')} = \langle f'_1, \dots f'_n\rangle^{\mathfrak{P}(S')} \circ \langle f_1, \dots f_n\rangle^{\mathfrak{P}(S')}$. Т. к. $\hat{\mathfrak{P}}(g)$ сохраняет сюръективность (биективность, инъективность) g, то функция $\langle f_1, \dots f_n\rangle^{\mathfrak{P}(S')} = \hat{\mathfrak{P}}(\langle f_1, \dots f_n\rangle^{S'})$ сюръективна (инъективна, биективна). Первое и второе утверждения теоремы доказаны.

Докажем третье утверждение теоремы. Пусть $f_1, \dots f_n$ — биекции. По доказанному, $\langle f_1, \dots f_n\rangle^S$ и $\langle f_1^{-1}, \dots f_n^{-1}\rangle^S$ — биекции и

$$\langle f_1, \dots f_n\rangle^S \circ \langle f_1^{-1}, \dots f_n^{-1}\rangle^S = \mathrm{id}_{S[x_1,\dots x_n]},$$

где id_u — тождественное отображение u в u, ставящее в соответствие каждому элементу u сам этот элемент. Отсюда следует, что $\langle f_1^{-1}, \dots f_n^{-1}\rangle^S = \Big(\langle f_1, \dots f_n\rangle^S\Big)^{-1}$, что и требовалось.▷

6. Напомним, что в главе 1 термин *теория* был определён как совокупность замкнутых формул (аксиом) некоторой сигнатуры. Далее в главе 2 мы рассмотрели сигнатуру с единственным предикатным символом «$\in$» и построили в ней теорию множеств ZFC. Мы отметили также, что ZFC не является единственной возможной теорией множеств: независимость аксиом выбора и континуум-гипотезы от остальных аксиом ZF, возможность их формулировки в различных «сильных» и «слабых» формах порождает боль-

шое количество вариантов того, что можно считать «теорией множеств».

Для дальнейших построений будет несущественно, какой из вариантов теории множеств выбрать. Для большей части построений этой главы существенной будет только выполнимость первых четырёх аксиом ZF (экстенсиональности, множества-степени, множества-суммы и схемы подстановки), которых, как мы знаем, достаточно для того, чтобы ввести операции построения множества частей $\mathfrak{P}(x)$ и декартова произведения $x \times y$. Для того чтобы наши рассуждения обрели максимальную общность, введём специальные соглашения.

С этого момента мы будем обозначать теории каллиграфической буквой $\mathcal{T}$ со штрихами и индексами. Будем говорить, что теория $\mathcal{T}'$ сильнее теории $\mathcal{T}$, если все без исключения теоремы $\mathcal{T}$ являются теоремами $\mathcal{T}'$. В частности, любая теория сильнее себя самой, противоречивая теория сильнее любой теории, и если $\mathcal{T}'$ получена добавлением новых аксиом к $\mathcal{T}$, то $\mathcal{T}'$ сильнее $\mathcal{T}$.

7. Пусть фиксированы

- теория множеств $\mathcal{T}$,
- переменные $x_1, \ldots x_n$, называемые *основными базисными множествами*;
- термы теории $\mathcal{T}$ $\theta_1, \ldots \theta_m$, называемые *вспомогательными базисными множествами*;
- схема S не более чем над $n+m$ множествами и соотношение типизации T вида $d \in S[x_1, \ldots x_n, \theta_1, \ldots \theta_m]$ (здесь и далее предполагается, что при построении ступени по схеме S индексы $n+i$ в выражении схемы заменяются на множества θ_i, т. е. d есть элемент некоторой ступени, построенной на множествах $x_1, \ldots x_n, \theta_1, \ldots \theta_m$), буква d будет называться *родовой константой*;

- переменные $x'_1, \dots x'_n$, переменные $f_1, \dots f_n$ и соотношение переноса F вида

$$f_1 : x_1 \leftrightarrow x'_1 \,\&\, \dots \,\&\, f_n : x_n \leftrightarrow x'_n$$

(каждая f_i есть биекция между x_i и x'_i).

Если значения переменных $x_1, \dots x_n$, $x'_1, \dots x'_n$, $f_1, \dots f_n$ заданы (т. е. приравнены некоторым термам теории $\mathcal{T}'$, совпадающей с $\mathcal{T}$ или более сильной), причём $\mathcal{T}' \vdash T \,\&\, F$, то мы можем построить множество $d' \in S[x'_1, \dots x'_n, \theta_1, \dots \theta_m]$ следующим образом:

$$d' = \langle f_1, \dots f_n, \mathrm{id}_{\theta_1}, \dots \mathrm{id}_{\theta_m} \rangle^S(d),$$

где id_{θ_i} — тождественное отображение θ_i в θ_i.

Таким образом, мы имеем дело с процессом, в котором основные базисные множества подвергаются преобразованиям при помощи биекций, вспомогательные базисные множества не изменяются, а типизированная переменная d преобразуется согласованным образом.

Формула R, возможно, содержащая в качестве параметров переменные $x_1, \dots x_n$ и переменную d, называется *биективно переносимой* (в теории $\mathcal{T}$ при типизации T), если

$$\mathcal{T} \vdash T \,\&\, F \Rightarrow (R \Leftrightarrow (x'_1 \mid x_1) \dots (x'_n \mid x_n)(d' \mid d)R).$$

Терм ξ, возможно, зависящий от переменных $x_1, \dots x_n$ и d, называется *биективно переносимым* (в теории $\mathcal{T}$ при типизации T), если имеется такая схема S_ξ, что выполняются следующие два условия:

1) $\mathcal{T} \vdash T \Rightarrow \xi \in S_\xi[x_1, \dots x_n, \theta_1, \dots \theta_m]$,

2) $\mathcal{T} \vdash T \,\&\, F \Rightarrow (x'_1 \mid x_1) \dots (x'_n \mid x_n)(d' \mid d)\xi = \langle f_1, \dots f_n, \mathrm{id}_{\theta_1}, \dots \mathrm{id}_{\theta_m} \rangle^{S_\xi}(\xi)$.

Примеры:

- если T есть $d \in x_1 \times x_1$, то соотношение $\mathrm{pr}_1(d) = \mathrm{pr}_2(d)$ биективно переносимо (пусть $d = (u, v)$, тогда $d' = (f_1(u), f_1(v))$ и $\mathrm{pr}_1(d) = \mathrm{pr}_2(d) \Leftrightarrow \mathrm{pr}_1(d') = \mathrm{pr}_2(d')$);

- соотношение $x_1 = x_2$ не является биективно переносимым (пусть $x_1 = x_2$, $x_1' = x_1$, $f_1 = \mathrm{id}_{x_1}$, в качестве x_2' возьмём любое равномощное x_2, но не равное x_2 множество и получим $x_1' \neq x_2'$);

- если T есть $d \in \mathfrak{P}(x_1)$, то соотношение $d = x_1$ биективно переносимо, а соотношение $d = x_2$ не является биективно переносимым;

- терм $x_1 \cup x_2$ не является биективно переносимым (нарушается первое условие биективной переносимости термов);

- если T есть $d \in \mathfrak{P}(x_1) \times \mathfrak{P}(x_1)$, то терм $\mathrm{pr}_1(d) \cup \mathrm{pr}_2(d)$ является биективно переносимым (с типом $\mathfrak{P}(x_1)$).

- терм $\{t \in S_\xi[x_1, \ldots] \mid x_1 = x_2\}$ не является биективно переносимым (выполняется первое условие: терм имеет типизацию $\mathfrak{P}(S_\xi[x_1, \ldots])$, но нарушается второе условие биективной переносимости термов).

8. Условия биективной переносимости. Выявим некоторые достаточные условия биективной переносимости термов и соотношений.

Теорема 67. *Справедливы следующие утверждения:*

- *если ни одна из букв $x_1, \ldots x_n$, d не встречается в соотношении R, то R биективно переносимо;*

- *терм $\varnothing$ есть биективно переносимый терм типа $\mathfrak{P}S'[x_1, \ldots]$, какова бы ни была схема S';*

- *при типизации $d \in S[x_1, \ldots]$ x_i — биективно переносимые термы типа $\mathfrak{P}(x_i)$, θ_i — биективно переносимые термы типа $\mathfrak{P}(\theta_i)$, d — биективно переносимый терм типа $S[x_1, \ldots]$;*

- *если R и R' — биективно переносимые соотношения, то же верно и для соотношений $\neg R$, $R \vee R'$, $R \& R'$, $R \Rightarrow R'$, $R \Leftrightarrow R'$.*

◁Эти условия вытекают непосредственно из определений.▷

Теорема 68. *Справедливы следующие утверждения:*

- *если ξ — биективно переносимый терм типа $S_\xi[x_1, \ldots]$ и η — биективно переносимый терм типа $\mathfrak{P}(S_\xi[x_1, \ldots])$, то соотношение $\xi \in \eta$ биективно переносимо;*

- *если ξ и η — биективно переносимые термы одного и того же типа $S_\xi[x_1, \ldots]$, то соотношение $\xi = \eta$ биективно переносимо.*

◁Пусть, для краткости, $f^{S_\xi} = \langle f_1, \ldots f_n, \mathrm{id}_{\theta_1}, \ldots \mathrm{id}_{\theta_m} \rangle^{S_\xi}$. Докажем первое утверждение. По условию,

$$\mathcal{T} \vdash T \,\&\, F \Rightarrow (x_1' \mid x_1) \ldots (d' \mid d)\xi = f^{S_\xi}(\xi) \& \\ \&(x_1' \mid x_1) \ldots (d' \mid d)\eta = \hat{\mathfrak{P}} f^{S_\xi}(\eta).$$

В силу свойств равенства

$$\mathcal{T} \vdash T \,\&\, F \Rightarrow (x_1' \mid x_1) \ldots (d' \mid d)(\xi \in \eta) \Leftrightarrow (f^{S_\xi}(\xi) \in \hat{\mathfrak{P}} f^{S_\xi}(\eta)).$$

Но $\hat{\mathfrak{P}} f^{S_\xi}(\eta) = f^{S_\xi}[\eta]$, откуда $f^{S_\xi}(\xi) \in \hat{\mathfrak{P}} f^{S_\xi}(\eta) \sim f^{S_\xi}(\xi) \in f^{S_\xi}[\eta]$.

В силу теоремы 66, поскольку все $f_1, \ldots f_n$ — биекции, f^{S_ξ} — также биекция, откуда следует $f^{S_\xi}(\xi) \in f^{S_\xi}[\eta] \sim \xi \in \eta$ и биективная переносимость соотношения $\xi \in \eta$.

Второе утверждение теоремы доказывается аналогичным образом.▷

Теорема 69. *Если термы ξ и η — переносимые термы типов соответственно $\mathfrak{P}(S_\xi[x_1,\ldots])$ и $\mathfrak{P}(S_\eta[x_1,\ldots])$, то $\xi\times\eta$ есть переносимый терм типа $\mathfrak{P}(S_\xi[x_1,\ldots]\times S_\eta[x_1,\ldots])$ и $\mathfrak{P}(\xi)$ есть переносимый терм типа $\mathfrak{P}\mathfrak{P}(S_\xi[x_1,\ldots])$.*

Обратим внимание: существенно, чтобы ξ и η имели характер множеств.

$\lhd$Докажем, что $(x'_1 \mid x_1)\ldots(d' \mid d)(\xi\times\eta) = \hat{\mathfrak{P}}(f^{S_\xi}\hat{\times}f^{S_\eta})(\xi\times\times\eta)$, для чего в силу биективной переносимости и характера ξ и η достаточно доказать, что $f^{S_\xi}[\xi]\times f^{S_\eta}[\eta] = f^{S_\xi}\hat{\times}f^{S_\eta}[\xi\times\eta]$.

Действительно, $t\in f^{S_\xi}[\xi]\times f^{S_\eta}[\eta] \sim \exists u\exists v(u\in f^{S_\xi}[\xi]\ \&\ v\in\in f^{S_\eta}[\eta]\ \&\ t=(u,v)) \sim \exists u\exists v(\exists z(z\in\xi\ \&\ f^{S_\xi}(z)=u)\ \&\ \exists w(w\in\eta\ \&\ \&\ f^{S_\eta}(w)=v)\&t=(u,v)) \sim \exists z\exists w(z\in\xi\&w\in\eta\&(f^{S_\xi}(z),f^{S_\eta}(w))=\\ =t) \sim t\in f^{S_\xi}\hat{\times}f^{S_\eta}[\xi\times\eta]$.

(Последний шаг выкладки выполнен с учётом $(f^{S_\xi}(z),f^{S_\eta}(w)) = f^{S_\xi}\hat{\times}f^{S_\eta}((z,w))$.)

Докажем биективную переносимость терма $\mathfrak{P}(\xi)$.

$(x'_1 \mid x_1)\ldots(d' \mid d)\mathfrak{P}(\xi) = \mathfrak{P}(f^{S_\xi}[\xi]) = \{t \mid t\subseteq f^{S_\xi}[\xi]\} = \{t \mid \exists u(u\subseteq\xi\ \&\ t=f^{S_\xi}[u])\} = \{t \mid \exists u(u\in\mathfrak{P}(\xi)\ \&\ t=\hat{\mathfrak{P}}f^{S_\xi}(u))\} = \\ =\hat{\mathfrak{P}}f^{S_\xi}[\mathfrak{P}(\xi)] = \hat{\mathfrak{P}}\hat{\mathfrak{P}}f^{S_\xi}(\mathfrak{P}(\xi))$.$\rhd$

Теорема 70. *Для всякой схемы конструкции ступени S' терм $S'[x_1,\ldots x_n,\theta_1,\ldots\theta_m]$ есть биективно переносимый терм типа $\mathfrak{P}S'[x_1,\ldots x_n,\theta_1,\ldots\theta_m]$.*

$\lhd$Доказывается с помощью теоремы 69 индукцией по построению S'.$\rhd$

Теорема 71. *Пусть формула R (зависящая, возможно, от t) удовлетворяет условию*

$$T\ \&\ F\ \&\ (t\in S_t[x_1,\ldots]) \Rightarrow (R \Leftrightarrow (x'_1 \mid x_1)\ldots(d' \mid d)(f^{S_t}(t) \mid t)R).$$

Тогда терм $\{t\in S_t[x_1,\ldots] \mid R\}$ биективно переносим.

(Заметим, что условие, налагаемое теоремой на R, по сути ничего нового не добавляет к условию биективной переносимости:

в частности, ему удовлетворяют не зависящие от t биективно переносимые соотношения и соотношения, биективно переносимые при соотношении типизации $t \in S_t[x_1, \ldots].$)

$\lhd$Нам нужно доказать, что в предположениях теоремы

$$\hat{\mathfrak{P}} f^{S_t}(\{t \in S_t[x_1, \ldots] \mid R\}) = (x_1' \mid x_1) \ldots (d' \mid d)\{t \in S_t[x_1, \ldots] \mid R\}.$$

Действительно: $f^{S_t}[\{t \in S_t[x_1, \ldots] \mid R\}] = \{t \mid \exists u(u \in S_t[x_1, \ldots] \&$ $\& (u \mid t)R \,\&\, t = f^{S_t}(u))\} = \{t \mid \exists u(u \in S_t[x_1, \ldots] \,\&\, t = f^{S_t}(u) \,\&$ $\& ((f^{S_t})^{-1}(t) \mid t)R)\} = \{t \in f^{S_t}[S[x_1, \ldots]] \mid ((f^{S_t})^{-1}(t) \mid t)R\}.$

К только что выведенному соотношению

$$f^{S_t}[\{t \in S_t[x_1, \ldots] \mid R\}] = \{t \in f^{S_t}[S[x_1, \ldots]] \mid ((f^{S_t})^{-1}(t) \mid t)R\}$$

можно прийти и таким неформальным рассуждением: чтобы найти «образ» терма $\{t \in S_t[x_1, \ldots] \mid R\}$, мы должны среди элементов множества $f^{S_t}[S_t[x_1, \ldots]]$ выбрать такие, чей «прообраз» удовлетворяет R.

В силу установленной в теореме 70 биективной переносимости терма $S_t[x_1, \ldots x_n, \theta_1, \ldots \theta_m]$, имеет место $f^{S_t}[S_t[x_1, \ldots]] =$ $= \hat{\mathfrak{P}} f^{S_t}(S_t[x_1, \ldots]) = (x_1' \mid x_1) \ldots (d' \mid d)S_t[x_1, \ldots]$, и для доказательства $\hat{\mathfrak{P}} f^{S_t}(\{t \in S_t[x_1, \ldots] \mid R\}) = (x_1' \mid x_1) \ldots (d' \mid d)\{t \in$ $\in S_t[x_1, \ldots] \mid R\}$ осталось установить, что

$$((f^{S_t}(t))^{-1} \mid t)R \Leftrightarrow (x_1' \mid x_1) \ldots (d' \mid d)R.$$

В силу свойства R, заданного условием, $((f^{S_t})^{-1}(t) \mid t)R \Leftrightarrow (x_1' \mid$ $x_1) \ldots (d' \mid d)(f^{S_t}((f^{S_t})^{-1}(t)) \mid (f^{S_t})^{-1}(t))((f^{S_t})^{-1}(t) \mid t)R$, но результат подстановок в правой части и есть формула $(x_1' \mid x_1) \ldots$ $(d' \mid d)R.\rhd$

Теорема 72. *Пусть формула R (зависящая, возможно, от t) удовлетворяет условию*

$$T \,\&\, F \,\&\, (t \in S_t[x_1, \ldots]) \Rightarrow (R \Leftrightarrow (x_1' \mid x_1) \ldots (d' \mid d)(f^{S_t}(t) \mid t)R).$$

Тогда соотношения

$$\exists t(t \in S_t[x_1, \ldots x_n, \theta_1, \ldots \theta_m] \,\&\, R),$$
$$\forall t(t \in S_t[x_1, \ldots x_n, \theta_1, \ldots \theta_m] \Rightarrow R)$$

биективно переносимы.

$\lhd$Терм $\xi = \{t \in S_t[x_1 \ldots] \mid R\}$ — биективно переносимый типа $\mathfrak{P}S[x_1, \ldots]$ (теорема 71). Первое соотношение эквивалентно $\neg(\xi = \varnothing)$, а второе — $\xi = S_t[x_1 \ldots]$. Из уже установленных условий биективной переносимости (теоремы 67, 68) следует, что оба этих соотношения биективно переносимы.$\rhd$

Соотношения рассматриваемого в теореме 72 вида (называемые соотношениями с *ограниченными кванторами*) часто записывают в сокращённом виде:

$$\exists t \in S_t[x_1, \ldots]R \rightleftharpoons \exists t(t \in S_t[x_1, \ldots] \,\&\, R),$$
$$\forall t \in S_t[x_1, \ldots]R \rightleftharpoons \forall t(t \in S_t[x_1, \ldots] \Rightarrow R).$$

Особое внимание следует обратить на то, что для квантора существования используется конъюнкция, а для квантора всеобщности — импликация. При таком определении ограниченных кванторов сохраняются законы де Моргана:

$$\neg\exists t \in S_t[x_1, \ldots]R \sim \forall t \in S_t[x_1, \ldots]\neg R,$$
$$\neg\forall t \in S_t[x_1, \ldots]R \sim \exists t \in S_t[x_1, \ldots]\neg R.$$

Действительно, используя эквивалентность $A \Rightarrow B \sim \neg A \vee B$ и законы де Моргана, имеем $\neg\forall x(x \in S[\ldots] \Rightarrow R) \sim \exists x\neg(\neg x \in S[\ldots] \vee R) \sim \exists x(x \in S[\ldots] \,\&\, \neg R) \sim \exists x \in S[\ldots]\neg R$. Обратно, $\neg\exists x(x \in S[\ldots] \,\&\, R) \sim \forall x(\neg x \in S[\ldots] \vee \neg R) \sim \forall v(x \in S[\ldots] \Rightarrow \Rightarrow \neg R) \sim \forall x \in S[\ldots]\neg R$.

Теорема 73. *Пусть ξ — биективно переносимый терм типа $\mathfrak{P}(S_\xi[x_1, \ldots])$, такой, что в $\mathcal{T}$ выводимо, что ξ — одноэлементный терм, т. е. $\mathcal{T} \vdash \forall x\forall y(x \in \xi \,\&\, y \in \xi \Rightarrow x = y)$. Тогда $\bigcup\xi$ (равный единственному элементу множества ξ) есть биективно переносимый терм типа $S_\xi[x_1, \ldots]$.*

◁Действительно, $(x'_1 \mid x_1)\dots(d' \mid d)\bigcup\xi = \{u \mid \exists t(t \in f^{S_\xi}[\xi]\ \&\ \&\ u \in t)\} = \{u \mid \exists t(\exists v(v \in \xi\ \&\ t = f^{S_\xi}(v))\ \&\ u \in t)\}$. Но, в силу того, что ξ — одноэлементное множество, $v \in \xi \Leftrightarrow v = \bigcup\xi$ и цепочка равенств продолжается следующим образом: $(x'_1 \mid x_1)\dots(d' \mid d)\bigcup\xi = \{u \mid \exists t(t = f^{S_\xi}(\bigcup\xi)\ \&\ u \in t)\} = \{u \mid u \in f^{S_\xi}(\bigcup\xi)\} = f^{S_\xi}(\bigcup\xi)$, что и требовалось доказать.▷

Итак, если биективно переносимый терм ξ имеет тип $\mathfrak{P}(S_\xi)$, то $\bigcup\xi$ биективно переносим, если ξ необходимо состоит из одного элемента. Если ξ может состоять более чем из одного элемента, то $\bigcup\xi$ может быть и не переносим биективно (так обстоит, например, с термом $\bigcup x_1$). Как мы увидим далее, если биективно переносимый терм ξ имеет тип $\mathfrak{PP}(S_\xi)$, то для биективной переносимости терма $\bigcup\xi$ не требуется дополнительных условий.

Теорема 74. *Пусть ξ — биективно переносимый терм типа $S_1[x_1,\dots] \times S_2[x_1,\dots]$. Тогда $\mathrm{pr}_1(\xi)$ есть биективно переносимый терм типа $S_1[x_1,\dots]$, $\mathrm{pr}_2(\xi)$ — биективно переносимый терм типа $S_2[x_1,\dots]$.*

◁Пусть $t = (u, v)$. Тогда

$$(x'_1 \mid x_1)\dots(d' \mid d)\,\mathrm{pr}_1(t) = \mathrm{pr}_1(f^{S_1}\hat{\times}f^{S_2}((u,v))) = \\ = \mathrm{pr}_1((f^{S_1}(u), f^{S_2}(v))) = f^{S_1}(u) = f^{S_1}(\mathrm{pr}_1(t)),$$

что и требовалось.▷

Упр. 92. Пусть ξ — биективно переносимый терм с типом $\mathfrak{P}(S_\xi[x_1,\dots])$. Введём сокращающие обозначения

$$\exists t \in \xi R \rightleftharpoons \exists t \in S_\xi[x_1,\dots](t \in \xi\ \&\ R),$$
$$\forall t \in \xi R \rightleftharpoons \forall t \in S_\xi[x_1,\dots](t \in \xi \Rightarrow R).$$

Докажите, что соотношения $\exists t \in \xi R$, $\forall t \in \xi R$ биективно переносимы.

Упр. 93. Пусть ξ, η — биективно переносимые термы одного и того же типа $\mathfrak{P}(S_\xi)$. Докажите, что соотношения $\xi \subseteq \eta$, $\xi \subset \eta$ биективно переносимы.

9. Рекурсивный характер только что доказанных условий биективной переносимости термов и соотношений позволяет дока-

зывать биективную переносимость индукцией по построению выражения терма или формулы. Подрезюмировав содержание теорем 67–74 в едином списке, можно определить класс формул и термов, биективно переносимых по построению. Оказывается, что этот класс достаточно широк и лишь некоторые, причём довольно необременительные, ограничения отделяют его от класса всех формул и термов теории множеств.

Для удобства введём следующие обозначения:

- $\tau(\xi)$ обозначает ступень, которой типизирован терм ξ, т. е. выражение $\tau(\xi) = S_\xi[x_1, \ldots]$ означает, что $\mathcal{T} \vdash T \Rightarrow \xi \in \in S_\xi[x_1, \ldots]$.

- DS обозначает схему конструкции ступени такую, что $\mathfrak{P}(DS)$ совпадает с S. Разумеется, это определение имеет смысл только в случае, когда S имеет вид $\mathfrak{P}(S')$ (и тогда DS есть S'). Ситуация, в которой DS не определена, означает нарушение какого-либо из условий биективной переносимости.

- P_1S и P_2S обозначают схемы конструкции ступеней, такие, что $P_1S \times P_2S = S$. Разумеется, это определение имеет смысл только в случае, когда S имеет вид $S_1 \times S_2$ (и тогда P_1S и P_2S есть S_1 и S_2, соответственно). Ситуация, в которой ступень P_1S или P_2S не определена, означает нарушение какого-либо из условий биективной переносимости.

Теоремы 67–74, сформулированные с использованием новых обозначений, гласят, в частности, что если в каждом из перечисленных случаев результирующие типы определены, то:

1) $\varnothing$ есть биективно переносимый терм типа $\mathfrak{P}(S'[x_1, \ldots])$, какова бы ни была схема S';

2) базисные множества $x_1, \ldots x_n$ есть биективно переносимые термы, $\tau(x_i) = \mathfrak{P}(x_i)$;

3) вспомогательные множества $\theta_1, \ldots \theta_m$ есть биективно переносимые термы, $\tau(\theta_i) = \mathfrak{P}(\theta_i)$;

4) родовая константа d, для которой вводится соотношение типизации $d \in S[x_1, \ldots]$, есть биективно переносимый терм, $\tau(d) = S[x_1, \ldots]$;

5) если R, возможно, зависящее от t, биективно переносимо в случае, когда $\tau(t) = S_t[x_1, \ldots]$, то $\{t \in S_t[x_1, \ldots] \mid R\}$ — биективно переносимый терм, $\tau(\{t \in S_t[x_1, \ldots] \mid R\}) = \mathfrak{P}(S_t[x_1, \ldots])$.

6) если ξ — биективно переносимый терм, причём $\mathcal{T} \vdash \forall x \forall y (x \in \xi \,\&\, y \in \xi \Rightarrow x = y)$, то $\bigcup \xi$ (равный единственному элементу множества ξ) есть биективно переносимый терм и $\tau(\bigcup \xi) = D\tau(\xi)$;

7) если ξ — биективно переносимый терм, то $\mathrm{pr}_1(\xi)$ и $\mathrm{pr}_2(\xi)$ — биективно переносимые термы, $\tau(\mathrm{pr}_1(\xi)) = P_1\tau(\xi)$, $\tau(\mathrm{pr}_2(\xi)) = P_2\tau(\xi)$;

8) если ξ и η — биективно переносимые термы и $\mathfrak{P}(\tau(\xi)) = \tau(\eta)$, то $\xi \in \eta$ — биективно переносимое соотношение;

9) если ξ и η — биективно переносимые термы и $\tau(\xi) = \tau(\eta)$, то $\xi = \eta$ — биективно переносимое соотношение;

10) если R и R' — биективно переносимые соотношения, то $\neg R$, $R \vee R'$, $R \,\&\, R'$, $R \Rightarrow R'$, $R \Leftrightarrow R'$ — биективно переносимые соотношения;

11) если R, возможно, зависящее от t, биективно переносимо в случае, когда $\tau(t) = S_t[x_1, \ldots]$, то $\forall t \in S_t[x_1, \ldots]R$ и $\exists t \in S_t[x_1, \ldots]R$ — биективно переносимые соотношения.

Примеры биективно переносимых термов и соотношений рассматриваемого вида:

1) для случая $d \in \mathfrak{P}(x_1 \times x_2)$ соотношения

   (a) $\forall v \in x_2, \exists u \in x_1 \times x_2 (u \in d \,\&\, \mathrm{pr}_2(u) = v)$;

(b) $\forall t_1 \in x_1 \times x_2, \forall t_2 \in x_1 \times x_2 (t_1 \in d \,\&\, t_2 \in d \,\&\, \mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$;

термы

(c) $\{t \in x_1 \mid \exists u \in x_1 \times x_2 (u \in d \,\&\, \mathrm{pr}_1(u) = t)\}$;

(d) $\{t \in \mathfrak{P}(x_1) \mid \exists u \in x_2\ t = \{a \in x_1 \mid \exists v \in x_1 \times x_2 (v \in d \,\&\, \&\, \mathrm{pr}_1(v) = a \,\&\, \mathrm{pr}_2(v) = u)\}\}$;

2) для случая $d \in \mathfrak{P}\mathfrak{P}(x_1)$ соотношения

(a) $\forall a \in \mathfrak{P}(x_1), \forall b \in \mathfrak{P}(x_1) (a \in d \,\&\, b \in d \Rightarrow \{t \in x_1 \mid t \in a \,\&\, \&\, t \in b\} \in d)$;

(b) $\forall a \in \mathfrak{P}(x_1), \forall b \in \mathfrak{P}(x_1), \forall t \in x_1 ((t \in a \Rightarrow t \in b) \Rightarrow b \in d)$;

термы

(c) $\{t \in x_1 \mid \exists v \in \mathfrak{P}(x_1) (v \in d \,\&\, t \in v)\}$;

(d) $\{t \in x_1 \times x_1 \mid \exists v \in \mathfrak{P}(x_1) (v \in d \,\&\, \mathrm{pr}_1(t) \in v \,\&\, \mathrm{pr}_2(t) \in v)\}$

и так далее.

Как видим, в отличие от термов и соотношений теории множеств общего вида, термы и соотношения рассматриваемого вида удовлетворяют двум основным принципам. Во-первых, любой терм — сам по себе или в составе подформулы — имеет свой тип (что неудивительно, т. к. наличие типа является необходимым условием биективной переносимости терма), тип связанных переменных декларируется (т. е. недопустимы выражения вида $\forall x R$, $\{x \mid R\}$, а только $\forall x \in S[x_1, \ldots] R$, $\{x \in S[x_1, \ldots] \mid R\}$). Во-вторых, действуют ограничивающие правила, предписывающие определённую типизацию термам, участвующим в выражениях вида $\xi \in \eta$, $\xi = \eta, \bigcup \xi, \mathrm{pr}_i(\xi)$. Если эти принципы выполняются на каждом шаге при построении выражения, то выражение оказывается биективно переносимой формулой или термом.

Упр. 94. Выделите подтермы в выражениях примеров, приведённых выше, и укажите их тип.

Частичное решение: в примере 1a $\tau(v) = x_2$, $\tau(u) = x_1 \times x_2$, $\tau(d) = \mathfrak{P}(x_1 \times x_2)$, $\tau(\mathrm{pr}_2(u)) = x_2$; в примере 1d $\tau(t) = \mathfrak{P}(x_1)$, $\tau(u) = x_2$, $\tau(a) = x_1$, $\tau(v) = x_1 \times x_2$, $\tau(d) = \mathfrak{P}(x_1 \times x_2)$, $\tau(\mathrm{pr}_1(v)) = x_1$, $\tau\,\mathrm{pr}_2(v) = x_2$, $\tau(\{a \in x_1 \mid \ldots\}) = \mathfrak{P}(x_1)$, $\tau(\{t \in \mathfrak{P}(x_1) \mid \ldots\}) = \mathfrak{P}\mathfrak{P}(x_1)$.

10. Приведённых выше условий биективной переносимости достаточно для того, чтобы распространить их на большинство стандартных разновидностей термов и соотношений теории множеств. Для этого обычные знаки для соотношений и термов должны быть переопределены как сокращающие обозначения для биективно переносимых соотношений и термов, с введением ограничений на типизацию аргументов. Например, переопределим отношение «$\subseteq$» как

$$\xi \subseteq \eta \rightleftharpoons \forall t \in D\tau(\xi)(t \in \xi \Rightarrow t \in \eta).$$

Так определённое отношение $\subseteq$ является биективно переносимым по построению. Конструкция $t \in D\tau(\xi)$ в ограничивающем выражении квантора обеспечивает совпадение типа связанной переменной t с типом каждого элемента ξ и правомерность (с точки зрения условий биективной переносимости) записи $t \in \xi$ в логическом выражении. Какие ограничения на ξ и η накладывает эта формула? Прежде всего отношение $\xi \subseteq \eta$ допустимо не на всех термах, а только на тех, у которых совпадает типизация. Это следует из того, что отношение «$\in$» применяется в двух случаях: $t \in \xi$ и $t \in \eta$, но переменная t имеет одну и ту же типизацию. Далее применение $D\tau(\xi)$ предполагает, что оба терма должны иметь характер множеств. Последнее условие интуитивно можно трактовать следующим образом: использование знака «$\subseteq$» бессмысленно между элементами или кортежами, а имеет смысл только между множествами. Если указанные условия выполняются, «биективно переносимый вариант» отношения «$\subseteq$» имеет тот же смысл, что и обычное отношение «$\subseteq$» в теории множеств.

Обобщение ограниченных кванторов:

$\forall x \in \xi R \rightleftharpoons \forall x \in D\tau(\xi)(x \in \xi \Rightarrow R)$,

$\exists x \in \xi R \rightleftharpoons \exists x \in D\tau(\xi)(x \in \xi \,\&\, R)$,

$\forall x \subseteq \xi R \rightleftharpoons \forall x \in \tau(\xi)(x \subseteq \xi \Rightarrow R)$,
$\exists x \subseteq \xi R \rightleftharpoons \exists x \in \tau(\xi)(x \subseteq \xi \,\&\, R)$.

Для знаков «$\subset$» определения аналогичные.

11. Определим биективно переносимые варианты некоторых из операций над термами, введённых в § 2.2.

- Синглетон:

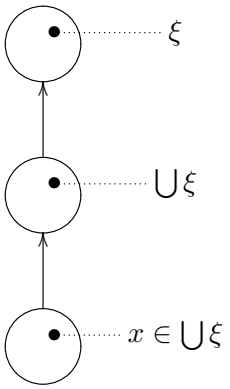
$$\{\xi\} \rightleftharpoons \{x \in \tau(\xi) | (x = \xi)\}, \quad \tau(\{\xi\}) = \mathfrak{P}(\tau(\xi)).$$

Для биективной переносимости $\{\xi\}$ достаточно биективной переносимости ξ, на вид типизирующей терм ξ ступени не накладывается никаких ограничений.

- Множество-сумма:

$$\bigcup \xi \rightleftharpoons \{x \in DD\tau(\xi) | \exists u \in \xi(x \in u)\},$$

$$\tau(\bigcup \xi) = \mathfrak{P}(DD\tau(\xi)).$$



На диаграмме показана «верхушка» М-графа для ступеней, типизирующих термы ξ, $\bigcup\xi$ и связанную переменную x, фигурирующую в определении $\bigcup\xi$.

Таким образом, множество-сумма, образованное от биективно переносимого терма с типом $\mathfrak{P}\mathfrak{P}(S[x_1,\ldots])$, биективно переносимо (для случая типизации $\mathfrak{P}(S[x_1,\ldots])$ см. теорему 73).

Выражение $\mathfrak{P}(DD\tau(\xi))$ не сокращается до $D\tau(\xi)$, поскольку иначе потеряется ограничение на типизацию аргумента ($D\tau(\xi)$ определена и для типов $\mathfrak{P}(S[x_1,\ldots])$, не только $\mathfrak{P}\mathfrak{P}(S[x_1,\ldots])$). Общее правило таково: допустимо сокращать конфигурацию $D\mathfrak{P}$ (т. к. она всюду применима и тождественна), но недопустимо сокращать конфигурацию $\mathfrak{P}D$ (т. к. она, хотя и является тождественной, применима только для ступеней вида $\mathfrak{P}(S[x_1,\ldots])$). На M-графе видно, что при построении выражения необходимо «спускаться» на два шага вниз.

Упр. 95. Докажите, что

$$\tau(\underbrace{\bigcup\ldots\bigcup}_{n\text{ раз}}(\xi)) = \mathfrak{P}(D^{n+1}\tau(\xi)).$$

- Объединение, пересечение, дополнение и симметрическая разность:

$$\xi\cup\eta \rightleftharpoons \{x\in D\tau(\xi)|(x\in\xi)\vee(x\in\eta)\},$$

$$\xi\cap\eta \rightleftharpoons \{x\in D\tau(\xi)|(x\in\xi)\,\&\,(x\in\eta)\},$$

$$\xi\setminus\eta \rightleftharpoons \{x\in D\tau(\xi)|(x\in\xi)\,\&\,(x\notin\eta)\},$$

$$\xi\triangle\eta \rightleftharpoons \{x\in D\tau(\xi)|(x\in\xi)\oplus(x\in\eta)\},$$

$$\begin{aligned}&\tau(\xi\cup\eta)=\tau(\xi\cap\eta)=\\&=\tau(\xi\setminus\eta)=\tau(\xi\triangle\eta)=\\&\quad=\mathfrak{P}(D(\tau(\xi)))=\mathfrak{P}(D(\tau(\eta))).\end{aligned}$$

Для биективной переносимости этих термов требуется, чтобы биективно переносимые аргументы имели характер множеств и были *одинаково типизированы*. Совпадения типов требуют логические условия в выражениях: например, в выражении для $\xi\cup\eta$ связанная переменная имеет тип $D\tau(\xi)$ и, чтобы подформула $x\in\eta$ также была биективно переносимой, требуется $\tau(\xi)=\tau(\eta)$.

- Дополнение множества относительно собственного типа:

$$\complement\xi \rightleftharpoons \{x \in D\tau(\xi) | \neg(x \in \xi)\},$$

$$\tau(\complement\xi) = \mathfrak{P}(D\tau(\xi)).$$

- Неупорядоченная пара:

$$\{\xi, \eta\} \rightleftharpoons \{\xi\} \cup \{\eta\},$$

$$\tau(\{\xi, \eta\}) = \mathfrak{P}(D\mathfrak{P}(\xi)) = \mathfrak{P}(\xi) = \mathfrak{P}(\eta).$$

Здесь вновь требуется совпадение типов ξ и η.

- Упорядоченная пара:

$$(\xi, \eta) = \bigcup(\{x \in \tau(\xi) \times \tau(\eta) | (\mathrm{pr}_1(x) = \xi)\ \&\ (\mathrm{pr}_2(x) = \eta)\}),$$

$$\tau((\xi, \eta)) = \tau(\xi) \times \tau(\eta).$$

- Декартово произведение:

$$\xi \times \eta \rightleftharpoons \{x \in D\tau(\xi) \times D\tau(\eta) \mid (\mathrm{pr}_1(x) \in \xi)\ \&\ (\mathrm{pr}_2(x) \in \eta)\},$$

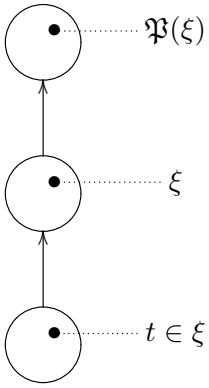
$$\tau(\xi \times \eta) = \mathfrak{P}(D\tau(\xi) \times D\tau(\eta)).$$

Заметим, что, в отличие от упорядоченной пары, биективно переносимой при как угодно типизированных ξ и η, декартово произведение биективно переносимо для термов, имеющих характер множеств.

- Множество-степень:

$$\mathfrak{P}(\xi) \rightleftharpoons \{x \in \tau(\xi) | (x \subseteq \xi)\},$$

$$\tau(\mathfrak{P}(\xi)) = \mathfrak{P}(\mathfrak{P}(D\tau(\xi))).$$



Сравните определение биективно переносимого множества-степени с определением биективно переносимого синглетона, а также выражения для их типов. Использование в выражении множества-степени знака «$\subseteq$» неявно задействует определение $(\xi \subseteq \eta) \rightleftharpoons \forall t \in D\tau(\xi)(t \in \xi \Rightarrow t \in \eta)$, предполагающее «спуск на ступень вниз» по M-графу, что и приводит к другому выражению для типа $\mathfrak{P}(\xi)$ и другим требованиям к типизации аргумента. В отличие от операции образования синглетона, которую можно применять к как угодно типизированному терму, операция $\mathfrak{P}$ допустима только для термов, имеющих характер множества.

- Большая проекция:

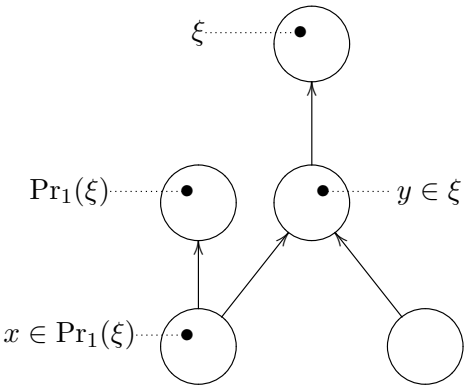
$$\mathrm{Pr}_i(\xi) \rightleftharpoons \{x \in P_i D\tau(\xi) | \exists y \in \xi(x = \mathrm{pr}_i(y))\},$$

$$\tau(\mathrm{Pr}_i(\xi)) = \mathfrak{P}(P_i D\tau(\xi)).$$

Для биективной переносимости терма $\mathrm{Pr}_i(\xi)$ достаточно, чтобы терм ξ был биективно переносимым термом и выражение $P_i D\tau(\xi)$ было определено, т. е. чтобы ξ был типизирован ступенью $\mathfrak{P}(S_1[x_1, \ldots] \times S_2[x_1, \ldots])$.

Для того, чтобы «добраться» до типизации *элемента* $\mathrm{Pr}_i(\xi)$, необходимо сначала получить $D\tau(\xi)$ — типизацию элемента ξ

(а каждый элемент ξ есть кортеж), затем — $P_iD\tau(\xi)$, т. е. типизацию i-го компонента элемента ξ. Наконец, множество элементов, типизированных $P_iD\tau(\xi)$, будет иметь тип $\mathfrak{P}(P_iD\tau(\xi))$, как показано на М-графе:



Упр. 96. На с. 132 определена операция ξ^η, представляющая собой множество всевозможных отображений из η в ξ. При каких условиях эта операция является биективно переносимой и какова её результирующая типизация? (Ответ: ξ и η должны иметь характер множеств, $\tau(\xi^\eta) = \mathfrak{P}\mathfrak{P}(D\tau(\eta) \times D\tau(\xi))$.)

§ 3.2. Определение и примеры

1. Чтобы заранее представлять себе назначение всех составляющих вводимого ниже понятия «род структуры», рассмотрим предварительные примеры.

Из §2.4 известно, что для того, чтобы задать *отображение* из одного множества в другое, необходимо располагать множествами x, y и f, такими, что $f \subseteq x \times y$ (или, что то же, $f \in \mathfrak{P}(x \times y)$), а также

$\forall u \in x, \exists v \in y((u, v) \in f)$,

$\forall t_1 \in f, \forall t_2 \in f(\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$.

При этом не важен характер множеств x и y. Например, это могут быть некоторые числовые множества. Может быть и так, что

одно из них или оба сами являются отображениями (напомним, что отображение из множества функций в множество функций называется *оператором*, отображение множества функций в множество действительных чисел — *функционалом*). При этом некоторые общие для всех отображений понятия (такие, например, как *область значений* $f[x]$) и некоторые свойства (например, $f[a]\setminus f[b] \subseteq f[a\setminus b]$) будут сохраняться вне зависимости от характера множеств x и y.

Из § 2.6 известно, что для того, чтобы задать *частичный порядок* на множестве x, необходимо задать множество $r \in \mathfrak{P}(x \times x)$ такое, что выполняются условия транзитивности, антисимметричности и рефлексивности:

$\forall a \in x, \forall b \in x, \forall c \in x((a,b) \in r \,\&\, (b,c) \in r \Rightarrow (a,c) \in r)$,

$\forall a \in x, \forall b \in x((a,b) \in r \,\&\, (b,a) \in r \Rightarrow a = b)$,

$\forall a \in x(a,a) \in r$.

Наконец, чтобы задать *группу* на множестве x, необходимо задаться отображением из $x \times x$ в x, таким, что выполняются условия ассоциативности, существования левого нейтрального и левого обратного элемента. В формальной записи,

$g \in \mathfrak{P}((x \times x) \times x)$,

$\forall u \in x \times x, \exists v \in x((u,v) \in g)$,

$\forall t_1 \in g, \forall t_2 \in g(\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$,

$\forall a \in x, \forall b \in x, \forall c \in x((a \cdot b) \cdot c = a \cdot (b \cdot c))$,

$\exists e \in x, \forall a \in x(e \cdot a = a)$,

$\forall a \in x, \exists a' \in x, \forall b((a' \cdot a) \cdot b = b)$.

Здесь $a \cdot b$ всюду обозначает терм $\bigcup\{u \in x \mid ((a,b),u) \in g\}$.

Можно доказать, что вне зависимости от того, что представляет из себя множество x, в группе существует единственный *нейтральный элемент* — терм 1, такой, что $a \cdot 1 = 1 \cdot a = a$; кроме того, для всякого a существует единственный *обратный элемент* a^{-1}, такой, что $a \cdot a^{-1} = a^{-1} \cdot a = 1$, и т. д.

Во всех рассмотренных случаях для построения математического объекта мы использовали одно или несколько исходных (базисных) множеств (в примерах — x и y), на которых при помощи соотношения типизации вводились *отношения* (в примерах — f, r

и g), и на эти отношения затем накладывались необходимые требования в виде логических условий, зависящих от базисных множеств и отношений. Заметим также, что во всех случаях нам не составило труда записать эти требования в виде биективно переносимых формул.

2. Пусть зафиксирована некоторая теория множеств $\mathcal{T}$. *Род структуры* ([15], [16]) представляет собой текст из следующих составляющих (конституэнт):

1) переменных $x_1, \ldots x_n$, называемых *основными базисными множествами*;

2) термов $\theta_1, \ldots \theta_m$ теории $\mathcal{T}$, называемых *вспомогательными базисными множествами*;

3) формулы T вида $d \in S[x_1, \ldots x_n, \theta_1, \ldots \theta_m]$ (где $S[x_1, \ldots x_n, \theta_1, \ldots \theta_m]$ — ступень над $n + m$ множествами), являющейся соотношением типизации и называемой *ти́повой характеристикой рода структуры*, буква d при этом называется *родовой константой*;

4) формулы R, биективно переносимой при типизации T, называемой *аксиомой рода структуры*.

Если ти́повая характеристика имеет вид $d \in S_1[\ldots] \times \ldots \times S_k[\ldots]$, то мы можем эквивалентным образом говорить не об одной, а о k родовых константах $d_1, \ldots d_k$, таких, что $d_1 \in S_1[\ldots], \ldots d_k \in S_k[\ldots]$, полагая $d = (d_1, \ldots d_k)$ и используя буквы d_k в аксиоме R вместо соответствующих проекций d, что бывает удобнее в плане экономии места.

Если аксиома R рода структуры имеет вид $R_1 \,\&\, \ldots \,\&\, R_l$, где каждая R_i — биективно переносимая формула, то мы можем эквивалентным образом говорить не об одной, а об l аксиомах $R_1, \ldots R_l$.

3. Пусть даны некоторый род структуры Σ (в теории $\mathcal{T}$, с типовой характеристикой T и аксиомой R) и теория $\mathcal{T}'$, более сильная, чем $\mathcal{T}$. Тогда терм теории $\mathcal{T}'$ вида $(\xi_1, \ldots \xi_n, \delta)$ называется Σ-

объектом[2] (или *теоретико-множественной интерпретацией* Σ), если

$$\mathcal{T}' \vdash (\xi_1 \mid x_1) \dots (\xi_n \mid x_n)(\delta \mid d)(T \,\&\, R).$$

Иначе говоря, упорядоченный набор термов теории $\mathcal{T}'$ называется Σ-объектом, если подстановка этих термов на место соответствующих базисных множеств и родовой константы в типизирующую формулу и аксиому рода структуры приводит к выводимости этих формул в теории $\mathcal{T}'$. При этом про каждое из множеств ξ_i, δ, входящих в Σ-объект, мы будем говорить, что они *интерпретируют* соответствующие буквы x_i, d рода структуры Σ. Разумеется, вспомогательные базисные множества в интерпретации не нуждаются: являясь по определению термами $\mathcal{T}$, они останутся таковыми и в $\mathcal{T}'$.

Иногда бывает удобно говорить о классе (понятие класса, напоминаем, было введено на с. 177) всех Σ-объектов в теории $\mathcal{T}'$:

$$\mathcal{K}_\Sigma = \{(x_1, \dots x_n, d) \mid T \,\&\, R\}.$$

Т. к. соотношение $T \,\&\, R$ не обязательно является коллективизирующим в $\mathcal{T}'$ по $x_1, \dots x_n, d$ (а чаще всего именно так и есть), то класс $\mathcal{K}_\Sigma$ может и не являться множеством. Если $\sigma = (\xi_1, \dots \xi_n, \delta)$, то условия $\sigma \in K_\Sigma$, «σ есть Σ-объект», «σ есть теоретико-множественная интерпретация Σ» эквивалентны.

4. Если $\mathcal{T} \vdash T \,\&\, R \Rightarrow B$, то B называется *теоремой* Σ.

Теорема 75. *Пусть* $(\xi_1, \dots \xi_n, \delta)$ — Σ*-объект в* $\mathcal{T}'$. *Если формула* B — *теорема* Σ, *то*

$$\mathcal{T}' \vdash (\xi_1 \mid x_1) \dots (\xi_n \mid x_n)(\delta \mid d)B.$$

$\lhd$Т. к. $\mathcal{T}'$ сильнее $\mathcal{T}$, то $T \,\&\, R \Rightarrow B$ выводится также в $\mathcal{T}'$. По правилу обобщения, $\mathcal{T}' \vdash \forall x_1 \dots \forall x_n \forall d(T \,\&\, R \Rightarrow B)$. По $\forall$-схеме, $\mathcal{T}' \vdash (\xi_1 \mid x_1) \dots (\xi_n \mid x_n)(\delta \mid d)(T \,\&\, R \Rightarrow B)$. Но т. к. $(\xi_1, \dots \xi_n, \delta)$ —

[2] Термин Ю. Н. Павловского [16, 17].

Σ-объект, левая часть импликации выводится в $\mathcal{T}'$ и по modus ponens имеем $(\xi_1 \mid x_1)\ldots(\xi_n \mid x_n)(\delta \mid d)B$, что и требовалось.$\triangleright$

Таким образом, роды структур позволяют давать доказательства некоторым общим, родоструктурным теоремам, справедливым для любых представителей класса Σ-объектов, причём делать это средствами теории более слабой, чем та, которая требуется для построения Σ-объектов.

Будем называть род структуры *противоречивым*, если имеется такая формула C, что $\mathcal{T} \vdash T \,\&\, R \Rightarrow C$ и $\mathcal{T} \vdash T \,\&\, R \Rightarrow \neg C$. В этом и только этом случае $\mathcal{T} \vdash \neg(T \,\&\, R)$ (в силу схемы reductio ad absurdum), а также $\mathcal{T} \vdash T \,\&\, R \Rightarrow A$, где A — произвольная формула.

В самом деле: $\mathcal{T} \vdash \neg(T \,\&\, R) \Rightarrow (\neg A \Rightarrow \neg(T \,\&\, R))$ — по первой схеме исчисления высказываний, $\mathcal{T} \vdash \neg A \Rightarrow \neg(T \,\&\, R)$ — modus ponens, $\mathcal{T} \vdash T \,\&\, R \Rightarrow A$ — закон контрапозиции.

Теорема 76. *Пусть Σ — род структуры, $\mathcal{K}_\Sigma$ — класс всех Σ-объектов в $\mathcal{T}'$. $\mathcal{K}_\Sigma = \varnothing$ тогда и только тогда, когда Σ противоречив.*

$\triangleleft$В одну сторону. Пусть Σ противоречив. Как мы только что выяснили, это означает $\mathcal{T} \vdash \neg(T \,\&\, R)$, или, по правилу обобщения, $\mathcal{T} \vdash \forall x_1 \ldots \forall x_n \forall d \neg(T \,\&\, R)$.

Т. к. всякое утверждение, выводимое в $\mathcal{T}$, выводимо и в более сильной теории $\mathcal{T}'$, имеем $\mathcal{T}' \vdash \neg\exists x_1 \ldots \exists x_n \exists d(T \,\&\, R)$, из чего и следует, что класс $\mathcal{K}_\Sigma$ не может содержать элементов.

В обратную сторону: пусть $\mathcal{K}_\Sigma = \varnothing$, т. е. $\mathcal{T}' \vdash \forall x_1 \ldots \forall x_n \forall d \neg(T \,\&\, \&\, R)$, т. е. $\mathcal{T}' \vdash \neg(T \,\&\, R)$. Если при этом предположить, что Σ непротиворечив, т. е. $\mathcal{T} \vdash (T \,\&\, R)$ и $\mathcal{T}' \vdash (T \,\&\, R)$, то получится, что из теории $\mathcal{T}'$ следуют взаимоисключающие утверждения. Однако мы полагаем теорию $\mathcal{T}'$ непротиворечивой, и, следовательно, противоречивым должен быть Σ.$\triangleright$

Таким образом, все противоречивые роды структур эквивалентны между собой (класс их теоретико-множественных интерпрета-

ций пуст, в их теориях доказуемо всё, что угодно) и не представляют ни теоретического, ни прикладного интереса.

5. *Изоморфизмом* Σ-объекта $(\xi_1, \dots \xi_n, \delta)$ в Σ-объект $(\xi'_1, \dots \xi'_n, \delta')$ называется терм $(\varphi_1, \dots \varphi_n)$ теории $\mathcal{T}'$, такой, что

$$\mathcal{T}' \vdash \varphi_1 : \xi_1 \leftrightarrow \xi'_1 \,\&\, \dots \,\&\, \varphi_n : \xi_n \leftrightarrow \xi'_n \& \\ \&\langle \varphi_1, \dots \varphi_n, \mathrm{id}_{\theta_1}, \dots \mathrm{id}_{\theta_n} \rangle^S(\delta) = \delta'.$$

Для каждого Σ-объекта $\sigma = (\xi_1, \dots \xi_n, \delta)$ и набора биекций $(\varphi_1, \dots \varphi_n)$ существует единственный Σ-объект $\sigma' = (\xi'_1, \dots \xi'_n, \delta')$, такой, что $(\varphi_1, \dots \varphi_n)$ есть изоморфизм σ в σ'. Действительно, по определению σ' не может не совпадать с термом

$$(\varphi_1[\xi_1], \dots \varphi_n[\xi_n], \langle \varphi_1, \dots \varphi_n, \mathrm{id}_{\theta_1}, \dots \mathrm{id}_{\theta_n} \rangle^S(\delta)).$$

Но этот терм обязан быть Σ-объектом, т. к. является результатом биективного переноса множества δ с помощью биекций $\varphi_1, \dots \varphi_n$, а аксиома R любого рода структуры биективно переносима по определению рода структуры.

Следствием теоремы 66 и общих свойств отображений являются следующие свойства изоморфизмов:

1) если $\tilde{\varphi} = (\varphi_1, \dots \varphi_n)$ и $\tilde{\varphi}' = (\varphi'_1, \dots \varphi'_n)$ есть изоморфизмы соответственно σ в σ' и σ' в σ'', то $\tilde{\varphi}' \circ \tilde{\varphi} = (\varphi'_1 \circ \varphi_1, \dots \varphi'_n \circ \varphi_n)$ есть изоморфизм σ в σ'';

2) $\varphi'' \circ (\varphi' \circ \varphi) = (\varphi'' \circ \varphi') \circ \varphi$;

3) терм $\Delta = (\mathrm{id}_{x_1}, \dots \mathrm{id}_{x_n})$ является тождественным изоморфизмом любого объекта σ в самого себя и обладает свойством $\tilde{\varphi} \circ \Delta = \Delta \circ \tilde{\varphi} = \tilde{\varphi}$;

4) для каждого изоморфизма $\tilde{\varphi}$ объекта σ в σ' имеется обратный ему изоморфизм $\tilde{\varphi}^{-1}$ объекта σ' в σ, равный $(\varphi_1^{-1}, \dots \varphi_n^{-1})$ и обладающий свойством $\tilde{\varphi} \circ \tilde{\varphi}^{-1} = \tilde{\varphi}^{-1} \circ \tilde{\varphi} = \Delta$.

Изоморфизм называется *автоморфизмом*, если переводит множества $\xi_1, \dots \xi_n$ в себя. Суперпозиция автоморфизмов является

автоморфизмом, то же верно для изоморфизма, обратного автоморфизму. Таким образом, множество автоморфизмов множеств $\xi_1, \ldots \xi_n$ удовлетворяет аксиомам группы относительно операции суперпозиции.

Далее в качестве примеров рассматриваются некоторые стандартные роды структур.

6. Родами структур *бинарных отношений* в общем случае называются роды структур, у которых фигурирующая в типовой характеристике схема S имеет вид $\mathfrak{P}(S_1 \times S_2)$. Родами структур *бинарных отношений на двух множествах* называются роды структур с двумя базисными множествами x_1 и x_2 и типовой характеристикой $d \in \mathfrak{P}(x_1 \times x_2)$. Примерами биективно переносимых соотношений при такой типизации являются следующие:

R_1: $\forall u \in x_1, \exists v \in x_2((u, v) \in d)$ — *всюдуопределённость,*

R_2: $\forall t_1 \in d, \forall t_2 \in d(\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$ — *прямая однозначность,*

R_3: $\forall v \in x_2, \exists u \in x_1((u, v) \in d)$ — *всюдузначность,*

R_4: $\forall t_1 \in d, \forall t_2 \in d(\mathrm{pr}_2(t_1) = \mathrm{pr}_2(t_2) \Rightarrow t_1 = t_2)$ — *обратная однозначность.*

Бинарное отношение называется родом структуры *функции* (или *отображения*), если содержит аксиомы R_1, R_2; *сюръекции*, если содержит R_1, R_2, R_3; *инъекции*, если содержит R_1, R_2, R_4; *биекции*, если содержит R_1, R_2, R_3, R_4.

Функцией (сюръекцией, инъекцией, биекцией) принято называть как теоретико-множественную интерпретацию (ξ_1, ξ_2, ψ) рода структуры функции (сюръекции, инъекции, биекции), так и просто терм ψ. Изоморфизм функции ψ в функцию ψ' есть пара биекций $\varphi_1 : \xi_1 \leftrightarrow \xi_1'$, $\varphi_2 : \xi_2 \leftrightarrow \xi_2'$, таких, что $\psi' = \varphi_1 \hat{\times} \varphi_2[\psi]$, что эквивалентно условию $\forall t \in \xi_1(\psi'(\varphi_1(t)) = \varphi_2(\psi(t)))$ или $\psi' \circ \varphi_1 = \varphi_2 \circ \psi$. Наглядное представление о последнем утверждении помогает со-

ставить следующая диаграмма:

$$\begin{array}{ccc} \xi_1 & \xrightarrow{\psi} & \xi_2 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} \\ \xi_1' & \xrightarrow{\psi'} & \xi_2' \end{array}$$

7. Родами структур *бинарных отношений на одном множестве* называются роды структур с одним базисным множеством x и типовой характеристикой $d \in \mathfrak{P}(x \times x)$. Соотношения R_1–R_4 остаются применимыми в качестве аксиом и для этих родов структур, кроме того, в качестве аксиом могут быть использованы следующие соотношения:

R_5: $\forall a \in x, \forall b \in x, \forall c \in x((a,b) \in d \,\&\, (b,c) \in d \Rightarrow (a,c) \in d)$ — *транзитивность,*

R_6: $\forall a \in x, \forall b \in x((a,b) \in d \Rightarrow (b,a) \in d)$ — *симметричность,*

R_7: $\forall a \in x, \forall b \in x((a,b) \in d \,\&\, (b,a) \in d \Rightarrow a = b)$ — *антисимметричность,*

R_8: $\forall a \in x(a,a) \in d$ — *рефлексивность,*

R_9: $\forall a \in x(a,a) \notin d$ — *антирефлексивность,*

R_{10}: $\forall a \in x, \forall b \in x(a \neq b \Rightarrow (a,b) \in d \vee (b,a) \in d)$ — *линейность,*

R_{11}: $\forall u \subseteq x(u \neq \varnothing \Rightarrow \exists m \in u, \forall b \in u((m,b) \notin d))$ — *фундированность,*

R_{12}: $\forall a \in x, \forall b \in x, \exists u \in x((u,a) \in d \,\&\, (u,b) \in d \,\&\, \forall v \in x((v,a) \in d \& (v,b) \in d \Rightarrow (v,u) \in d))$ — *существование наибольшей нижней грани (infimum) у каждого двухэлементного множества,*

R_{13}: $\forall a \in x, \forall b \in x, \exists u \in x((a,u) \in d \,\&\, (b,u) \in d \,\&\, \forall v \in x((a,v) \in d \,\&\, (b,v) \in d \Rightarrow (u,v) \in d))$ — *существование наименьшей верхней грани (supremum) у каждого двухэлементного множества.*

Род структуры бинарного отношения называется родом структуры *эквивалентности*, если содержит R_5, R_6, R_8.

Род структуры бинарного отношения называется родом структуры *предпорядка*, если содержит R_5, R_8; *(частичного) (нестрогого) порядка*, если содержит R_5, R_7, R_8; *(частичного) строгого порядка*, если содержит R_5, R_7, R_9. Добавление к роду структуры

строгого или нестрогого частичного порядка аксиомы R_{10} порождает род структуры *линейного* (строгого или нестрогого) порядка.

Род структуры бинарного отношения называется родом структуры *вполне упорядоченного множества*, если содержит R_5, R_7, R_8, R_{10}, R_{11}; *решётки*, если содержит R_5, R_7, R_8, R_{12}, R_{13}.

Примеры интерпретаций родов структур порядков и их изоморфизмов были рассмотрены в § 2.6.

Вот некоторые примеры интерпретаций рода структуры решётки:

- Всякое линейно нестрого упорядоченное множество. В этом случае для любой пары элементов a, b либо $a \leqslant b$, либо $b \leqslant a$, и, например, если $a \leqslant b$, то $\sup\{a, b\} = b$ и $\inf\{a, b\} = a$.

- Множество всех подмножеств некоторого множества, частично упорядоченное по включению: при этом $\sup\{a, b\} = a \cup b$, $\inf\{a, b\} = a \cap b$.

- Множество натуральных чисел с частичным порядком, при котором $a \leqslant b$ значит «a делит b». Тогда $\sup\{a, b\}$ есть наименьшее общее кратное, а $\inf\{a, b\}$ есть наибольший общий делитель a и b.

- Множество всех действительных функций на отрезке $[0, 1]$, частично упорядоченное условием «$f \leqslant g$, если и только если $\forall t \in [0, 1](f(t) \leqslant g(t))$». Здесь $\sup\{a, b\}$ есть функция, в каждой точке t принимающая значение, равное большему из значений $f(t)$, $g(t)$; аналогично определяется $\inf\{a, b\}$.

8. Родами структур *тернарных отношений* называются роды структур, у которых фигурирующая в типовой характеристике схема S имеет вид $\mathfrak{P}((S_1 \times S_2) \times S_3)$ (или сокращённо $\mathfrak{P}(S_1 \times S_2 \times S_3)$).

Ниже мы будем рассматривать примеры родов структур тернарных отношений на одном множестве, типовая характеристика которых есть $d \in \mathfrak{P}((x \times x) \times x)$, причём род структуры включает в себя аксиомы R_1, R_2 для d, $x \times x$ и x (т. е. d является отображением из $x \times x$ в x). Введём, кроме того, сокращающее обозначение

$a \cdot b \rightleftharpoons \bigcup\{u \in x \mid ((a,b),u) \in d\}$. В силу принятых аксиом, для каждой пары (a,b) существует один и только один u такой, что $((a,b),u) \in d$, поэтому множество $\{u \in x \mid ((a,b),u) \in d\}$ состоит всего из одного элемента, и в силу теоремы 73 терм $a \cdot b$, равный этому самому элементу, биективно переносим. Роды структур, обладающие указанными свойствами, называются *группоидами*.

Изоморфизмом объекта-группоида $\{\xi, \delta\}$ в $\{\xi', \delta'\}$ является такая биекция $\varphi : \xi \leftrightarrow \xi'$, что в наших обозначениях $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

В качестве аксиом для тернарных отношений с указанными свойствами могут быть использованы следующие:

R_{14}: $\forall a \in x, \forall b \in x, \forall c \in x((a \cdot b) \cdot c = a \cdot (b \cdot c))$ — *ассоциативность*,

R_{15}: $\exists e \in x, \forall a \in x(e \cdot a = a)$ — *существование левого нейтрального элемента*,

R_{16}: $\forall a \in x, \exists a' \in x, \forall b((a' \cdot a) \cdot b = b)$ — *существование левого обратного элемента*,

R_{17}: $\forall a \in x, \forall b \in x(a \cdot b = b \cdot a)$ — *коммутативность*.

Род структуры тернарного отношения называется родом структуры *полугруппы*, если содержит R_1, R_2, R_{14}; *моноида*, если содержит R_1, R_2, R_{14}, R_{15}; *группы*, если содержит R_1, R_2, R_{14}, R_{15}, R_{16}; *коммутативной*, или *абелевой, группы*, если содержит R_1, R_2, R_{14}, R_{15}, R_{16}, R_{17}. Из определений следует, что любая интерпретация рода структуры абелевой группы является также интерпретацией рода структуры группы, любая интерпретация рода структуры группы является интерпретацией рода структуры моноида, любая интерпретация рода структуры моноида является интерпретацией рода структуры полугруппы.

Род структуры группы имеет множество интерпретаций, значимых не только в математике, но и в прикладных областях — механике, кристаллографии, криптографии и т. д. Рассмотрим лишь некоторые примеры.

- Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{K}$ целых, рациональных, действительных, комплексных чисел и кватернионов с операцией сложения образуют абелевы группы с нейтральным элементом 0

и обратным для a элементом $-a$. Эти же множества с операцией умножения образуют моноиды (нейтральный элемент — единица), но не группы, т. к. у нуля не существует обратного элемента по умножению. Множества $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ с операцией умножения образуют абелевы группы с нейтральным элементом 1 и обратным элементом $1/a$, множество $\mathbb{K}\setminus\{0\}$ образует группу, не являющуюся абелевой, т. к. умножение кватернионов некоммутативно.

- Множество обратимых матриц размерности $n \times n$ образует группу относительно умножения (нейтральный элемент — единичная матрица, обратный элемент — обратная матрица).

- Множество $\{0, 1, \ldots n-1\}$ натуральных чисел, меньших n, с операцией сложения по модулю n образует абелеву группу с нейтральным элементом 0 и обратным элементом $n-a$. Это же множество с операцией умножения по модулю n образует моноид (нейтральный элемент — единица), но не группу, т. к. по крайней мере у нуля не существует обратного элемента. Множество $\mathbb{Z}_n^*$ натуральных чисел, меньших n и *взаимно простых с* n, с операцией умножения по модулю n образует абелеву группу с нейтральным элементом 1 и существующим для любого $a \in \mathbb{Z}_n^*$ обратным элементом a', таким, что $a'a \bmod n = 1$. (Доказательство последнего утверждения, хотя в целом и несложное, требует некоторого углубления в модулярную арифметику.)

- Пусть x — произвольное множество. Множество всех биекций из x в x с операцией суперпозиции образует группу (нейтральный элемент — тождественное отображение id_x, обратный элемент — обратная функция). Множество x^x всех отображений из x в x с операцией суперпозиции образует моноид (нейтральный элемент — id_x).

- Пусть u — множество множеств, такое, что $\forall a \in u, \forall b \in \in u (a \triangle b \in u)$ (в частности, этому условию удовлетворяют

множества $\mathfrak{P}(x)$ и $\{\varnothing, x\}$ для произвольного x). Множество u с операцией $\triangle$ образует абелеву группу с нейтральным элементом $\varnothing$, обратным элементом к любому a в этой группе является само a (т. к. $a \triangle a = \varnothing$).

9. *Комплексными* будем называть роды структур, у которых фигурирующая в типовой характеристике схема S имеет вид $S_1 \times \times \ldots \times S_n$ при $n \geqslant 2$, что позволяет эквивалентным образом говорить об n родовых константах.

Рассмотрим роды структур с типовой характеристикой $d \in \in \mathfrak{P}((x \times x) \times x) \times \mathfrak{P}((x \times x) \times x)$, что позволяет эквивалентным образом говорить о двух родовых константах $d_1 \in \mathfrak{P}((x \times x) \times x)$ и $d_2 \in \mathfrak{P}((x \times x) \times x)$. Пусть эти роды структур включают в себя аксиомы R_1 и R_2 для обеих констант d_1 и d_2 (т. е. d_1 и d_2 являются отображениями из $x \times x$ в x). Введём, кроме того, сокращающие обозначения $a + b \rightleftharpoons \bigcup\{u \in x \mid ((a, b), u) \in d_1\}$, $a \cdot b \rightleftharpoons \bigcup\{u \in \in x \mid ((a, b), u) \in d_2\}$ (знак $+$ для d_1, знак $\cdot$ для d_2). Эти термы будут биективно переносимы по той же причине, что и терм $a \cdot b$ для рода структуры полугруппы. Примем, кроме того, традиционное соглашение о том, что операция $\cdot$ имеет более высокий приоритет, чем операции $+$, т. е. выражение $a+b\cdot c$ следует читать как $a+(b\cdot c)$.

В качестве аксиом могут быть использованы следующие:

R_{18}: $\forall a \in x, \forall b \in x, \forall c \in x(a \cdot (b + c) = a \cdot b + a \cdot c)$ — *дистрибутивность сложения слева,*

R_{19}: $\forall a \in x, \forall b \in x, \forall c \in x((a + b) \cdot c = a \cdot c + b \cdot c)$ — *дистрибутивность сложения справа,*

R_{20}: $\forall a \in x, \forall b \in x, \forall c \in x(a + b \cdot c = (a + b) \cdot (a + c))$ — *дистрибутивность умножения слева,*

R_{21}: $\forall a \in x, \forall b \in x, \forall c \in x(a \cdot b + c = (a + c) \cdot (b + c))$ — *дистрибутивность умножения справа,*

R_{22}: $\forall a \in x, \forall b \in x(a \cdot (a + b) = a)$ — *первый закон поглощения,*

R_{23}: $\forall a \in x, \forall b \in x(a + a \cdot b = a)$ — *второй закон поглощения.*

Комплексный род структуры с двумя тернарными отношениями называется *полукольцом*, если содержит аксиомы моноида

и коммутативности для d_1 (сложения), полугруппы для d_2 (умножения), а также аксиомы дистрибутивности через сложение R_{18}, R_{19}.

Комплексный род структуры с двумя тернарными отношениями называется *кольцом*, если содержит аксиомы абелевой группы для d_1 (сложения), полугруппы для d_2 (умножения), а также аксиомы дистрибутивности через сложение R_{18}, R_{19}.

Пусть дан род структуры кольца. Обозначим символом 0 терм, выражающий в этом роде структуры нейтральный элемент операции сложения. Кольцо называется *телом*, если элементы множества $x \setminus \{0\}$ образуют группу на d_2 (группу умножения). Тело называют *полем*, если данная группа является абелевой.

Рассмотрим некоторые интерпретации этих родов структур.

- Множества $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ рациональных, действительных и комплексных чисел с операциями сложения и умножения образуют поля. Множество вида $\{0, 1, \ldots p-1\}$, где p — простое число, с операциями сложения и умножения по модулю p, образует поле.

- Множество $\mathbb{K}$ кватернионов с операциями сложения и умножения образует тело, не являющееся полем, т. к. умножение кватернионов не коммутативно.

- Множество $\mathbb{Z}$ целых чисел с операциями сложения и умножения образует кольцо. Множество вида $\{0, 1, \ldots n-1\}$ натуральных чисел, меньших n, с операциями сложения и умножения по модулю n, в общем случае образует кольцо.

- Множество u, такое, что $\forall a \in u, \forall b \in u (a \triangle b \in u \,\&\, a \cap b \in u) \,\&\, \exists e \in u, \forall a \in u (a \subseteq e)$ с операцией $\triangle$, трактуемой как сложение, и $\cap$, трактуемой как умножение с нейтральным элементом e и без обратного элемента, образует кольцо. В частности, указанным условиям удовлетворяют множества $\mathfrak{P}(x)$ и $\{\varnothing, x\}$ для произвольного x.

- Множество натуральных чисел с обычными операциями сложения и умножения образует полукольцо.

Комплексный род структуры с двумя тернарными отношениями называется *алгебраической решёткой*, если содержит аксиомы полугруппы для сложения и умножения, сложение и умножение коммутативны, а также введены аксиомы поглощения R_{22}, R_{23}.

10. Дополним род структуры алгебраической решётки ещё тремя родовыми константами: $d_3 \in \mathfrak{P}(x \times x)$, $d_4 \in x$, $d_5 \in x$. Добавим аксиомы всюдуопределённости и прямой однозначности (R_1 и R_2) для d_3, так что d_3 будет отображением x в x и введём сокращающее обозначение биективно переносимого терма $\bar{a} \rightleftharpoons \bigcup\{u \in x \mid (a, u) \in \in d_3\}$.

С операциями $a + b$ и $a \cdot b$ операцию $\bar{a}$ могут связывать следующие соотношения:

R_{24}: $\forall a \in x(a \cdot \bar{a} = d_4)$ — *первый закон дополнительности,*

R_{25}: $\forall a \in x(a + \bar{a} = d_5)$ — *второй закон дополнительности.*

Добавив к аксиомам алгебраической решётки все четыре аксиомы дистрибутивности R_{18}, R_{19}, R_{20}, R_{21} и аксиомы дополнительности R_{24}, R_{25}, получим род структуры *булевой алгебры.*

Рассмотрим две интерпретации рода структуры булевой алгебры.

- Пусть $\mathfrak{f} = \varnothing$, $\mathfrak{t} = \{\varnothing\}$, множество x интерпретируется термом $\{\mathfrak{f}, \mathfrak{t}\}$, d_4 и d_5 — термами $\mathfrak{f}$ и $\mathfrak{t}$ соответственно. Коль скоро элементы x — истинностные значения, то входящие в род структуры отображения можно проинтерпретировать следующим образом: $a \cdot b$ как $a \,\&\, b$, $a + b$ как $a \vee b$, $\bar{a}$ как $\neg a$. Легко проверить, что аксиомы рода структуры булевой алгебры (которые состоят, напомним, из аксиом алгебраической решётки, дистрибутивности и дополнительности) при этом выполняются.

- Пусть теперь v — произвольное множество, x интерпретируется как $\mathfrak{P}(v)$ (множество всех подмножеств v), d_4 и d_5 — термами $\varnothing$ и v соответственно. Пусть $a \cdot b = a \cap b$, $a + b = a \cup b$,

$\bar{a} = v \setminus a$. Легко проверить, что и в этом случае все аксиомы рода структуры булевой алгебры выполняются, а предыдущий пример является частным случаем для $v = \{\varnothing\}$.

Все роды структур, базирующиеся на отображениях из декартова произведения элементов x в x (в частности, все рассмотренные нами тернарные отношения и комплексные роды структур), называются *алгебраическими структурами* и являются предметом изучения в абстрактной алгебре. Здесь упомянуты только самые базовые алгебраические структуры, в действительности их гораздо больше.

11. Рассмотрим роды структур с типовой характеристикой $d \in \mathfrak{PP}(x)$.

R_{26}: $\forall a \in x, \exists g \in d(a \in g)$ — *элементы d полностью покрывают множество x,*

R_{27}: $\forall g_1 \in d, \forall g_2 \in d((g_1 \cap g_2 = \varnothing) \vee (g_1 = g_2))$ — *любые два элемента из d либо не пересекаются, либо совпадают,*

R_{28}: $\forall g \subseteq d(\bigcup g \in d)$ — *множество-объединение любого подмножества d принадлежит d,*

R_{29}: $\forall a \in d, \forall b \in d(a \cap b \in d)$ — *пересечение пары любых элементов d принадлежит d,*

R_{30}: $x \in d$ — *x принадлежит d,*

R_{31}: $\varnothing \notin d$ — *пустое множество не принадлежит d,*

R_{32}: $\forall a \in d, \forall b \subseteq x(a \subseteq b \Rightarrow b \in d)$ — *надмножество любого элемента d является элементом d,*

R_{33}: $\forall g \subseteq x(g \in d \vee x \setminus g \in d)$ — *для любого подмножества x либо оно само, либо его дополнение до x принадлежит d.*

Род структуры с рассматриваемой типовой характеристикой называется *фактормножеством*, или *разбиением множества*, если содержит аксиомы R_{26} и R_{27}; *топологическим пространством*, если содержит аксиомы R_{28}, R_{29}, R_{30} (множество d при этом интерпретируется как множество всех открытых множеств); *фильтром на множестве*, если содержит аксиомы R_{29}, R_{30}, R_{31}, R_{32}; *уль-*

трафильтром на множестве, если содержит аксиомы R_{29}, R_{30}, R_{31}, R_{32}, R_{33}.

12. Другой способ задать топологическое пространство — использовать типовую характеристику $d \in \mathfrak{P}(\mathfrak{P}(x) \times \mathfrak{P}(x))$, где d интерпретируется как функция, ставящая в соответствие множеству точек топологического пространства его замыкание. Таким образом, род структуры топологии на базе типизации $d \in \mathfrak{P}(\mathfrak{P}(x) \times \times \mathfrak{P}(x))$ должен содержать аксиомы R_1, R_2 для d и $\mathfrak{P}(x)$. Определим сокращающее обозначение $[a] \rightleftharpoons \bigcup\{u \in \mathfrak{P}(x) \mid (a, u) \in d\}$ для терма, обозначающего замыкание множества a. Род структуры топологии в этом случае должен содержать также аксиомы

R_{34}: $\forall a \in \mathfrak{P}(x)(a \subseteq [a])$ — *замыкание множества есть надмножество исходного множества,*

R_{35}: $\forall a \in \mathfrak{P}(x)([[a]] = [a])$ — *идемпотентность замыкания,*

R_{36}: $\forall a \in \mathfrak{P}(x), \forall b \in \mathfrak{P}(x)([a \cup b] = [a] \cup [b])$ — *замыкание объединения пары множеств есть объединение замыканий данных множеств,*

R_{37}: $[\varnothing] = \varnothing$ — *замыкание пустого множества есть пустое множество.*

13. Рассмотрим род структуры *линейного векторного пространства над полем* $\mathbb{R}$ *действительных чисел.* Он содержит две родовых константы: $d_1 \in \mathfrak{P}((x \times x) \times x)$, задающую операцию сложения векторов, и $d_2 \in \mathfrak{P}((\mathbb{R} \times x) \times x)$, задающую умножение вектора на скаляр. Соответствующие варианты аксиом всюдуопределённости и прямой однозначности (R_1 и R_2) вводятся для d_1 и d_2, что позволяет воспользоваться стандартными знаками $+$ и $\cdot$. Относительно операции сложения векторов вводятся аксиомы абелевой группы. Относительно операции умножения вектора на скаляр должны быть введены следующие аксиомы (по традиции и для удобства будем выделять жирным шрифтом переменные, типизированные как элементы множества x):

R_{38}: $\forall a \in \mathbb{R}, \forall b \in \mathbb{R}, \forall \mathbf{c} \in x((a \cdot b) \cdot \mathbf{c} = a \cdot (b \cdot \mathbf{c}))$ — *ассоциативность умножения на скаляр.* Заметим, что здесь выражение $a \cdot b$ должно пониматься как произведение действительных чи-

сел, во всех же остальных случаях знак $\cdot$ трактуется как операция, задаваемая константой d_2.

R_{39}: $\forall a \in \mathbb{R}, \forall b \in \mathbb{R}, \forall \mathbf{c} \in x((a+b)\cdot\mathbf{c} = a\cdot\mathbf{c} + b\cdot\mathbf{c})$ — *дистрибутивность скалярной суммы.* Заметим, что в левой части равенства выражение $a+b$ должно пониматься как сумма действительных чисел, в правой же части равенства знак $+$ трактуется как операция, задаваемая константой d_1.

R_{40}: $\forall a \in \mathbb{R}, \forall \mathbf{b} \in x, \forall \mathbf{c} \in x(a\cdot(\mathbf{b}+\mathbf{c}) = a\cdot\mathbf{b} + a\cdot\mathbf{c})$ — *дистрибутивность векторной суммы.*

R_{41}: $\forall \mathbf{c} \in x(1\cdot\mathbf{c} = \mathbf{c})$ — *единица служит нейтральным элементом умножения на скаляр.* В этом случае знак 1 указывает на нейтральный элемент операции умножения поля $\mathbb{R}$, т. е. на действительное число 1.

Род структуры линейного пространства над полем $\mathbb{C}$ комплексных чисел строится аналогичным образом.

14. Вывод структур. Пусть дан род структуры Σ на n базисных множествах $x_1, \ldots x_n$ с типовой характеристикой T_Σ вида $d_\Sigma \in S_\Sigma[x_1, \ldots x_n]$ и аксиомой R_Σ. Пусть также дан род структуры Θ, который построен на базисных множествах $x_{n+1}, \ldots x_{n+m}$, с типовой характеристикой T_Θ вида $d_\Theta \in S_\Theta[x_{n+1}, \ldots x_{n+m}]$ и аксиомой R_Θ.

Терм $(\psi_1, \ldots \psi_m, \zeta)$ называется *способом вывода структуры рода* Θ *из структуры рода* Σ, если он

1) биективно переносим при типизации T_Σ;

2) не содержит никаких параметров, кроме, возможно, $x_1, \ldots x_n, d_\Sigma$;

3) соотношение $(\psi_1 \mid x_{n+1}) \ldots (\psi_m \mid x_{n+m})(\zeta \mid d_\Theta)(T_\Theta \,\&\, R_\Theta)$ является теоремой Σ.

Всякий терм, удовлетворяющий первым двум из перечисленных условий, называется *внутренним термом* Σ.

Если дан Σ-объект $(\xi_1, \dots \xi_n, \delta)$ и способ вывода $(\psi_1, \dots \psi_m, \zeta)$ структуры рода Θ из структуры рода Σ, то, очевидно, терм

$$(\xi_1 \mid x_1) \dots (\xi_n \mid x_n)(\delta \mid d_\Sigma)(\psi_1, \dots \psi_m, \zeta)$$

будет являться Θ-объектом. Мы будем говорить, что Θ-объект рассматриваемого вида является *подчинённым* Σ*-объекту* $(\xi_1, \dots \xi_n, \delta)$ *посредством способа вывода* $(\psi_1, \dots \psi_m, \zeta)$.

Если имеется способ вывода Θ из Σ, то для всякой теоремы B рода структуры Θ формула $(\psi_1 \mid x_{n+1}) \dots (\psi_m \mid x_{n+m})(\zeta \mid d_\Theta)B$ будет, как легко убедиться, теоремой рода структуры Σ.

Часто имеет место случай, когда удаётся построить такой способ вывода, что термы $\psi_1, \dots \psi_m$ совпадают с некоторыми из базисных множеств Σ $x_1, \dots x_n$. В этом случае подчинённый Θ-объект называют *нижележащим* по отношению к Σ-объекту $(\xi_1, \dots \xi_n, \delta)$.

Наконец, если T_Θ совпадает с T_Σ и аксиома R_Θ отсутствует либо имеет место $\mathcal{T} \vdash R_\Sigma \Rightarrow R_\Theta$, то способ вывода Θ из Σ особенно прост и представляет собой терм

$$(x_1, \dots x_n, d_\Sigma).$$

Иначе говоря, в этом случае любой Σ-объект является также и Θ-объектом. В этом случае говорят, что род структуры Σ *богаче* рода структуры Θ.

Рассмотрим примеры.

- Род структуры биекции богаче родов структур инъекции и сюръекции, т. к. отличается от инъекции наличием аксиомы R_3 и от сюръекции наличием аксиомы R_4. Вследствие этого каждая биекция является также и инъекцией, и сюръекцией, способ вывода тривиален: (x_1, x_2, d).

- Род структуры абелевой группы богаче рода структуры группы, род структуры группы богаче рода структуры моноида, род структуры моноида богаче рода структуры полугруппы. Род структуры поля богаче рода структуры тела, род

структуры тела богаче рода структуры кольца, род структуры кольца богаче рода структуры полукольца.

- Род структуры нестрогого линейного порядка богаче рода структуры решётки, т. к. всякий объект, удовлетворяющий аксиомам нестрогого линейного порядка, удовлетворяет также и аксиомам решётки.

- Пусть дан род структуры булевой алгебры, построенный на базисном множестве x и родовых константах $d_1,\ldots d_5$. Тогда (x, d_1, d_2) является способом вывода рода структуры алгебраической решётки из рода структуры булевой алгебры. Решётка (x, d_1, d_2) при этом является нижележащей по отношению к булевой алгебре $(x, d_1, \ldots d_5)$.

- Пусть дан некоторый произвольный род структуры, содержащий базисное множество x. Терм $(x^x, \{((u, v), w) \in (\mathfrak{P}(x \times \times x) \times \mathfrak{P}(x \times x)) \times \mathfrak{P}(x \times x) \mid u \in x^x \,\&\, v \in x^x \,\&\, w = u \circ v\})$ есть способ вывода рода структуры моноида из произвольного рода структуры. Напомним, что x^x обозначает множество всех отображений x на себя, $u \circ v$ — суперпозицию отображений, множество всех отображений множества на себя образует моноид по операции суперпозиции с нейтральным элементом id_x.

Упр. 97. Пусть Σ представляет собой род структуры топологии с типовой характеристикой $d_1 \in \mathfrak{P}\mathfrak{P}(x)$, интерпретируемой как множество всех открытых подмножеств x. Дополним также Σ родовой константой $d_2 \in x$, выделяющей в x некоторую точку. 1) Постройте терм ζ, являющийся внутренним термом Σ, равный множеству всех открытых окрестностей точки d_2. 2) Покажите, что (x, ζ) есть способ вывода рода структуры фильтра из рода структуры Σ.

Упр. 98. Постройте способ вывода рода структуры разбиения из рода структуры функции из x_1 в x_2. Указание: разбиение строится на множестве x_1.

15. Эквивалентные роды структур. Пусть Σ и Θ — два ро-

да структуры с родовыми константами d_Σ и d_Θ, удовлетворяющие следующим условиям:

1) Σ и Θ имеют одни и те же базисные множества $x_1, \ldots x_n$;

2) имеются способ вывода $(x_1, \ldots x_n, \zeta)$ Θ из Σ и способ вывода $(x_1, \ldots x_n, \omega)$ Σ из Θ;

3) соотношение $(\zeta \mid d_\Theta)\omega = d_\Sigma$ является теоремой Σ и соотношение $(\omega \mid d_\Sigma)\zeta = d_\Theta$ является теоремой Θ.

В этом случае говорят, что роды структур Σ и Θ эквивалентны посредством способов вывода $(x_1, \ldots x_n, \zeta)$ и $(x_1, \ldots x_n, \omega)$.

Третье условие обеспечивает взаимную однозначность соответствия между Σ и Θ-объектами через термы ζ и ω. Если $(\xi_1, \ldots \xi_n, \delta_\Sigma)$ и $(\xi_1, \ldots \xi_n, \delta_\Theta)$ есть соответственно Σ и Θ-объекты, такие, что $\mathcal{T}' \vdash (\delta_\Sigma \mid d_\Sigma)\zeta = \delta_\Theta$ (в силу условия 3 это имеет место тогда и только тогда, когда $\mathcal{T}' \vdash (\delta_\Theta \mid d_\Theta)\omega = \delta_\Sigma$ — проверьте самостоятельно), то объекты $(\xi_1, \ldots \xi_n, \delta_\Sigma)$ и $(\xi_1, \ldots \xi_n, \delta_\Theta)$ называют *эквивалентными*.

Наконец, эквивалентные роды структур обладают тем свойством, что для всякой теоремы B рода структуры Θ формула $(\zeta \mid d_\Theta)B$ будет теоремой рода структуры Σ и для всякой теоремы C рода структуры Σ формула $(\omega \mid d_\Sigma)C$ будет теоремой рода структуры Θ.

Рассмотрим примеры.

- Род структуры отношения эквивалентности эквивалентен роду структуры разбиения множества. Действительно: пусть d_Σ задаёт отношение эквивалентности, d_Θ — разбиение на базисном множестве x. В этом случае фактормножество $x/d_\Sigma = \{u \in \mathfrak{P}(x) \mid \exists a \in x(u = \{t \in x \mid (t, a) \in d_\Sigma\})\}$ есть способ ζ вывода разбиения из отношения эквивалентности, а терм $\{t \in x \times x \mid \exists v \in d_\Theta(\mathrm{pr}_1(t) \in v \;\&\; \mathrm{pr}_2(t) \in v)\}$ есть способ ω вывода отношения эквивалентности из разбиения, как показано в теореме 49. Убедимся, что $(\zeta \mid d_\Theta)\omega = d_\Sigma$ в Σ. В самом

деле: $\{t \in x \times x \mid \exists v \in \mathfrak{P}(x), \exists a \in x(v = \{g \in x \mid (g,a) \in d_\Sigma\}$ & & $\mathrm{pr}_1(t) \in v$ & $\mathrm{pr}_2(t) \in v)\} = \{t \in x \times x \mid \exists a \in x(\mathrm{pr}_1(t) \in x$ & & $(\mathrm{pr}_1(t), a) \in d_\Sigma$ & $\mathrm{pr}_2(t) \in x$ & $(\mathrm{pr}_2(t), a) \in d_\Sigma)\} = \{t \in x \times$ $\times x \mid (\mathrm{pr}_1(t), \mathrm{pr}_2(t)) \in d_\Sigma\} = d_\Sigma$. Аналогичным образом можно проверить, что $(\omega \mid d_\Sigma)\zeta = d_\Theta$ в Θ.

- Род структуры решётки эквивалентен роду структуры алгебраической решётки.

  Действительно, пусть d_Σ задаёт род структуры решётки, $d_\Theta = (d^1_\Theta, d^2_\Theta)$ — род структуры алгебраической решётки. Обозначим для любой пары элементов a, b через $\inf\{a,b\}$ — их точную нижнюю грань, через $\sup\{a,b\}$ их точную верхнюю грань. В силу аксиом решётки точная верхняя и точная нижняя грани существуют у любой пары элементов. Тогда терм $(\{(a,b,c) \in x \times x \times x \mid c = \sup\{a,b\}\}, \{(a,b,c) \in x \times x \times$ $\times x \mid c = \inf\{a,b\}\})$ есть способ вывода рода структуры алгебраической решётки из рода структуры решётки. Иначе говоря, мы отождествляем значение $\sup\{a,b\}$ со значением $a + b$, $\inf\{a,b\}$ — с $a \cdot b$. Легко проверить, что так введённые операции $+$ и $\cdot$ коммутативны, ассоциативны и удовлетворяют аксиомам поглощения.

  С другой стороны, рассмотрим терм $\{t \in x \times x \mid (\mathrm{pr}_1(t), \mathrm{pr}_2(t), \mathrm{pr}_2(t)) \in d^1_\Theta$ & $(\mathrm{pr}_1(t), \mathrm{pr}_2(t), \mathrm{pr}_1(t)) \in d^2_\Theta\}$. Иначе говоря, мы считаем, что $a \leqslant b$ тогда и только тогда, когда $a \cdot b = a$ и $a + b = b$. Нетрудно проверить, что данный терм является способом вывода рода структуры решётки из рода структуры алгебраической решётки, а также что $(\zeta \mid d_\Theta)\omega =$ $= d_\Sigma$ в Σ и $(\omega \mid d_\Sigma)\zeta = d_\Theta$ в Θ.

- Два указанных выше способа определения топологических пространств (путём задания множества открытых множеств и операции замыкания множества) эквивалентны. Пусть d_Σ задаёт множество открытых множеств топологического пространства, d_Θ — операцию замыкания.

Исходя из множества открытых множеств d_Σ, определим понятие *точки прикосновения к множеству* следующим образом: a есть точка прикосновения к множеству u, если любое открытое множество, содержащее a, содержит также хотя бы одну точку u. Терм, задающий множество всевозможных пар «$u \subseteq x$, совокупность всех точек прикосновения к u» является способом вывода рода структуры Θ из Σ: можно проверить, что если действие этого терма на множество $u \subseteq x$ обозначить как $[u]$, то при этом выполняются свойства $u \subseteq [u]$, $[[u]] = [u]$, $[u \cup v] = [u] \cup [v]$, $[\varnothing] = \varnothing$.

С другой стороны, исходя из операции замыкания, заданной с помощью d_Θ, можно определить множество всех замкнутых множеств пространства как множество множеств u, таких, что $[u] = u$, и множество всех открытых множеств пространства как множество множеств u, таких, что $x \setminus u$ есть замкнутое множество. Так определённое множество всех открытых множеств пространства является способом вывода рода структуры Σ из Θ, и можно проверить, что аксиомы топологического пространства и требования $(\zeta \mid d_\Theta)\omega = d_\Sigma$ и $(\omega \mid d_\Sigma)\zeta = d_\Theta$ выполняются.

Упр. 99. Докажите, что род структуры частичного нестрогого порядка эквивалентен роду структуры частичного строгого порядка.

Рассмотренные примеры показывают, что в определённом смысле одна и та же математическая конструкция может быть определена в родах структур внешне совершенно разными способами.

§ 3.3. Операции над родами структур

1. Операциями над родами структур называются формальные преобразования, позволяющие из существующих текстов родов структур получать новые роды структур с некоторыми заранее определёнными свойствами. Наибольшее прикладное значение

имеют операция порождения множества структур данного рода и операция синтеза.

2. Порождение множества структур данного рода. Пусть дан род структуры Σ, имеющий типовую характеристику $d \in S[x_1, \dots x_n]$ и класс Σ-объектов $\mathcal{K}_\Sigma$. Операция порождения множества структур данного рода позволяет в этом случае построить из Σ такой род структуры $\tilde{\Sigma}$, что класс $\tilde{\Sigma}$-объектов будет удовлетворять условию

$$\mathcal{K}_{\tilde{\Sigma}} = \{(x_1, \dots x_n, \tilde{d}) \mid \forall d(d \in \tilde{d} \Rightarrow (x_1, \dots x_n, d) \in \mathcal{K}_\Sigma)\}.$$

Например, если Σ есть род структуры функции из x_1 в x_2, то $\tilde{\Sigma}$, получаемый из него операцией порождения множества структур данного рода, есть род структуры *множества* функций из x_1 в x_2. В $\tilde{\Sigma}$-объекте элементами множества, соответствующего родовой константе, являются множества, которые могут интерпретировать родовую константу Σ при фиксированной интерпретации базисных множеств.

Построить $\tilde{\Sigma}$ можно по следующим правилам:

1) базисные множества не изменяются;

2) типовая характеристика T вида $d \in S[x_1, \dots x_n]$ заменяется на $\tilde{T}$ вида $\tilde{d} \in \mathfrak{P}S[x_1, \dots x_n]$;

3) аксиома R заменяется на аксиому $\tilde{R}$ вида

$$\forall u \in \tilde{d}((u \mid d)R).$$

Как видим, родовая константа в этом процессе превращается во множество, каждый элемент которого типизирован как исходная родовая константа. Заметим, что прежние выражения для внутренних термов Σ теряют смысл в $\tilde{\Sigma}$ в силу изменения типизации родовой константы.

Рассмотрим пример. Пусть x_1 и x_2 — базисные множества, тогда

- род структуры функции Σ:

  $d \in \mathfrak{P}(x_1 \times x_2)$;

  $R_1 : \forall u \in x_1, \exists v \in x_2((u, v) \in d)$;

  $R_2 : \forall t_1 \in d, \forall t_2 \in d(\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$;

- род структуры множества функций $\tilde{\Sigma}$:

  $\tilde{d} \in \mathfrak{P}\mathfrak{P}(x_1 \times x_2)$;

  $R_1 : \forall z \in \tilde{d}, \forall u \in x_1, \exists v \in x_2((u, v) \in z)$;

  $R_2 : \forall z \in \tilde{d}, \forall t_1 \in z, \forall t_2 \in z(\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$.

Теорема 77. *Если $\tilde{\Sigma}$ построена из Σ при помощи операции порождения структур данного рода, то класс $\tilde{\Sigma}$-объектов удовлетворяет условию*

$$\mathcal{K}_{\tilde{\Sigma}} = \{(x_1, \ldots x_n, \tilde{d}) \mid \forall d(d \in \tilde{d} \Rightarrow (x_1, \ldots x_n, d) \in \mathcal{K}_\Sigma)\}.$$

$\lhd$В силу определения $\mathfrak{P}$, $\tilde{T} \sim \tilde{d} \in \mathfrak{P}S[x_1, \ldots x_n] \sim \forall d(d \in \tilde{d} \Rightarrow$ $\Rightarrow d \in S[x_1, \ldots x_n])$, откуда $\tilde{T} \sim \forall d(d \in \tilde{d} \Rightarrow T)$. По определению $\tilde{R} \sim \forall d(d \in \tilde{d} \Rightarrow R)$, из чего следует

$$\tilde{T}\ \&\ \tilde{R} \sim \forall d(d \in \tilde{d} \Rightarrow T\ \&\ R),$$

откуда и вытекает требуемое.$\rhd$

Род структуры $\tilde{\Sigma}$, полученный операцией порождения множества структур данного рода, заведомо непротиворечив, т. к. $(\xi_1, \ldots \xi_n, \varnothing)$ есть, как легко видеть, $\tilde{\Sigma}$-объект при любых множествах $\xi_1, \ldots \xi_n$.

Упр. 100. Докажите, что среди $\tilde{\Sigma}$-объектов $(\xi_1, \ldots \xi_n, \tilde{\delta})$ существуют объекты с непустым $\tilde{\delta}$ тогда и только тогда, когда Σ непротиворечив.

Теорема 78. *Если F — теорема Σ, то формула $\tilde{F}$ вида $\forall u \in$ $\in \tilde{d}(u \mid d)F$ есть теорема $\tilde{\Sigma}$.*

◁При доказательстве предыдущей теоремы было установлено, что

$$\vdash \tilde{T} \,\&\, \tilde{R} \Rightarrow \forall u(u \in \tilde{d} \Rightarrow (u \mid d)(T \,\&\, R)).$$

Но если $\mathcal{T}' \vdash T \,\&\, R \Rightarrow F$, то $\mathcal{T}' \vdash (u \mid d)(T \,\&\, R) \Rightarrow (u \mid d)F$, и

$$\mathcal{T}' \vdash \tilde{T} \,\&\, \tilde{R} \Rightarrow \forall u(u \in \tilde{d} \Rightarrow (u \mid d)F),$$

т. е. $\tilde{F}$ — теорема $\tilde{\Sigma}$.▷

3. Синтез родов структур. Потребность в синтезе родов структур возникает, когда имеется набор родов структур, описывающих различные аспекты изучаемой области, и требуется построить обобщающий, комплексный род структуры. Пусть даны род структуры Σ с типовой характеристикой T_Σ и аксиомой R_Σ и род структуры Θ с типовой характеристикой T_Θ и аксиомой R_Θ. Теоретико-множественные интерпретации Σ и Θ будут рассматриваться в некоторой единой теории $\mathcal{T}'$.

Везде в дальнейшем мы будем предполагать, что имена всех конституэнт выбраны таким образом, что ни одно имя конституэнты (за исключением, может быть, имён вспомогательных базисных множеств) из Σ не встречается среди имён конституэнт Θ: простой перенумерацией конституэнт одной из родовых структур этого всегда можно добиться. Таким образом, текст, полученный простым объединением текстов Σ и Θ, является родом структуры с типовой характеристикой $T_\Sigma \,\&\, T_\Theta$ и аксиомой $R_\Sigma \,\&\, R_\Theta$. Всякая пара, состоящая из Σ- и Θ-объектов, будет его объектом, поэтому класс теоретико-множественных интерпретаций такого рода структуры будет в некотором смысле равен $\mathcal{K}_\Sigma \times \mathcal{K}_\Theta$ и не будет пустым, если одновременно не пусты $\mathcal{K}_\Sigma$ и $\mathcal{K}_\Theta$.

Обычного слияния текстов родов структур бывает недостаточно: часто к получившемуся роду структуры необходимо добавлять утверждения о тождестве некоторых множеств Σ некоторым множествам Θ.

Рассмотрим пример. Предположим, что имеется род структуры Σ линейного векторного пространства над полем действительных чисел $\mathbb{R}$ с базисным множеством векторов x_1 и родовой кон-

стантой $d_1 \in \mathfrak{P}(x_1 \times x_1 \times x_1) \times \mathfrak{P}(\mathbb{R} \times x_1 \times x_1)$. Пусть далее имеется род структуры Θ множества функций из x_2 в x_3 с родовой константой $d_2 \in \mathfrak{P}\mathfrak{P}(x_2 \times x_3)$. Объединив тексты этих родов структур и отождествив множество функций с базисным множеством векторов, т. е. добавив условие $d_2 = x_1$, мы получим систему, некоторым образом описывающую линейные пространства над множеством функций. Эта система, однако, не будет являться родом структуры, т. к. соотношение $d_2 = x_1$ не является биективно переносимым. Но мы можем обойти эту ситуацию следующим образом: отбросить базисное множество x_1, родовую константу d_1 заменить на $\tilde{d} \in \mathfrak{P}(\mathfrak{P}(x_2 \times \times x_3) \times \mathfrak{P}(x_2 \times x_3) \times \mathfrak{P}(x_2 \times x_3)) \times \mathfrak{P}(\mathbb{R} \times \mathfrak{P}(x_2 \times x_3) \times \mathfrak{P}(x_2 \times x_3))$, добавить аксиому $\tilde{d} \in \mathfrak{P}(d_2 \times d_2 \times d_2) \times \mathfrak{P}(\mathbb{R} \times d_2 \times d_2)$ и по всему тексту заменить x_1 на d_2. Получившаяся система уже будет родом структуры с вполне корректной типовой характеристикой и биективно переносимой аксиомой, класс теоретико-множественных интерпретаций которого представляет собой класс линейных пространств функций над полем действительных чисел.

Подобную процедуру мы можем проделать в любом случае, когда базисное множество Σ отождествляется с термом рода структуры Θ типа $\mathfrak{P}(S)$ (т. е. с термом, имеющим характер множества, но не элемента или кортежа). Разумеется, чтобы привести типизацию этого терма к нужному виду, можно воспользоваться операцией порождения множества структур данного рода над Θ.

Рассмотрим ещё один, прикладной, пример: пусть имеется род структуры, описывающий «теорию субординации» в организации, в котором задано множество сотрудников x_1, и на этом множестве введено отношение «подчинения» $d_1 \in \mathfrak{P}(x_1 \times x_1)$. Пусть, кроме этого, имеется род структуры, описывающий «теорию родства», в котором задано множество людей x_2 и на этом множестве введено отношение «быть родителем» $d_2 \in \mathfrak{P}(x_2 \times x_2)$. Если теперь отождествить множество сотрудников в первой теории и людей во второй (что в рассматриваемом случае можно сделать простой заменой x_1 на x_2 по всему тексту рода структуры), то в синтезированной теории будет выразимо и отношение «подчинения», и от-

ношение «быть родителем». Также можно будет образовать принципиально новые термы, в которых используются оба эти отношения. Например, терм «множество подчинённых, которые являются детьми своего начальника».

Таким образом, в синтезированном роде структуры (если такой можно построить) появляется возможность выводить термы и формулировать утверждения, невыразимые в синтезируемых родах структур.

Теперь перейдём к формальному определению. Пусть даны

1) род структуры Σ (который будем называть конкретизируемым родом структуры) с выделенными в нём p базисными множествами. Без ограничения общности можно считать, что Σ построен на n базисных множествах $x_1, \dots x_n$, из которых выделены p первых $x_1, \dots x_p$, $p \leqslant n$, и имеет родовую константу d_Σ, типовую характеристику T_Σ вида $d_\Sigma \in \in S_\Sigma[x_1, \dots x_n]$ и аксиому R_Σ;

2) род структуры Θ (который будем называть конкретизирующим родом структуры) с выделенными в нём p внутренними термами[3] $\psi_1, \dots \psi_p$ с типами $\mathfrak{P}(S_1), \dots \mathfrak{P}(S_p)$, причём не исключается случай, когда любой из ψ_i совпадает либо с базисным множеством Θ, либо с родовой константой Θ. Без ограничения общности можно считать, что Θ построен на m базисных множествах $x_{n+1}, \dots x_{n+m}$ и имеет родовую константу d_Θ, типовую характеристику T_Θ вида $d_\Theta \in \in S_\Theta[x_{n+1}, \dots x_{n+m}]$ и аксиому R_Θ.

В этом случае мы будем говорить, что Σ и Θ удовлетворяют условиям синтеза.

Рассмотрим класс

$$\tilde{\mathcal{K}} = \{(x_1, \dots x_n, d_\Sigma, x_{n+1}, \dots x_{n+m}, d_\Theta) \mid (T_\Sigma \,\&\, R_\Sigma \,\&\, T_\Theta \,\&\, R_\Theta \,\&\, (\psi_1 = x_1) \,\&\, \dots \,\&\, (\psi_p = x_p))\}.$$

[3] Напомним, что биективно переносимый при типовой характеристике рода структуры Σ терм называется внутренним, если не содержит никаких параметров, кроме, возможно, базисных множеств и родовой константы Σ.

Это есть интересующий нас класс пар вида «Σ-объект, Θ-объект», таких, что базисные множества $x_1, \dots x_p$ рода структуры Σ тождественны термам $\psi_1, \dots \psi_p$ рода структуры Θ. Но коль скоро термы $\psi_1, \dots \psi_p$ могут быть вычислены при данных $x_{n+1}, \dots x_{n+m}, d_\Theta$, то каждому элементу $\tilde{\mathcal{K}}$ можно поставить во взаимно однозначное соответствие элемент класса

$$\mathcal{K}_{\tilde{\Sigma}} = \{(x_{p+1}, \dots x_n, d_\Sigma, x_{n+1}, \dots x_{n+m}, d_\Theta) \mid (\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma \,\&\, T_\Theta \,\&\, R_\Theta)\}.$$

Если $(\xi_1, \dots \xi_n, \delta_\Sigma, \xi_{n+1}, \dots \xi_{n+m}, \delta_\Theta) \in \tilde{\mathcal{K}}$, то отбрасывание из этого кортежа компонентов $\xi_1, \dots \xi_p$ даёт в силу свойств равенства (теорема 29) элемент класса $K_{\tilde{\Sigma}}$; если же дан элемент $(\xi_{p+1}, \dots \xi_n, \delta_\Sigma, \xi_{n+1}, \dots \xi_{n+m}, \delta_\Theta) \in K_{\tilde{\Sigma}}$, то добавление компонентов $(\xi_{n+1} \mid x_{n+1}) \dots (\xi_{n+m} \mid x_{n+m})(\delta_\Theta \mid d_\Theta)\psi_i$, $i = 1, \dots p$ в качестве первых p множеств ξ_i даёт, опять же в силу свойств равенства, элемент класса $\tilde{\mathcal{K}}$.

В определении класса $\mathcal{K}_{\tilde{\Sigma}}$ отсутствуют не переносимые биективно условия $(\psi_1 = x_1) \,\&\, \dots \,\&\, (\psi_p = x_p)$, и этот класс, как мы сейчас убедимся, является классом теоретико-множественных интерпретаций некоторого рода структуры $\tilde{\Sigma}$, который формально строится из родов структур Σ и Θ и который мы будем называть *синтезированным родом структуры*.

Правила построения синтезированного рода структуры $\tilde{\Sigma}$:

1) конкретизируемые множества $x_1, \dots x_p$ удаляются из текста конкретизируемого рода структуры (их место в синтезированном роде структуры займут термы $\psi_1, \dots \psi_p$);

2) тексты обоих родов структур объединяются в один текст (предполагается, что имена всех конституэнт выбраны таким образом, что ни одно имя конституэнты из Σ не встречается среди имён конституэнт Θ); если в текстах Σ и Θ имеются совпадающие вспомогательные базисные множества, то в тексте $\tilde{\Sigma}$ оставляется одна копия;

3) типовая характеристика T_Σ вида

$$d_\Sigma \in S_\Sigma[x_1, \ldots x_p, x_{p+1}, \ldots x_n]$$

заменяется на типовую характеристику $\tilde{T}$ вида

$$\tilde{d} \in S_\Sigma[S_1[x_{n+1}, \ldots x_{n+m}], \ldots S_p[x_{n+1}, \ldots x_{n+m}], x_{p+1}, \ldots x_n]$$

(напомним, что термы $\psi_1, \ldots \psi_p$ имеют типы $\mathfrak{P}(S_1), \ldots \mathfrak{P}(S_p)$);

4) во всех прочих выражениях все вхождения букв $x_1, \ldots x_p$ заменяются на термы $\psi_1, \ldots \psi_p$: мы будем обозначать через $\tilde{R}$ результат этой замены в аксиоме R_Σ; ясно, что выражения T_Θ и R_Θ, не содержащие $x_1, \ldots x_p$ в качестве параметров, в синтезированную схему перейдут без изменений;

5) добавляется *аксиома синтеза* R_S вида $(\psi_1 \mid x_1) \ldots (\psi_p \mid x_p) T_\Sigma$.

При этом мы говорим, что множества $x_1, \ldots x_p$ рода структуры Σ отождествляются с термами $\psi_1, \ldots \psi_p$ рода структуры Θ. Вновь заметим, что не исключается случай, когда любой из ψ_i совпадает либо с базисным множеством Θ, либо с родовой константой Θ (второе, правда, возможно лишь в случае, когда $d_\Theta \in \mathfrak{P}(\ldots)$, т. е. d_Θ имеет характер множества).

Рассмотрим теперь уже более развёрнуто ещё один пример синтеза: рода структуры функции с родом структуры разбиения множества, где каждый элемент разбиения отождествляется с аргументом функции.

- Род структуры функции Σ:

  x_1, x_2;

  $d_\Sigma \in \mathfrak{P}(x_1 \times x_2)$;

  $R_1 : \forall u \in x_1, \exists v \in x_2((u, v) \in d_\Sigma)$;

  $R_2 : \forall t_1 \in d_\Sigma, \forall t_2 \in d_\Sigma(\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$.

- Род структуры разбиения множества Θ:

  x_3;

  $d_\Theta \in \mathfrak{PP}(x_3)$;

  $R_3 : \forall u \in x_3, \exists g \in d_\Theta (u \in g)$;

  $R_4 : \forall g_1 \in d_\Theta, \forall g_2 \in d_\Theta ((g_1 = g_2) \vee (g_1 \cap g_2 = \varnothing))$.

- Род структуры функции от элементов разбиения $\tilde{\Sigma}$:

  x_2, x_3;

  $\tilde{d} \in \mathfrak{P}(\mathfrak{P}(x_3) \times x_2)$;

  $d_\Theta \in \mathfrak{PP}(x_3)$;

  $\tilde{R}_1 : \forall u \in d_\Theta, \exists v \in x_2 ((u, v) \in \tilde{d})$;

  $\tilde{R}_2 : \forall t_1 \in \tilde{d}, \forall t_2 \in \tilde{d} (\mathrm{pr}_1(t_1) = \mathrm{pr}_1(t_2) \Rightarrow t_1 = t_2)$;

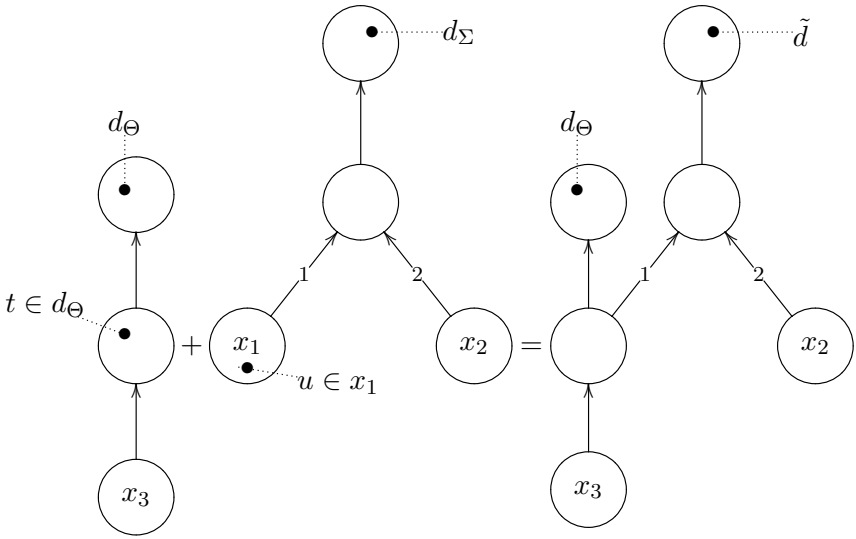
  $R_3 : \forall u \in x_3, \exists g \in d_\Theta (u \in g)$;

  $R_4 : \forall g_1 \in d_\Theta, \forall g_2 \in d_\Theta ((g_1 = g_2) \vee (g_1 \cap g_2 = \varnothing))$;

  $R_S : \tilde{d} \in \mathfrak{P}(d_\Theta \times x_2)$.

Может ли каждый элемент первой большой проекции $\tilde{d}$ быть любым подмножеством x_3? Разумеется, нет: синтезируя Σ и Θ, мы предполагаем, что каждый аргумент функции $\tilde{d}$ является элементом разбиения d_Θ. Но легко видеть, что сам по себе этот факт не есть теорема $\tilde{\Sigma}$, поэтому в синтезированный род структуры добавляется аксиома синтеза R_S. Заметим, что в этом случае вкупе с соотношением типизации для $\tilde{d}_\Sigma$ аксиома синтеза эквивалентна утверждению $\mathrm{Pr}_1(\tilde{d}) \subseteq d_\Theta$.

Произведённые нами действия можно следующим образом проиллюстрировать на М-графах:



Упр. 101. Пусть базисное множество x_1 отождествляется с термом ψ. Проверьте, что при типовых характеристиках 1) $d \in x_1$, 2) $d \in \in x_1 \times x_2$, 3) $d \in \mathfrak{P}(x_1 \times x_2)$, 4) $d \in \mathfrak{PP}(x_1 \times x_1)$, 5) $d \in \mathfrak{PPP}(x_1 \times x_2)$, 6) $d \in \mathfrak{P}((x_1 \times x_2) \times x_1)$, 7) $d \in \mathfrak{P}(x_1) \times x_1 \times x_2$, аксиомы синтеза вместе с новым соотношением типизации будут эквивалентны соответственно 1) $d \in \psi$, 2) $\mathrm{pr}_1(d) \in \psi$, 3) $\mathrm{Pr}_1(d) \subseteq \psi$, 4) $\mathrm{Pr}_1(\bigcup d) \subseteq \psi$ & $\mathrm{Pr}_2(\bigcup d) \subseteq \psi$, 5) $\mathrm{Pr}_1(\bigcup\bigcup d) \subseteq \psi$, 6) $\mathrm{Pr}_1(\mathrm{Pr}_1(d)) \subseteq \psi$ & $\mathrm{Pr}_2(d) \subseteq \psi$, 7) $\mathrm{pr}_1(d) \subseteq \psi$ & & $\mathrm{pr}_2(d) \in \psi$.

Теорема 79. *Пусть $\tilde{\Sigma}$ — синтезированный из Σ и Θ род структуры, $\mathcal{K}_{\tilde{\Sigma}}$ — класс $\tilde{\Sigma}$-объектов. В этом случае выполняется соотношение*

$$\mathcal{K}_{\tilde{\Sigma}} = \{(x_{p+1}, \ldots x_n, d_\Sigma, x_{n+1}, \ldots x_{n+m}, d_\Theta) \mid (\psi_1 \mid x_1) \ldots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma \,\&\, T_\Theta \,\&\, R_\Theta)\}.$$

(Как мы помним, из этого класса можно построить класс пар вида «Σ-объект, Θ-объект», таких, что базисные множества

$x_1, \dots x_p$ рода структуры Σ тождественны термам $\psi_1, \dots \psi_p$ рода структуры Θ.)

$\lhd$В соответствии с определениями операции синтеза и класса теоретико-множественных интерпретаций

$$\mathcal{K}_{\tilde{\Sigma}} = \{(x_{p+1}, \dots x_n, d_\Sigma, x_{n+1}, \dots x_{n+m}, d_\Theta) \mid \tilde{T} \,\&\, T_\Theta \,\&\, R_\Theta \,\&\, (\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma)\}.$$

Здесь знаком $\tilde{T}$ обозначено соотношение типизации, получаемое из T_Σ заменой всех вхождений букв $x_1, \dots x_p$ на $S_1[\dots], \dots S_p[\dots]$. Выражение $(\psi_1 \mid x_1) \dots (\psi_p \mid x_p) T_\Sigma$ соответствует аксиоме синтеза. Иначе говоря, требуется доказать, что

$$(\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma \,\&\, T_\Theta \,\&\, R_\Theta) \sim \sim \tilde{T} \,\&\, T_\Theta \,\&\, R_\Theta \,\&\, (\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma).$$

Формула $T_\Theta \,\&\, R_\Theta$, унаследованная из конкретизирующего рода структуры, не содержит в качестве параметров букв $x_1, \dots x_p$, поэтому $(\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Theta \,\&\, R_\Theta) \sim T_\Theta \,\&\, R_\Theta$, и эту формулу вообще можно исключить из рассмотрения, доказывая лишь, что

$$(\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma) \sim \sim \tilde{T} \,\&\, (\psi_1 \mid x_1) \dots (\psi_p \mid x_p)(T_\Sigma \,\&\, R_\Sigma).$$

Но для этого достаточно доказать, что

$$\vdash (\psi_1 \mid x_1) \dots (\psi_p \mid x_p) T_\Sigma \Rightarrow \tilde{T}.$$

Напомним, что формула T_Σ имеет вид $d_\Sigma \in S_\Sigma[x_1, \dots x_n]$, а $\tilde{T}$ — вид

$$d_\Sigma \in S_\Sigma[S_1[x_{n+1}, \dots x_{n+m}], \dots S_p[x_{n+1}, \dots x_{n+m}], x_{p+1}, \dots x_n],$$

где $\mathfrak{P}S_i[x_{n+1}, \dots x_{n+m}]$ — типизация терма ψ_i, $i = 1, \dots p$. Докажем $(\psi_1 \mid x_1) \dots (\psi_p \mid x_p) T_\Sigma \Rightarrow \tilde{T}$ индукцией по построению схемы S_Σ.

1) Если $S_\Sigma = i$, то возможны два варианта. Случай $i > p$ тривиален: замены нет и T_Σ и $\tilde{T}$ есть одна и та же формула. Если $i \leqslant p$, то $u \in \psi_i \,\&\, \psi_i \in \mathfrak{P}S_i[x_{n+1}, \dots x_{n+m}] \Rightarrow u \in \in S_i[x_{n+1}, \dots x_{n+m}]$.

2) Если $S_\Sigma = \mathfrak{P}(S^*)$, причём по предположению индукции

$$(\psi_1 \mid x_1)\dots(\psi_p \mid x_p)(u \in S^*) \Rightarrow \\ \Rightarrow u \in S^*[S_1[x_{n+1},\dots x_{n+m}],\dots \\ \dots S_p[x_{n+1},\dots x_{n+m}], x_{p+1},\dots x_n],$$

то с учётом

$$u \in \mathfrak{P}(S^*) \sim \forall t(t \in u \Rightarrow t \in S^*)$$

имеем

$$(\psi_1 \mid x_1)\dots(\psi_p \mid x_p)(u \in \mathfrak{P}(S^*)) \Rightarrow \\ \Rightarrow u \in \mathfrak{P}(S^*[S_1[x_{n+1},\dots x_{n+m}],\dots \\ \dots S_p[x_{n+1},\dots x_{n+m}], x_{p+1},\dots x_n]).$$

3) Если $S_\Sigma = S_1^* \times S_2^*$, то

$$u \in S_1^*[\dots]\times S_2^*[\dots] \Rightarrow \exists v \exists w(v \in S_1^*[\dots] \& w \in S_2^*[\dots] \& (v,w) = u),$$

откуда с использованием предположения индукции уже легко получить требуемое.▷

Упр. 102. Проверьте, что если F — теорема Σ, то $(\psi_1 \mid x_1)\dots(\psi_p \mid x_p)F$ — теорема $\tilde{\Sigma}$.

4. Критерий непротиворечивости. Будет ли построенный при помощи синтеза род структуры $\tilde{\Sigma}$ непротиворечивым? Легко видеть, что необходимым условием непротиворечивости синтезированного рода структуры является непротиворечивость синтезируемых родов структур.

Однако даже при синтезе непротиворечивых родов структур может образоваться противоречивый род структуры. Например, характер аксиом Σ может влечь бесконечность множества, соответствующего x_1, в любой теоретико-множественной интерпретации Σ, а терм ψ_1 рода структуры Θ может быть конечным в любой теоретико-множественной интерпретации Θ. Ясно, что если попытаться отождествить x_1 с ψ_1, то для синтезированного рода структуры не найдётся теоретико-множественных интерпретаций, т. е. он будет противоречивым.

Теорема 80. *Пусть Σ — конкретизируемый, Θ — конкретизирующий род структуры, причём множества $x_1,\dots x_p$ рода структуры Σ отождествляются с термами $\psi_1,\dots\psi_p$ рода структуры Θ. Синтезированный род структуры $\tilde{\Sigma}$ непротиворечив тогда и только тогда, когда одновременно выполнены следующие условия:*

1) *существует Σ-объект $\upsilon = (\xi_1,\dots\xi_n,\delta_\Sigma)$;*

2) *существует Θ-объект $\omega = (\xi_{n+1},\dots\xi_{n+m},\delta_\Theta)$;*

3) *каждое из множеств $\xi_1,\dots\xi_p$ равномощно соответствующему множеству*

$$\bar{\psi}_i = (\xi_{n+1} \mid x_{n+1})\dots(\xi_{n+m} \mid x_{n+m})(\delta_\Theta \mid d_\Theta)\psi_i,$$

где $i = 1\dots p$, $p \leqslant n$.

Иначе говоря, род структуры, полученный синтезом, непротиворечив тогда и только тогда, когда у каждого из синтезируемых родов структур имеется по теоретико-множественной интерпретации, причём эти интерпретации таковы, что каждый терм, соответствующий конкретизируемому базисному множеству первого рода структуры, равномощен терму, соответствующему конкретизирующему терму второго рода структуры.

$\lhd$В одну сторону: пусть указанная пара объектов υ, ω существует. По условию должны существовать биекции $\varphi_1 : \xi_1 \leftrightarrow \bar{\psi}_1$, $\varphi_2 : \xi_2 \leftrightarrow \bar{\psi}_2 \dots \varphi_p : \xi_p \leftrightarrow \bar{\psi}_p$ и возможен перенос $\xi_1,\dots\xi_p$ на $\bar{\psi}_1,\dots\bar{\psi}_p$ при типовой характеристике рода структуры Σ с построением терма $\tilde{\delta}$ из терма δ_Σ при помощи канонического распространения. Покажем, что $\tilde{\Sigma}$-объектом является объект, построенный следующим образом:

1) базисные множества, унаследованные из Σ, интерпретируются термами $\xi_{p+1},\dots\xi_n$;

2) базисные множества, унаследованные из Θ, интерпретируются термами $\xi_{n+1}, \ldots \xi_{n+m}$;

3) множество, интерпретирующее родовую константу $\tilde{d}$, получается из δ_Σ переносом $\xi_1, \ldots \xi_p$ на $\bar{\psi}_1, \ldots \bar{\psi}_p$ при типовой характеристике рода структуры Σ;

4) родовая константа, унаследованная из Θ, интерпретируется термом δ_Θ.

Поскольку $\xi_{n+1}, \ldots \xi_{n+m}$ и δ_Θ, составляющие Θ-объект ω, используются без изменений, то переходящие без текстуальных изменений в синтезированный род структуры соотношения $T_\Theta \& R_\Theta$ продолжают выполняться. Аксиома R_Σ выполняется в силу своей биективной переносимости, аксиома синтеза выполняется по построению, типовая характеристика $\tilde{T}$ синтезированного рода структуры выполняется в силу

$$\vdash (\psi_1 \mid x_1) \ldots (\psi_p \mid x_p) T_\Sigma \Rightarrow \tilde{T}$$

(см. доказательство теоремы 79).

В обратную сторону: пусть имеется $\tilde{\Sigma}$-объект ζ. Тогда терм ω, полученный отбрасыванием из ζ множеств, соответствующих базисным множествам и родовой константе, унаследованным из Σ, является Θ-объектом $(\tilde{T} \,\&\, T_\Theta \,\&\, R_\Theta \,\&\, (\psi_1 \mid x_1) \ldots (\psi_p \mid x_p)(T_\Sigma \,\&\, \& \, R_\Sigma) \Rightarrow T_\Theta \,\&\, R_\Theta)$.

Пусть полученный таким образом объект ω равен $(\xi_{n+1}, \ldots \xi_{n+m}, \delta_\Theta)$, а $\bar{\psi}_i = (\xi_{n+1} \mid x_{n+1}) \ldots (\xi_{n+m} \mid x_{n+m})(\delta_\Theta \mid d_\Theta)\psi_i$, $i = 1 \ldots p$. Терм υ, полученный из ζ использованием

1) $\bar{\psi}_1, \ldots \bar{\psi}_p$ для интерпретации первых p базисных множеств;

2) множеств, интерпретирующих унаследованные из Σ, для интерпретации базисных множеств с номерами $p+1 \ldots n$;

3) множества, интерпретирующего синтезированную родовую константу, для интерпретации родовой константы d_Σ,

есть Σ-объект. Первые p множеств этого Σ-объекта совпадают по построению с термами $\bar{\psi}_1, \ldots \bar{\psi}_p$, следовательно, они равномощны этим термам.$\triangleright$

СПИСОК ЛИТЕРАТУРЫ

Математическая логика

1. Ершов Ю. Л. Математическая логика: Учебное пособие / Ершов Ю. Л., Палютин Е. А. — 3-е, стереотип. изд. — СПб.: «Лань», 2004. — 336 с.

2. Лавров И. А. Задачи по теории множеств, математической логике и теории алгорифмов / Лавров И. А., Максимова Л. Л. — 5-е, исправл. изд. — М.: ФИЗМАТЛИТ, 2004. — 256 с.

3. Клини С. К. Математическая логика / Клини С. К. — 2-е, стереотип. изд. — М.: УРСС, 2005. — 480 с.

4. Клини С. К. Введение в метаматематику / Клини С. К.; Под ред. В. А. Успенского. — М.: Изд-во иностранной лит-ры, 1957. — 528 с.

5. Колмогоров А. Н. Математическая логика / Колмогоров А. Н., Драгалин А. Г. — 2-е, стереотип. изд. — М.: УРСС, 2005. — 240 с.

6. Верещагин Н. К. Лекции по математической логике и теории алгоритмов. Ч. 2. Языки и исчисления / Верещагин Н. К., Шень А. Х. — М.: МЦНМО, 2002. — 288 с. —

   `ftp://ftp.mmce.ru/users/shen/logic/firstord/`.

Теория множеств

7. Верещагин Н. К. Лекции по математической логике и теории алгоритмов. Ч. 1. Начала теории множеств / Верещагин Н. К., Шень А. Х. — М.: МЦНМО, 2002. — 128 с. —

   `ftp://ftp.mmce.ru/users/shen/logic/sets/`.

8. Френкель А. А. Основания теории множеств / Френкель А. А., Бар-Хиллел И.; Под ред. А. С. Есенина–Вольпина. — М.: Мир, 1966. — 556 с.

9. Йех Т. Теория множеств и метод форсинга / Йех Т. — М.: Мир, 1973. — 150 с.

10. Казимиров Н. И. Введение в аксиоматическую теорию множеств / Казимиров Н. И. — 2000. — Интернет-издание.

`http://lib.mexmat.ru/books/1394`.

11. Куратовский К. Теория множеств / Куратовский К., Мостовский А. — М.: Мир, 1970. — 416 с.

12. Коэн П. Дж. Теория множеств и континуум-гипотеза / Коэн П. Дж. — М.: Мир, 1969. — 347 с.

13. Хаусдорф Ф. Теория множеств / Хаусдорф Ф.; Под ред. П. С. Александрова, А. Н. Колмогорова. — 3-е, стереотип. изд. — М.: УРСС, 2004. — 204 с.

14. Ященко И. В. Парадоксы теории множеств / Ященко И. В. — М.: МЦНМО, 2002. — 40 с.

Роды структур

15. Бурбаки Н. Теория множеств: Пер. с фр. / Бурбаки Н.; Под ред. В. А. Успенского. — М.: Мир, 1965. — 455 с.

16. Павловский Ю. Н. Проблема декомпозиции в математическом моделировании / Павловский Ю. Н., Смирнова Т. Г. — М.: ФАЗИС, 1998. — 266 с.

17. Павловский Ю. Н. Шкалы родов структур, термы и соотношения, сохраняющиеся при изоморфизмах / Павловский Ю. Н., Смирнова Т. Г. — М.: ВЦ РАН, 2003. — 92 с.

ОГЛАВЛЕНИЕ

выходные данные