Министерство образования и науки Российской Федерации
Государственное образовательное учреждение
“Тобольская государственная социально-педагогическая академия им. Д.И. Менделеева”

Валицкас А.И.

КОНСПЕКТ ЛЕКЦИЙ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

Учебно-методическое пособие для студентов физико-математических специальностей

Рекомендовано

УМО по математике педвузов Волго-Вятского региона в качестве учебного пособия для студентов физико-математических специальностей высших учебных заведений

Тобольск – 2010

УДК 510.6
ББК 22.12 я 73
В 15

Печатается по решению редакционно-издательского совета Тобольской государственной социально-педагогической академии им. Д.И. Менделеева

Валицкас А.И. Конспект лекций по математической логике: Учебно-методическое пособие для студентов физико-математических факультетов педвузов. – Тобольск, 2010. – 186 с.

Учебно-методическое пособие представляет конспект курса лекций по математической логике, читаемого автором в течение ряда лет на математическом факультете в Тобольской государственной социально-педагогической академии им. Д.И. Менделеева.

Пособие предназначено, в первую очередь, для студентов физико-математических специальностей пединститутов. Оно может быть использовано также при чтении курса математической логики для специалистов, связанных с информатикой. Пособие будет полезно всем, кто интересуется математикой и проблемами её обоснования.

Рецензенты:

М.А. Люстиг, кандидат педагогических наук, доцент, зав. кафедрой естественно-научных дисциплин Тобольского филиала ТюмГАСУ, г. Тобольск

В.Г. Ярков, кандидат педагогических наук, доцент, декан математического факультета ТГСПА им. Д.И. Менделеева, г. Тобольск

ISBN 978-5-85944-273-7

С О Д Е Р Ж А Н И Е

П Р Е Д И С Л О В И Е

Хотя настоящее учебно-методическое пособие предназначено, в первую очередь, для студентов физико-математических специальностей пединститутов, оно может быть использовано и при чтении курса математической логики для специалистов, связанных с информатикой. Автор надеется, что предлагаемое пособие заинтересует всех, кто не равно дышит к математике, проблемам её обоснования, или просто желает расширить свой кругозор. С этой целью некоторые разделы курса изложены более широко, чем этого требует программа, а материал каждого параграфа подкреплён примерами и упражнениями для самостоятельного решения, которые помогут вдумчивому читателю научиться решать стандартные задачи по математической логике. Качественное изучение математической логики даёт выпускнику педагогического вуза возможность обучения школьников методам строгих математических рассуждений, что особенно важно в условиях отмечающегося в последнее время неуклонного снижения уровней логического мышления и доказательности в математических рассуждениях школьников.

Первые две главы “Алгебра высказываний” и “Алгебра предикатов” содержат традиционный материал по неформальному изложению исчислений высказываний и предикатов. Следует отметить, что приводимые в главе I § 8 приложения этих теорий представляют интерес для всех, кто имеет отношение к программированию.

Большое внимание уделено в третьей главе различным вопросам построения формальных аксиоматических теорий. Достаточно подробно (с полными доказательствами) рассматривается теория исчисления высказываний. Теории предикатов и формальной арифметики обсуждаются в общих чертах. В приложении неформально излагается формальная теория множеств (§ 2) и обсуждаются некоторые проблемы аксиоматизации теории множеств (§ 3). Первый параграф приложения содержит азы наивной теории множеств для тех, кто столкнётся с трудностями теоретико-множественного характера в главе II.

Автор выражает благодарность всему коллективу кафедры алгебры, геометрии и ТиМОМ ТГСПА им. Д.И. Менделеева за поддержку и заинтересованность в этой работе и благодарен рецензентам, обратившим внимание на некоторые неточности и опечатки. Особая благодарность – д.ф.-м.н., профессору Е.М. Вечтомову, без участия которого этот труд не был бы завершён. Автор будет признателен всем, кто пожелает высказать любые конструктивные замечания и пожелания по тексту данного пособия.

ГЛАВА I. АЛГЕБРА ВЫСКАЗЫВАНИЙ

§ 1. Понятие высказывания

Математика, как это не кажется странным, – наука устная: математики, рассуждая, оперируют высказываниями, именно общение является питательной средой математического творчества, в которой создаётся математический фольклор, передаваемый изустно. На интуитивном уровне *высказывание* – это повествовательное предложение, которому можно приписать одно из значений *истина* или *ложь*. Нужно отчётливо понимать, что данное описание понятия "высказывание" не является определением, т.к. строго не объяснено, что значит "можно приписать значение" предложению, и не определены понятия *истина* и *ложь*. Поэтому следует задуматься: что же такое определение ?

Определение – это лишь введение синонима, заменяющего некоторое описание свойств объекта. Например, определение *"прямоугольный треугольник* – это треугольник, у которого один из углов прямой" вводит синоним *"прямоугольный треугольник"* для словосочетания "треугольник, у которого один из углов прямой". В свою очередь, чтобы объяснить использованные в определении прямоугольного треугольника понятия, необходимо дать определения *треугольника*, *величины угла треугольника* и *равенства* величин. Для этого придётся привлечь понятия *геометрической фигуры*, *числа* и их *равенства*.

Таким образом, давая очередное определение, мы вынуждены опираться на неопределённые до сих пор понятия и их отношения. Поскольку человек не может оперировать сразу бесконечным количеством понятий, при построении любой содержательной теории невозможно дать определение всему: рано или поздно приходится опираться на *первопонятия*, т.е. неопределяемые понятия и *первоотношения*, т.е. неопределяемые отношения между неопределяемыми понятиями. Например, в геометрии первопонятиями являются *"точка"*, *"прямая"*, *"плоскость"*, а первоотношениями *"точка лежит на прямой"*, *"прямая лежит в плоскости"*, *"точка A лежит на прямой между точек B и C"* и другие, полный список которых можно составить, открыв школьный учебник геометрии на последних страницах и проанализировав какую-либо конкретную аксиоматику евклидовой геометрии. Первопонятия и первоотношения есть и в любой другой науке: в физике таковыми являются *"сила"*, *"энергия"*, *"время"*, *"материальная точка"*, *"действие силы на материальную точку"* и другие.

Высказывание – это одно из неопределяемых понятий математики, смысл которого был проиллюстрирован предыдущими нестрогими рассуждениями. Ещё более сложно объяснить смысл понятий *истина* и *ложь*, которые в математике также являются неопределяемыми. По этой причине не существует строгого математического алгоритма приписывания произвольным предложениям значений *истина* и *ложь*. На интуитивном уровне этот "алгоритм" можно описать так:

(1): уяснить смысл высказывания,

(2): убедиться, что объекты и их отношения, о которых идёт речь, можно сравнить с действительностью,

(3): если установленные в высказывании отношения между объектами согласуются с действительностью, то высказывание считается *"истинным"*, в противном случае – *"ложным"*.

Здесь под объектами, их отношениями и действительностью следует понимать не только объекты и их отношения в грубом физическом мире, но и всю совокупность идеальных объектов и их отношений, с которыми имеет дело та или иная теория, в рамках которой исследуется истинность или ложность того или иного утверждения. В противном случае, нет возможности оценить истинность, например, такого математического высказывания: *"5 – простое число"*. Конечно, сравнить с действительностью какое-либо утверждение не просто, а часто и невозможно, т.к. эта действительность должна включать не только известные факты рассматриваемой науки, но и ещё не известные в данный момент факты, объекты и отношения. Поэтому, истинность большинства научных утверждений лишь относительна, приближённа.

Если пользоваться таким алгоритмом приписывания истинностных значений, то становится понятно, что не всякое повествовательное предложение является высказыванием.

Примеры: 1. Любое определение – не высказывание, т.к. весь его смысл сводится к введению синонима для какого-либо перечня свойств объекта.

2. **Утверждение в этой рамке ложно.** Это – не высказывание. Действительно, если это утверждение истинно, то справедливо то, что оно говорит о себе: оно ложно, – противоречие. Если же оно ложно, то неверно то, что оно говорит о себе: оно говорит, что ложно, а значит, является истинным, – опять противоречие. Таким образом, в любом случае попытка приписать значение истинности этому утверждению ведёт к противоречию.

В чём причина невозможности приписать утверждению в рамке значение истинности ? Она состоит в том, что не срабатывает схема **(1) – (3)** приписывания истинностного значения. Это утверждение оперирует единственной реальностью – своей ложностью, а значит, для проверки истинности этого утверждения нужно проверить его ложность, в свою очередь, для этого, необходимо опять проверить ложность рассматриваемого утверждения, и.т.д. – получается замкнутый круг, из которого нет выхода. Вот почему **рассматриваемое утверждение не является высказыванием**.

3. **Утверждение в этой рамке истинно.** Если это утверждение истинно, то никакого противоречия не возникает: оно и утверждает свою истинность. Если это утверждение ложно, то неверно то, что оно говорит о своей истинности, и значит, оно ложно – противоречия нет и в этом случае. Так каково же истинностное значение этого предложения ?

На самом деле, в этом примере, как и в предыдущем, нет возможности разумным образом реализовать схему **(1) – (3)** приписывания истинностного значения. Рассматриваемое утверждение оперирует единственной реальностью – своей истинностью, а значит, для проверки истинности этого утверждения нужно проверить его истинность. В свою очередь, для этого, необходимо опять проверить истинность рассматриваемого утверждения, и.т.д. – получается замкнутый круг, из которого нет выхода. Рассматриваемое утверждение не является высказыванием[1].

Упражнение: Найдите ошибку в "доказательстве" следующей "теоремы". Зелюки, о которых в ней идёт речь – это персонажи книги Л. Кэрролла "Алиса в стране чудес":

Варкалось… Хливкие шорьки
Пырялись по наве,
И глюкотали зелюки,
Как мумзики в мове…

(Л. Кэрролл "Алиса в стране чудес",
перевод Н. Демуровой)

"Теорема". *Зелюки существуют.*

"Доказательство". Рассмотрим следующие три утверждения:

(a) зелюки существуют,

(b) *1 = 1*,

[1] Любознательный читатель может обратиться к замечательной книге: Смаллиан Р.М. Как же называется эта книга ? – М.: Мир, 1981.

(c) среди утверждений (a), (b), (c) ровно два ложных.

Для утверждения (c) возможны два случая:

1) утверждение (c) истинно. Это значит, что среди (a), (b), (c) ровно два ложных. Но (c) не ложно, и поэтому ложны первые два утверждения (a), (b), что невозможно, т.к. утверждение (b) заведомо истинно. Значит рассматриваемый случай **1)** не реализуется.

2) утверждение (c) ложно. Тогда среди высказываний (a), (b), (c) число ложных не равно двум. Если бы (a) было ложно, то (ввиду заведомой истинности (b)) высказывание (c) оказалось бы истинным, вопреки рассматриваемому случаю. Итак, (a) истинно, что и доказывает существование зелюков. "Теорема" доказана.

Этот же "метод" годится для "доказательства" любого утверждения.

§ 2. Язык исчисления высказываний

В любом естественном языке есть возможность строить из простых высказываний более сложные.

Примеры: 1. "Сейчас температура воздуха на улице от *–25* до *–30* градусов Цельсия", "*5* – простое число", "Сегодня скорость ветра в г. Тобольске больше *5 м / сек.*" – всё это элементарные высказывания.

2. "Сейчас температура воздуха на улице от *–25* до *–30* градусов Цельсия" и "*5* – простое число"; Если "сегодня скорость ветра в г. Тобольске больше *5 м / сек.*", то "*5* – простое число"; Неверно, что "*5* – простое число", "*5* – простое число" тогда и только тогда, когда "Сейчас температура воздуха на улице от *–25* до *–30* градусов Цельсия"; "Сейчас температура воздуха на улице от *–25* до *–30* градусов Цельсия" или "Сегодня скорость ветра в г. Тобольске больше *5 м / сек.*" – всё это сложные высказывания, полученные из предыдущих с помощью специальных языковых конструкций.

Говоря формально, некоторые из использованных в этих примерах утверждений высказываниями не являются: их невозможно соотнести с действительностью, поскольку они не содержат полной информации о констатируемом факте. Например, не ясно ни где именно измеряется температура воздуха или скорость ветра, ни когда именно это происходило. Такое положение дел присуще большинству из используемых в быту "высказываний". Если мы, общаясь, понимаем

друг друга, то благодаря тому, что воспринимаем "высказывания" собеседника по умолчанию с местом действия "здесь" и временем действия – "сейчас".

Не дело математики и, в частности, логики выяснять истинность или ложность высказываний, оперирующих понятиями из других областей знания или жизненного опыта. Логика даёт средства для построения из элементарных высказываний, ответственность за истинность или ложность которых лежит на пользователе каждой науки, более сложных высказываний, а также – для построения истинностных значений этих сложных высказываний в зависимости от истинностных значений элементарных высказываний, из которых они построены. Для этого создан специальный язык исчисления высказываний, к изучению которого, мы и переходим.

Для обозначения элементарных высказываний будем использовать, как правило, малые буквы доступных алфавитов, с индексами или без них: $a, b, c, d, \ldots \ldots, б_{345}, \ldots,$ которые будем называть *пропозициональными переменными* или просто *переменными*.

Для построения более сложных осмысленных выражений используют следующие специальные знаки, называемые *логическими связками*:

Знак	Название	Языковой аналог	Использование
$\wedge$	***конъюнкция***	*A и B*	$A \wedge B$
$\vee$	***дизъюнкция***	*A или B*	$A \vee B$
$\rightarrow$	***импликация***	*если A, то B*	$A \rightarrow B$
$\leftrightarrow$	***эквивалентность***	*A тогда и только тогда, когда B*	$A \leftrightarrow B$
$\overline{\bullet}$	***отрицание***	*неверно, что A*	$\overline{A}$

Наконец, как и во всяком языке, в языке исчисления высказываний будут использоваться *служебные символы – скобки*: левая скобка *(* и правая скобка *)*.

Таким образом, *алфавит языка исчисления высказываний* состоит из трёх описанных выше групп символов: пропозициональных переменных, логических связок и служебных символов.

Кроме того, язык исчисления высказываний, как и любой естественный язык, предполагает наличие правил конструирования фраз – осмысленных предложений языка, состоящих из слов. Слова состоят из букв, но не всякая комбинация букв является словом, и не всякий набор слов образует фразу. В языке исчисления высказываний осмысленными фразами служат *формулы*.

Понятие *формулы языка исчисления высказываний* строится от простого к сложному с помощью следующих трёх правил:

(Ф1): *любая пропозициональная переменная является формулой.*

(Ф2): *если* A *и* B *– формулы, то* $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $\overline{A}$, $\overline{B}$ *– тоже формулы.*

(Ф3): *других формул нет.*

Процесс построения формул похож на игру в детский конструктор, в котором дан набор деталей (правило ***(Ф1)*** о пропозициональных переменных), соединительные узлы (правило ***(Ф2)*** о логических связках), а в остальном предоставлена полная свобода конструирования **предоставленными средствами** (ограничительное правило ***(Ф3)***).

Примеры формул и не формул

Формулы	**Использованные правила**	**Не формулы**	**Нарушенные правила**
$\overline{\overline{a}}$	a ***(Ф1)*** $\overline{a}$ ***(Ф2)*** $\overline{\overline{a}}$ ***(Ф2)***	$\overline{(a)}$	*(a) – не формула* ***(Ф2)***
$(a \vee b)$	a ***(Ф1)*** b ***(Ф1)*** $(a \vee b)$ ***(Ф2)***	ab	***(Ф2)***
$(\overline{(a \wedge b)} \to c)$	a ***(Ф1)*** b ***(Ф1)*** c ***(Ф1)*** $(a \wedge b)$ ***(Ф2)*** $\overline{(a \wedge b)}$ ***(Ф2)*** $(\overline{(a \wedge b)} \to c)$ ***(Ф2)***	$a \vee b \wedge c$	*нет скобок* ***(Ф2)***
$\overline{(c \leftrightarrow \overline{a})}$	a ***(Ф1)*** c ***(Ф1)*** $\overline{a}$ ***(Ф2)*** $(c \leftrightarrow \overline{a})$ ***(Ф2)*** $\overline{(c \leftrightarrow \overline{a})}$ ***(Ф2)***	$\overline{c \leftrightarrow \overline{a}}$	$c \leftrightarrow \overline{a}$ *– не формула* ***(Ф2)***

Итак, введённое понятие формулы исчисления высказываний позволяет из элементарных высказываний, которые можно подставлять вместо пропозициональных переменных, строить более сложные высказывания с помощью естественных языковых конструкций, используя логические связки и разделительные скобки.

Несмотря на то, что отсутствие скобок является ошибкой при написании формулы, самые внешние скобки в формуле можно опустить, не нарушая её

смысла. Поэтому **в дальнейшем для упрощения записи условимся в формулах допускать отсутствие самых внешних скобок** (их всегда можно поставить, восстановив *status quo*). Таким образом, по-прежнему ошибочна запись $a \vee b \wedge c$, но допустимо выражение $c \leftrightarrow \overline{c}$, т.к. оно станет формулой после добавления внешних скобок: $(c \leftrightarrow \overline{c})$.

Иногда для экономии места применяют следующее ***правило восстановления скобок по умолчанию***:

(C1): *скобки в формуле расставляются в несколько проходов, рассматривая входящие в неё символы слева направо.*

(C2): *на каждом проходе обрабатываются логические связки одного из типов в соответствии с их приоритетами:* $\overline{\bullet}$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ *(это значит, что двигаясь слева направо, вначале находят первое ещё не обработанное отрицание и обрабатывают его в соответствии с правилом* ***(C3)****, при отсутствии таковых – первую ещё не обработанную конъюнкцию, затем – дизъюнкцию, далее – импликацию и, наконец, эквивалентность, и.т.д).*

(C3): *обработка отрицания состоит в расстановке всех скобок в формуле, стоящей под этим отрицанием (в соответствии с правилами* ***(C1)–(C4)****).*

(C4): *обработка остальных логических связок* $\omega \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ *состоит в нахождении их минимальных формул-аргументов* Φ_1, Φ_2 *и расстановке внешних скобок для получения выражения* $(\Phi_1\ \omega\ \Phi_2)$.

Проиллюстрируем это правило на нескольких примерах:

Примеры: 1. Для выражения $a \vee b \wedge c$ после первого прохода получится выражение $a \vee (b \wedge c)$ – конъюнкция обрабатывается раньше дизъюнкции, а при втором проходе – формула $(a \vee (b \wedge c))$.

2. Для выражения $a \rightarrow b \wedge c \leftrightarrow c \wedge d \rightarrow a$ результаты проходов таковы:

а. $a \rightarrow (b \wedge c) \leftrightarrow (c \wedge d) \rightarrow a$ *(обработано две конъюнкции),*

б. $(a \rightarrow (b \wedge c)) \leftrightarrow ((c \wedge d) \rightarrow a)$ *(обработано две импликации),*

в. $((a \rightarrow (b \wedge c)) \leftrightarrow ((c \wedge d) \rightarrow a))$ *(обработана эквивалентность).*

3. Для выражения $a \rightarrow b \wedge (c \leftrightarrow c) \wedge d \rightarrow a$ результаты будут следующими:

а. $a \rightarrow ((b \wedge (c \leftrightarrow c)) \wedge d) \rightarrow a$ *(обработано две конъюнкции),*

б. $((a \rightarrow ((b \wedge (c \leftrightarrow c)) \wedge d)) \rightarrow a)$ *(обработано две импликации).*

4. Для выражения $\overline{a \wedge b \rightarrow a \vee c \rightarrow \overline{a \leftrightarrow c \vee b}} \vee a \wedge b \vee \overline{b \rightarrow \overline{b \vee c \leftrightarrow a}}$ результаты проходов таковы:

а. $\overline{((a \wedge b) \rightarrow (a \vee c)) \rightarrow \overline{(a \leftrightarrow (c \vee b))}} \vee a \wedge b \vee \overline{(b \rightarrow \overline{((b \vee c) \leftrightarrow a)})}$

(обработано два отрицания),

б. $\overline{((a\wedge b)\to(a\vee c))\to\overline{(a\leftrightarrow(c\vee b))}}\ \vee(a\wedge b)\vee\overline{(b\to\overline{((b\vee c)\leftrightarrow a)})}$

(обработана конъюнкция),

в. $\overline{(((a\wedge b)\to(a\vee c))\to\overline{(a\leftrightarrow(c\vee b))})}\ \vee(a\wedge b))\vee\overline{(b\to\overline{((b\vee c)\leftrightarrow a)})})$

(обработано две дизъюнкции).

Итак, в дальнейшем, если некоторое выражение в алфавите языка исчисления высказываний не является формулой по причине отсутствия некоторых скобок, то это выражение можно пытаться превратить в формулу, расставляя в нём недостающие скобки с помощью описанного выше правила.

§ 3. Истинностные значения формул

Истинность или ложность элементарных высказываний оставляется на совести той области знания, к которой они относятся. Логика позволяет по заданным истинностным значениям элементарных высказываний вычислять истинностные значения построенных из них сложных высказываний.

Прежде, чем переходить к формальным рассуждениям, введём следующие соглашения: вместо значения *истина* будем писать *1*, а вместо значения *ложь* – *0*. *Интерпретацией формулы* $A(x_1, \dots, x_n)$ назовём любой набор $\varepsilon = (\varepsilon_1; \dots; \varepsilon_n)$ значений переменных $x_1 = \varepsilon_1, \dots, x_n = \varepsilon_n$ $(\varepsilon_i \in \{0, 1\},\ 1 \le i \le n)$.

Теперь любой формуле исчисления высказываний $A(x_1, \dots, x_n)$ от пропозициональных переменных $x_1, \dots, x_n$ можно присвоить *истинностное значение* $A(\varepsilon) = A(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}$ при данной интерпретации $\varepsilon = (\varepsilon_1; \dots; \varepsilon_n)$ по следующим правилам:

(И1): *если* $A(x_1, \dots, x_n)$ *– одна из пропозициональных переменных* $x_1, \dots, x_n$, *то её истинностное значение уже определено: в случае* $A(x_1, \dots, x_n) = x_i$ *полагаем* $A(\varepsilon) = \varepsilon_i$;

(И2): *если* $A(x_1, \dots, x_n) = (B(x_1, \dots, x_n)\ \omega\ C(x_1, \dots, x_n))$ *или* $A(x_1, \dots, x_n) = \overline{B(x_1, \dots, x_n)}$, *где* ω *– одна из логических связок* $\wedge$, $\vee$, $\to$, $\leftrightarrow$ *(т.е. формула* $A(x_1, \dots, x_n)$ *получена из более простых формул* $B(x_1, \dots, x_n)$ *и* $C(x_1, \dots, x_n)$ *с помощью одной из конструкций правила образования формул* ***(Ф2)****), а значения* $B(\varepsilon) = B(\varepsilon_1, \dots, \varepsilon_n)$ *и* $C(\varepsilon) = C(\varepsilon_1, \dots, \varepsilon_n)$ *уже вычислены, то истинностное значение* $A(\varepsilon) = A(\varepsilon_1, \dots, \varepsilon_n)$ *приписывается с помощью следующих аксиом логических связок:*

$B(\varepsilon)$	$C(\varepsilon)$	$\overline{B}\,(\varepsilon)$	$(B(\varepsilon) \wedge C(\varepsilon))$	$(B(\varepsilon) \vee C(\varepsilon))$	$(B(\varepsilon) \to C(\varepsilon))$	$(B(\varepsilon) \leftrightarrow C(\varepsilon))$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Следует подчеркнуть, что ***законы вычисления этих логических связок являются именно аксиомами – они принимаются на веру***. Часть из них согласуется со здравым смыслом и интуитивными описаниями значения логических связок. Некоторые значения менее очевидны, и осознание необходимости их использования нуждается в дополнительных аргументах, которые рождаются только в результате работы мысли.

Наиболее трудна для понимания аксиома вычисления импликации, в частности, нуждается в дополнительных аргументах тот факт, что при ложной посылке $B(\varepsilon)$ значение импликации всегда истинно. По смыслу логическая связка импликация $\to$ означает следование, выводимость. Таким образом, нужно понять, почему из ложного утверждения выводится любое другое. В связи с этим невозможно не упомянуть случай, произошедший с Бертраном Расселом – известным специалистом по математической логике *XX* в. Он читал лекцию для философов, когда один из них попросил объяснить, почему из ложного утверждения можно вывести всё, что угодно ? Тогда Рассел для примера доказал, что из утверждения $2\times2 = 5$ следует, что он – Папа Римский. Вот это остроумное доказательство:

$$2\times2 = 5,\ 2+2 = 2+3,\ 2 = 3,\ 1+1 = 2+1,\ 1 = 2,$$

Рассел и Папа Римский – их двое, но $2 = 1$, *так что они – одно лицо, ч.т.д.*

Отметим ещё, что значение импликации огромно: любое научное утверждение формулируется в *импликативном* виде, т.е. в виде импликации $A \to B$. Например, теорема Пифагора *"сумма квадратов катетов равна квадрату гипотенузы"* на самом деле означает следующее: если ABC – треугольник с прямым углом C, то $AB^2 = AC^2 + BC^2$. Точно так же формулируются и утверждения других наук: в них всегда должна присутствовать *посылка* A и *заключение* B, а само утверждение означает истинность импликации $A \to B$. Если посылка A истинна, то истинность импликации означает истинность заключения B. Если же посылка ложна, то импликация всё равно истинна. Поэтому, если вдруг выяснилось, что B ложно, это ещё не значит, что нарушен закон той или иной науки, просто, возможно, посылка A стала ложной, а импликация всё равно истинна.

Как с помощью сформулированных аксиом вычислить значение любой формулы при заданных значениях её пропозициональных переменных ? Значение формулы вычисляется последовательно, начиная со значений пропозициональных переменных в соответствии с построением самой формулы по правилу ***(Ф2)*** с применением на каждом шаге описанных выше аксиом.

Примеры: 1. Вычислить значение формулы $(\overline{a} \vee b)$ при $a = 1,\ b = 0.$

Формула $(\overline{a} \vee b)$ построена из формул $\overline{a}$ и b путём применением конструкции $(A \vee B)$ правила ***(Ф2).*** Поэтому вначале нужно вычислить значения формул $\overline{a}$ и $b,$ а затем применить аксиому вычисления дизъюнкции. Значение $b = 0$ дано, а значение формулы $\overline{a}$ вычисляется из заданного значения формулы a по аксиоме значения отрицания: $\overline{a} = \overline{1} = 0.$ Таким образом, по аксиоме значения дизъюнкции получаем в итоге $(\overline{a} \vee b) = (0 \vee 0) = 0.$

Следует отметить, что при других наборах значений переменных значение этой же формулы может быть другим. Например, если $a = 0 = b,$ то $\overline{a} = 1$ и $(\overline{a} \vee b) = (1 \vee 0) = 1.$

2. Вычислить значение формулы $(\overline{(a \wedge b)} \to c)$ при $a = 1,\ b = 1, c = 0$.

Опишем процесс построения формулы по правилу ***(Ф2)***, одновременно вычисляя на каждом шаге истинностные значения получаемых формул при заданных значениях пропозициональных переменных: $a = 1,\ b = 1,\ c = 0,\ (a \wedge b) = 1,$ $\overline{(a \wedge b)} = \overline{1} = 0,\ (\overline{(a \wedge b)} \to c) = (0 \to 0) = 1.$ Таким образом, искомое значение равно $1.$

Для $a = 0, b = 0, c = 0$ получим $(a \wedge b) = (0 \wedge 0) = 0,\ \overline{(a \wedge b)} = \overline{0} = 1,$ $(\overline{(a \wedge b)} \to c) = (1 \to 0) = 0.$

Предыдущие примеры показывают, что значение формулы зависит от конкретного набора её пропозициональных переменных, т.е. от конкретной интерпретации формулы: при разных интерпретациях значения формулы могут быть различными. Поэтому ***говорить об истинности или ложности формулы, не указывая интерпретации, бессмысленно***.

На практике обычно заранее неизвестно, какие именно значения принимают пропозициональные переменные. Поэтому для нахождения всех истинностных значений формулы $A(x_1, \dots, x_n)$ строят её *таблицу истинности*, т.е. таблицу указанного слева

x_1	…	x_n	…	$A(x_1, \dots, x_n)$
…	…	…	…	…
ε_1	…	ε_n	…	$A(\varepsilon_1, \dots, \varepsilon_n)$
…	…	…	…	…

вида, которая имеет (как будет показано ниже) 2^n строк, каждая из которых в первых n столбцах содержит конкретные значения $\varepsilon_1, \dots, \varepsilon_n$ пропозициональных переменных $x_1, \dots, x_n$, в последующих столбцах – вычисленные промежуточные значения более простых формул, из которых строится рассматриваемая формула, а в последнем столбце – значение формулы $A(x_1, \dots, x_n)$ при интерпретации $\varepsilon = (\varepsilon_1; \dots; \varepsilon_n)$. При этом в первых n столбцах таблицы истинности должны быть ровно по одному разу перечислены все возможные наборы значений пропозициональных переменных $x_1, \dots, x_n$.

Примеры: 1. Строим таблицы истинности формул $\overline{a} \vee b$ и $\overline{a \to b} \wedge \overline{b \to a}$.

a	b	$\overline{a}$	$\overline{a} \vee b$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

a	b	$a \to b$	$\overline{a \to b}$	$b \to a$	$\overline{b \to a}$	$\overline{a \to b} \wedge \overline{b \to a}$
0	0	1	0	1	0	0
0	1	1	0	0	1	0
1	0	0	1	1	0	0
1	1	1	0	1	0	0

a	b	c	1	2	3	4	5	6
0	0	0	0	0	0	0	0	1
0	0	1	0	1	1	1	1	1
0	1	0	0	0	0	1	0	1
0	1	1	0	1	1	1	1	1
1	0	0	0	0	1	0	0	1
1	0	1	0	1	1	1	1	1
1	1	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1

2. Построим таблицу истинности для формулы $((a \wedge b) \vee c) \leftrightarrow ((a \vee c) \wedge (b \vee c))$.

В ней цифрами обозначены формулы: $\mathbf{1} = (a \wedge b)$, $\mathbf{2} = (\mathbf{1} \vee c)$, $\mathbf{3} = (a \vee c)$, $\mathbf{4} = (b \vee c)$, $\mathbf{5} = (\mathbf{3} \wedge \mathbf{4})$, $\mathbf{6} = \mathbf{2} \leftrightarrow \mathbf{5}$. Такие сокращения удобны для построения таблиц истинности громоздких формул. Использованные в обозначениях числа определяют и порядок вычислений.

Для того чтобы успешно строить таблицы истинности формул, нужно иметь алгоритм перечисления всех возможных наборов значений n её пропозициональных переменных $x_1, \dots, x_n$. Можно воспользоваться, например, двоичной системой счисления: каждая интерпретация $\varepsilon = (\varepsilon_1; \dots; \varepsilon_n)$ отождествляется с двоичным числом $\overline{(\varepsilon_1 \dots \varepsilon_n)}_2$ из n двоичных цифр $\varepsilon_1, \dots, \varepsilon_n \in \{0, 1\}$, которое в десятичном виде выглядит как $\varepsilon_1 \cdot 2^{n-1} + \dots + \varepsilon_n \cdot 2^0$. Наименьшее число $0 = 0 \dots 0_2 = 0 \cdot 2^{n-1} + \dots + 0 \cdot 2^0$ соответствует интерпретации $\varepsilon = (0; \dots; 0)$, а наибольшее $1 \dots 1_2 = 1 \cdot 2^{n-1} + \dots + 1 \cdot 2^0 = 2^{n-1} + 2^{n-2} + \dots + 2 + 1 = \frac{2^n - 1}{2 - 1} = 2^n - 1$ (по формуле суммирования геометрической прогрессии) – интерпретации $\varepsilon = (1; \dots; 1)$. Поэтому для перечисления всех интерпретаций достаточно использовать двоичные

0	2	10	2	10	2	10	2
0	00000	8	01000	16	10000	24	11000
1	00001	9	01001	17	10001	25	11001
2	00010	10	01010	18	10010	26	11010
3	00011	11	01011	19	10011	27	11011
4	00100	12	01100	20	10100	28	11100
5	00101	13	01101	21	10101	29	11101
6	00110	14	01110	22	10110	30	11110
7	00111	15	01111	23	10111	31	11111

коды чисел от 0 до $2^n - 1$, которые приведены в таблице ($n = 5$).

Здесь использована пятиразрядная двоичная запись чисел, но незначащие нули по мере необходимости можно отбросить так же, как это сделано в приводимых ниже примерах перечисления интерпретаций для $n = 1, 2, 3, 4$.

Примеры: $n = 1$:

x_1
0
1

, $n = 2$:

x_1	x_2
0	0
0	1
1	0
1	1

, $n = 3$:

x_1	x_2	x_3
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

, $n = 4$:

x_1	x_2	x_3	x_4
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

Теорема (о правиле перечисления интерпретаций). *В таблице, построенной путём выписывания n-значных двоичных кодов всех чисел от 0 до $2^n - 1$, перечисляются ровно по одному разу всевозможные наборы значений n пропозициональных переменных.*

Доказательство. Как было отмечено, каждой интерпретации $\varepsilon = (\varepsilon_1 ; \dots ; \varepsilon_n)$ соответствует двоичное число $\overline{(\varepsilon_1 \dots \varepsilon_n)}_2$ из n двоичных цифр $\varepsilon_1 , \dots , \varepsilon_n$, которое находится в диапазоне от 0 до $2^n - 1$. При этом разным интерпретациям будут отвечать и разные числа: если $\varepsilon = (\varepsilon_1 ; \dots ; \varepsilon_n) \neq (\delta_1 ; \dots ; \delta_n) = \delta$, то $\overline{(\varepsilon_1 \dots \varepsilon_n)}_2 \neq \overline{(\delta_1 \dots \delta_n)}_2$. Кроме того, в результате такого сопоставления будут перечислены без пропусков <u>все</u> двоичные числа от 0 до $2^n - 1$: число $\overline{(\varepsilon_1 \dots \varepsilon_n)}_2$ появится при рассмотрении интерпретации $\varepsilon = (\varepsilon_1 ; \dots ; \varepsilon_n)$.

Теорема доказана.

Следствие (о количестве наборов из нулей и единиц длины n). *Количество всевозможных наборов длины n из нулей и единиц равно 2^n. Столько же и строк в любой таблице истинности формулы от n переменных.*

Доказательство очевидно, т.к. количество всевозможных наборов длины n из нулей и единиц равно количеству всевозможных интерпретаций для n пропозициональных переменных, которое (ввиду доказанной теоремы) равно количеству чисел от 0 до $2^n - 1$, т.е. 2^n. Следствие доказано.

Следствие (о количестве подмножеств n-элементного множества). *Любое n-элементное множество содержит 2^n подмножеств.*

Доказательство. Пусть дано множество $A = \{a_1 , \dots , a_n \}$. Каждому его подмножеству $X \subseteq A$ сопоставим набор $(\varepsilon_1 ; \dots ; \varepsilon_n)$ из нулей и единиц длины n, полностью определяющий это подмножество. Для этого положим $\varepsilon_i = 1$, если $a_i \in X$, и $\varepsilon_i = 0$, если $a_i \notin X$ $(1 \le i \le n)$. Кстати, именно такой способ интерпретации множеств реализуется в некоторых языках программирования.

Примеры: Для множества $A = \{a_1 , a_2 , a_3 \}$ подмножеству $X = \{a_1 , a_3\}$ будет соответствовать набор $(1; 0; 1)$, а подмножеству $X = \{a_2 \}$ – набор $(0; 1; 0)$. Пустому подмножеству (не содержащему элементов) будет сопоставлен набор $(0; 0; 0)$, а всему множеству A – набор $(1; 1; 1)$.

Легко понять, что по любому набору $(\varepsilon_1 ; \dots ; \varepsilon_n)$ из нулей и единиц длины n однозначно восстанавливается соответствующее ему подмножество: именно в множестве X нужно собрать все те элементы a_i, для которых $\varepsilon_i = 1$ $(1 \le i \le n)$. Поэтому подмножеств в n-элементном множестве будет столько, сколько существует наборов из нулей и единиц длины n, т.е. 2^n. Следствие доказано.

Пример. Перечислим все подмножества 4-элементного множества.

Будем перечислять подмножества, выписывая соответствующие им наборы нулей и единиц, построенные по двоичным числам из диапазона от 0 до $2^4 = 16$:

№	набор	подмножество	№	набор	подмножество
0	$(0; 0; 0; 0)$	$\varnothing$	**8**	$(1; 0; 0; 0)$	$\{a_1 \}$
1	$(0; 0; 0; 1)$	$\{a_4 \}$	**9**	$(1; 0; 0; 1)$	$\{a_1 , a_4 \}$
2	$(0; 0; 1; 0)$	$\{a_3 \}$	**10**	$(1; 0; 1; 0)$	$\{a_1 , a_3 \}$
3	$(0; 0; 1; 1)$	$\{a_3 , a_4 \}$	**11**	$(1; 0; 1; 1)$	$\{a_1 , a_3 , a_4 \}$
4	$(0; 1; 0; 0)$	$\{a_2 \}$	**12**	$(1; 1; 0; 0)$	$\{a_1 , a_2 \}$
5	$(0; 1; 0; 1)$	$\{a_2 , a_4 \}$	**13**	$(1; 1; 0; 1)$	$\{a_1 , a_2 , a_4 \}$
6	$(0; 1; 1; 0)$	$\{a_2 , a_3 \}$	**14**	$(1; 1; 1; 0)$	$\{a_1 , a_2 , a_3 \}$
7	$(0; 1; 1; 1)$	$\{a_2 , a_3 , a_4 \}$	**15**	$(1; 1; 1; 1)$	$\{a_1 , a_2 , a_3 , a_4 \}$

§ 4. Законы логики, противоречия, выполнимые и равносильные формулы

Примеры предыдущего параграфа показывают, что таблицы истинности формул могут быть разнообразны. Формулы, принимающие при любых наборах значений пропозициональных переменных одно и то же значение *0*, называются *противоречиями* или *тождественно ложными*. Формулы, принимающие при любых наборах значений пропозициональных переменных одно и то же значение *1*, называются *тавтологиями*, *законами логики* или *тождественно истинными*. Остальные формулы, которые принимают хотя бы одно значение *0* и хотя бы одно значение *1*, называются *выполнимыми*. Для обозначения противоречия или закона логики $A(x_1, \dots, x_n)$ кратко будем писать $A(x_1, \dots, x_n) \equiv \mathbf{0}$ и $A(x_1, \dots, x_n) \equiv \mathbf{1}$ соответственно.

Как следует из определений, для того, чтобы проверить к какому именно виду (закон логики, противоречие или выполнимая) относится данная формула, нужно построить её таблицу истинности и проанализировать последний столбец этой таблицы: если он состоит из одних единиц, то формула будет законом логики, если – из одних нулей, то – противоречием, а в противном случае – формула выполнима.

Пример: Определить вид формулы $A = (\overline{\overline{a} \wedge b} \to a) \leftrightarrow (a \vee b)$.

Строим таблицу истинности:

a	b	$\overline{a}$	$\overline{a} \wedge b$	$\overline{\overline{a} \wedge b}$	$\overline{\overline{a} \wedge b} \to a$	$a \vee b$	A
0	0	1	0	1	0	0	1
0	1	1	1	0	1	1	1
1	0	0	0	1	1	1	1
1	1	0	0	1	1	1	1

Таким образом, формула является законом логики: $A \equiv \mathbf{1}$.

Теорема (об основных законах логики). *Для любых формул A, B, C следующие формулы являются законами логики:*

(1) $A \leftrightarrow A$ *(закон тождества),*

(2) $(A \wedge A) \leftrightarrow A$ *(идемпотентность конъюнкции),*

$(A \vee A) \leftrightarrow A$ *(идемпотентность дизъюнкции),*

(3) $(A \wedge B) \leftrightarrow (B \wedge A)$ *(коммутативность конъюнкции),*

$(A \vee B) \leftrightarrow (B \vee A)$ *(коммутативность дизъюнкции),*

(4) $((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$ *(ассоциативность конъюнкции),*

$((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$ *(ассоциативность дизъюнкции),*

(5) $((A \vee B) \wedge C) \leftrightarrow ((A \wedge C) \vee (B \wedge C))$ *(законы дистрибутивности*

$((A \wedge B) \vee C) \leftrightarrow ((A \vee C) \wedge (B \vee C))$ *конъюнкции и дизъюнкции),*

(6) $\overline{\overline{A}} \leftrightarrow A$ *(закон двойного отрицания),*

(7) $\overline{(A \wedge B)} \leftrightarrow (\overline{A} \vee \overline{B})$ *(законы*

$\overline{(A \vee B)} \leftrightarrow (\overline{A} \wedge \overline{B})$ *де Моргана),*

(8) $(A \to B) \leftrightarrow (\overline{B} \to \overline{A})$ *(закон контрапозиции),*

(9) $(A \leftrightarrow B) \leftrightarrow (\overline{B} \leftrightarrow \overline{A})$ *(закон противоположности),*

(10) $(A \vee (A \wedge B)) \leftrightarrow A$ *(закон поглощения),*

(11) $(A \wedge (A \vee B)) \leftrightarrow A$ *(закон ограничения),*

(12) $(A \vee (\overline{A} \wedge B)) \leftrightarrow (A \vee B)$ *(законы*

$(A \wedge (\overline{A} \vee B)) \leftrightarrow (A \wedge B)$ *удаления),*

(13) $(A \wedge B) \vee (A \wedge \overline{B}) \leftrightarrow A$ *(законы склеивания*

$(A \vee B) \wedge (A \vee \overline{B}) \leftrightarrow A$ *по B),*

(14) $(A \to (B \to C)) \leftrightarrow (B \to (A \to C))$ *(закон перестановки посылок),*

(15) $((A \to B) \wedge (B \to C)) \to (A \to C)$ *(закон силлогизма),*

(16) $(A \wedge B) \to A,\ (A \wedge B) \to B$ *(законы удаления конъюнкции),*

(17) $A \to (A \vee B),\quad B \to (A \vee B)$ *(законы введения дизъюнкции),*

(18) $((\overline{A} \to B) \wedge (\overline{A} \to \overline{B})) \leftrightarrow A$ *(закон обоснования от противного),*

(19) $(A \vee B) \wedge (A \to C) \wedge (B \to C) \to C$ *(закон разбора случаев),*

(20) $((A \vee B) \wedge (C \vee \overline{B})) \to (A \vee C)$ *(законы*

$(B \wedge (C \vee \overline{B})) \to C$ *резолюций),*

законы, выражающие одни логические связки через другие:

(21) $(A \to B) \leftrightarrow (\overline{A} \vee B),\ (A \to B) \leftrightarrow \overline{(A \wedge \overline{B})}$,

(22) $(A \leftrightarrow B) \leftrightarrow (A \to B) \wedge (B \to A),\ (A \leftrightarrow B) \leftrightarrow \overline{(A \wedge \overline{B})} \wedge \overline{(B \wedge \overline{A})}$,

$(A \leftrightarrow B) \leftrightarrow \overline{\overline{(A \vee \overline{B})} \vee \overline{(B \vee \overline{A})}}$, $(A \leftrightarrow B) \leftrightarrow (A \wedge B) \vee (\overline{A} \wedge \overline{B})$,

$\overline{(A \leftrightarrow B)} \leftrightarrow (A \wedge \overline{B}) \vee (\overline{A} \wedge B)$,

(23) $(A \wedge B) \leftrightarrow \overline{(A \to \overline{B})}$, $(A \wedge B) \leftrightarrow \overline{(\overline{A} \vee \overline{B})}$, $A \wedge \overline{B} \leftrightarrow \overline{(A \to B)}$,

(24) $(A \vee B) \leftrightarrow (\overline{A} \to B),\ (A \vee B) \leftrightarrow \overline{(\overline{A} \wedge \overline{B})}$,

законы действий с тавтологиями и противоречиями:

(25) $(A \wedge \mathbf{1}) \leftrightarrow A$, $(A \vee \mathbf{1}) \leftrightarrow \mathbf{1}$,

(26) $(A \wedge \mathbf{0}) \leftrightarrow \mathbf{0}$, $(A \vee \mathbf{0}) \leftrightarrow A$,

(27) $(A \wedge \overline{A}) \leftrightarrow \mathbf{0}$, $(A \vee \overline{A}) \leftrightarrow \mathbf{1}$,

(28) $(A \to A) \leftrightarrow \mathbf{1}$, $(\mathbf{0} \to A) \leftrightarrow \mathbf{1}$, $(\mathbf{1} \to A) \leftrightarrow A$, $(A \to \mathbf{0}) \leftrightarrow \overline{A}$, $(A \to \mathbf{1}) \leftrightarrow \mathbf{1}$,

(29) $(A \leftrightarrow A) \leftrightarrow \mathbf{1}$, $(A \leftrightarrow \overline{A}) \leftrightarrow \mathbf{0}$, $(A \leftrightarrow \mathbf{1}) \leftrightarrow A$, $(A \leftrightarrow \mathbf{0}) \leftrightarrow \overline{A}$,

(30) $\overline{\mathbf{1}} \leftrightarrow \mathbf{0}$, $\overline{\mathbf{0}} \leftrightarrow \mathbf{1}$.

Доказательство. Упражняйтесь в построении таблиц истинности.

Замечание: Многочисленные законы логики, приведённые в этой теореме (так же как многочисленные основные равносильности, выписанные ниже, и правила логического вывода из § 7 главы I), даны не для механического заучивания наизусть, но для осмысления основных логических законов и форм умозаключений. Целью должно являться понимание логических связей, рассуждений и доказательств, а не фотографическое воспроизведение мегабайт бесполезной информации.

Как будет показано ниже, законы логики важны для обеспечения механизма логических умозаключений: все правила логического вывода, применяемые человеком, используют те или иные законы логики. Ясно, что отрицание закона логики является противоречием, и наоборот – отрицание противоречия приводит к закону логики. Поэтому предыдущая теорема даёт и многочисленные примеры противоречий.

Разные по внешнему виду формулы могут иметь одинаковые таблицы истинности, в частности, теорема об основных законах логики даёт много тождественно истинных формул, принимающих только одно значение – *1*. Формулы с одинаковыми таблицами истинности, отличаясь лексикографически, одинаковы с точки зрения логики. Поэтому оправдано следующее определение: формулы $A(x_1, \dots, x_k, y_1, \dots, y_m)$ и $B(y_1, \dots, y_m, z_1, \dots, z_n)$, где $y_1, \dots, y_m$ – все их общие пропозициональные переменные, называются *равносильными*, если при любых наборах значений переменных $x_1, \dots, x_k$, $y_1, \dots, y_m$, $z_1, \dots, z_n$ они принимают одинаковые значения. В этом случае пишут $A \equiv B$.

Пример: $A(x, z) = x \vee (x \wedge z)$, $B(x, y) = (x \wedge y) \vee (x \wedge \overline{y})$.

Построим таблицы истинности этих формул от переменных x, y, z:

x	y	z	$x \wedge z$	A	$x \wedge y$	$\overline{y}$	$x \wedge \overline{y}$	B
0	0	0	0	0	0	1	0	0
0	0	1	0	0	0	1	0	0
0	1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0
1	0	0	0	1	0	1	1	1
1	0	1	1	1	0	1	1	1
1	1	0	0	1	1	0	0	1
1	1	1	1	1	1	0	0	1

Видно, что при любых значениях пропозициональных переменных x, y, z формулы A и B принимают одинаковые истинностные значения, так что $A \equiv B$. С точки зрения истинности эти формулы неразличимы. При этом $A \equiv x$, $B \equiv x$.

Лемма (о свойствах отношения равносильности формул). *Для любых формул A, B, C справедливы следующие утверждения:*

(1) $A \equiv B$ *тогда и только тогда, когда* $(A \leftrightarrow B)$ *– закон логики,*

(2) $A \equiv A$ *(рефлексивность равносильности),*

(3) если $A \equiv B$, *то* $B \equiv A$ *(симметричность равносильности),*

(4) если $A \equiv B$ *и* $B \equiv C$, *то* $A \equiv C$ *(транзитивность равносильности)*

(5) если $A \equiv B$, $C \equiv D$, *то* $\overline{A} \equiv \overline{B}$ *и для любой логической связки* $\omega \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ *верно* $(A \,\omega\, C) \equiv (B \,\omega\, D)$, $(C \,\omega\, A) \equiv (D \,\omega\, B)$.

Доказательство. *(1)* Пусть вначале $A \equiv B$. Рассмотрим таблицу истинности формулы $A \leftrightarrow B$ и любую её строку с интерпретацией $\varepsilon = (\varepsilon_1 ; \ldots ; \varepsilon_s)$. По определению равносильности формул имеем $A(\varepsilon) = B(\varepsilon)$, и значит, $(A(\varepsilon) \leftrightarrow B(\varepsilon)) = 1$. Таким образом, формула $(A \leftrightarrow B)$ – закон логики.

Пусть наоборот, $(A \leftrightarrow B)$ – закон логики, т.е. при любой интерпретации $\varepsilon = (\varepsilon_1 ; \ldots ; \varepsilon_s)$ верно $A(\varepsilon) = B(\varepsilon)$, а значит, $A \equiv B$.

(2), (3) очевидны.

(4) Пусть $A \equiv B$ и $B \equiv C$. Тогда при любом наборе $\varepsilon = (\varepsilon_1 ; \ldots ; \varepsilon_s)$ значений переменных верно $A(\varepsilon) = B(\varepsilon)$ и $B(\varepsilon) = C(\varepsilon)$, т.е. $A(\varepsilon) = C(\varepsilon)$, $A \equiv C$.

(5) Если $A \equiv B$, $C \equiv D$, то для любой интерпретации $\varepsilon = (\varepsilon_1 ; \ldots ; \varepsilon_s)$ верно $A(\varepsilon) = B(\varepsilon)$, $C(\varepsilon) = D(\varepsilon)$. Поэтому $\overline{A}(\varepsilon) = \overline{A(\varepsilon)} = \overline{B(\varepsilon)} = \overline{B}(\varepsilon)$ и для любой логической связки $\omega \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ имеем $(A \,\omega\, C)(\varepsilon) = (A(\varepsilon) \,\omega\, C(\varepsilon)) = (B(\varepsilon) \,\omega\, D(\varepsilon)) = (B \,\omega\, D)(\varepsilon)$. Аналогично и $(C \,\omega\, A)(\varepsilon) = (D \,\omega\, B)(\varepsilon)$.

Лемма доказана.

Теорема (об основных равносильностях). *Для любых формул A, B, C справедливы следующие равносильности:*

(1) $A \equiv A$ *(закон тождества),*

(2) $(A \wedge A) \equiv A$ *(идемпотентность конъюнкции),*

$(A \vee A) \equiv A$ *(идемпотентность дизъюнкции),*

(3) $(A \wedge B) \equiv (B \wedge A)$ *(коммутативность конъюнкции),*

$(A \vee B) \equiv (B \vee A)$ *(коммутативность дизъюнкции),*

(4) $((A \wedge B) \wedge C) \equiv (A \wedge (B \wedge C))$ *(ассоциативность конъюнкции),*

$((A \vee B) \vee C) \equiv (A \vee (B \vee C))$ *(ассоциативность дизъюнкции),*

(5) $((A \vee B) \wedge C) \equiv ((A \wedge C) \vee (B \wedge C))$ *(законы дистрибутивности*

$((A \wedge B) \vee C) \equiv ((A \vee C) \wedge (B \vee C))$ *конъюнкции и дизъюнкции),*

(6) $\overline{\overline{A}} \equiv A$ *(закон двойного отрицания),*

(7) $\overline{(A \wedge B)} \equiv (\overline{A} \vee \overline{B})$ *(законы*

$\overline{(A \vee B)} \equiv (\overline{A} \wedge \overline{B})$ *де Моргана),*

(8) $(A \to B) \equiv (\overline{B} \to \overline{A})$ *(закон контрапозиции),*

(9) $(A \leftrightarrow B) \equiv (\overline{B} \leftrightarrow \overline{A})$ *(закон противоположности),*

(10) $(A \vee (A \wedge B)) \equiv A$ *(закон поглощения),*

(11) $(A \wedge (A \vee B)) \equiv A$ *(закон ограничения),*

(12) $(A \vee (\overline{A} \wedge B)) \equiv (A \vee B)$ *(законы*

$(A \wedge (\overline{A} \vee B)) \equiv (A \wedge B)$ *удаления),*

(13) $(A \wedge B) \vee (A \wedge \overline{B}) \equiv A$ *(закон склеивания*

$(A \vee B) \wedge (A \vee \overline{B}) \equiv A$ *по B),*

(14) $(A \to (B \to C)) \equiv (B \to (A \to C))$ *(закон перестановки посылок),*

(15) $((\overline{A} \to B) \wedge (\overline{A} \to \overline{B})) \equiv A$ *(закон рассуждений от противного),*

законы, выражающие одни логические связки через другие:

(16) $(A \to B) \equiv (\overline{A} \vee B)$, $(A \to B) \equiv \overline{(A \wedge \overline{B})}$,

(17) $(A \leftrightarrow B) \equiv (A \to B) \wedge (B \to A)$, $(A \leftrightarrow B) \equiv \overline{(A \wedge \overline{B})} \wedge \overline{(B \wedge \overline{A})}$,

$(A \leftrightarrow B) \equiv \overline{\overline{(A \vee \overline{B})} \vee \overline{(B \vee \overline{A})}}$, $(A \leftrightarrow B) \equiv (A \wedge B) \vee (\overline{A} \wedge \overline{B})$,

$\overline{(A \leftrightarrow B)} \equiv (A \wedge \overline{B}) \vee (\overline{A} \wedge B)$,

(18) $(A \wedge B) \equiv \overline{(A \to \overline{B})}$, $(A \wedge B) \equiv \overline{(\overline{A} \vee \overline{B})}$, $A \wedge \overline{B} \equiv \overline{(A \to B)}$,

(19) $(A \vee B) \equiv (\overline{A} \to B)$, $(A \vee B) \equiv \overline{(\overline{A} \wedge \overline{B})}$,

законы действий с тавтологиями и противоречиями:

(20) $(A \wedge \mathbf{1}) \equiv A$, $(A \vee \mathbf{1}) \equiv \mathbf{1}$,

(21) $(A \wedge \mathbf{0}) \equiv \mathbf{0}$, $(A \vee \mathbf{0}) \equiv A$,

(22) $(A \wedge \overline{A}) \equiv \mathbf{0}$, $(A \vee \overline{A}) \equiv \mathbf{1}$,

(23) $(A \to A) \equiv \mathbf{1}$, $(\mathbf{0} \to A) \equiv \mathbf{1}$, $(\mathbf{1} \to A) \equiv A$, $(A \to \mathbf{0}) \equiv \overline{A}$, $(A \to \mathbf{1}) \equiv \mathbf{1}$,

(24) $(A \leftrightarrow A) \equiv \mathbf{1}$, $(A \leftrightarrow \overline{A}) \equiv \mathbf{0}$, $(A \leftrightarrow \mathbf{1}) \equiv A$, $(A \leftrightarrow \mathbf{0}) \equiv \overline{A}$,

(25) $\overline{\mathbf{1}} \equiv \mathbf{0}$, $\overline{\mathbf{0}} \equiv \mathbf{1}$.

Доказательство. Упражняйтесь в построении таблиц истинности или примените теорему об основных законах логики и утверждение *(1)* леммы о свойствах отношения равносильности формул.

Приведённые в теореме простейшие равносильности вместе с утверждением *(5)* леммы о свойствах отношения равносильности формул позволяют упрощать формулы, точнее – находить для заданной формулы более простую, равносильную ей. Правда, понятие простоты субъективно, т.к. критерии простоты могут быть разными.

Примеры: 1. $\overline{(a \to b \vee c)} \to a \equiv \{(16)\} \equiv \overline{\overline{(a \to b \vee c)}} \vee a \equiv$ *{двойное отрицание}* $\equiv (a \to (b \vee c)) \vee a \equiv \{(16)\} \equiv (\overline{a} \vee b \vee c) \vee a \equiv$ *{ассоциативность}* $\equiv \overline{a} \vee b \vee c \vee a \equiv$ *{коммутативность}* $\equiv (a \vee \overline{a}) \vee b \vee c \equiv \{(22)\} \equiv \mathbf{1} \vee (b \vee c) \equiv \{(20)\} \equiv \mathbf{1}$.

2. $(a \to b) \to \overline{a} \equiv \{(16)\} \equiv (\overline{a} \vee b) \to \overline{a} \equiv \{?!\} \equiv \overline{\overline{a} \vee b} \vee \overline{a} \equiv$ *{де Морган}* $\equiv (\overline{\overline{a}} \wedge \overline{b}) \vee \overline{a} \equiv$ *{двойное отрицание}* $\equiv (a \wedge \overline{b}) \vee \overline{a} \equiv \{?!\} \equiv \overline{a} \vee \overline{b}$.

3. $\overline{(a \to b)} \vee (a \to c) \wedge \overline{a} \equiv \{(16)\} \equiv \overline{\overline{a} \vee b} \vee ((\overline{a} \vee c) \wedge \overline{a}) \equiv$ *{де Морган, ограничение}* $\equiv \overline{\overline{a}} \wedge \overline{b} \vee \overline{a} \equiv$ *{двойное отрицание}* $\equiv (a \wedge \overline{b}) \vee \overline{a} \equiv$ *{дистрибутивность}* $\equiv (a \vee \overline{a}) \wedge (\overline{b} \vee \overline{a}) \equiv \{(22)\} \equiv \mathbf{1} \wedge (\overline{b} \vee \overline{a}) \equiv \{(20)\} \equiv \overline{b} \vee \overline{a}$.

4. $((\overline{a} \leftrightarrow c) \to b) \vee a \vee c \equiv \{(16)\} \equiv \overline{\overline{a} \leftrightarrow c} \vee b \vee a \vee c \equiv \{(17)\} \equiv \overline{(\overline{a} \wedge c) \vee (\overline{\overline{a}} \wedge \overline{c})} \vee b \vee a \vee c \equiv$ *{де Морган}* $\equiv (a \vee \overline{c}) \wedge (\overline{a} \vee c) \vee b \vee a \vee c \equiv$ *{дистрибутивность,* $\mathbf{0}$*,* $\mathbf{1}$*}* $\equiv (a \wedge c \vee \overline{c} \wedge \overline{a}) \vee b \vee a \vee c \equiv$ *{ассоциативность, коммутативность, поглощение}* $\equiv \overline{a} \wedge \overline{c} \vee b \vee (a \vee c) \equiv$ *{коммутативность}* $\equiv (a \vee \overline{a} \wedge \overline{c}) \vee c \vee b \equiv$ *{удаление}* $\equiv (a \vee \overline{c}) \vee c \vee b \equiv \{(22)\} \equiv a \vee \mathbf{1} \vee b \equiv \{(20)\} \equiv \mathbf{1}$.

Общий алгоритм упрощения формул сформулировать затруднительно, поскольку нет общепринятого критерия простоты формулы. Однако предыдущие примеры показывают, что в равносильных преобразованиях формул можно выделить следующие этапы:

1. *избавляемся от импликаций и эквивалентностей,* используя равносильности $A \to B \equiv \overline{A} \vee B$ и $A \leftrightarrow B \equiv (A \wedge B) \vee (\overline{A} \wedge \overline{B})$,

2. *избавляемся от длинных отрицаний* (т.е. отрицаний, стоящих не над переменными) с помощью законов де Моргана: $\overline{A \wedge B} \equiv \overline{A} \vee \overline{B}$, $\overline{A \vee B} \equiv \overline{A} \wedge \overline{B}$,

3. *избавляемся от многократных отрицаний* (двукратных и более) с помощью закона двойного отрицания $\overline{\overline{A}} \equiv A$,

После этих преобразований получим формулу, записанную с помощью конъюнкций, дизъюнкций и коротких отрицаний, стоящих над пропозициональными переменными. На эту формулу можно смотреть как на алгебраическое выражение от переменных $x_1, \dots, x_n, \overline{x_1}, \dots, \overline{x_n}$. При этом ввиду законов дистрибутивности можно равноправно считать, что роль сложения выполняет операция $\vee$ дизъюнкции, а роль умножения – операция $\wedge$ конъюнкции, или же наоборот: роль сложения выполняет операция $\wedge$ конъюнкции, а роль умножения – операция $\vee$ дизъюнкции.

4. *если считать, что* $\vee$ *– аналог сложения, а* $\wedge$ *– умножения, то раскрывая скобки (по дистрибутивности) и учитывая законы коммутативности* $A \vee B \equiv B \vee A$, $A \wedge B \equiv B \wedge A$, *идемпотентности* $A \vee A \equiv A$, $A \wedge A \equiv A$, *и правила действий с противоречиями, приведём формулу к дизъюнктивной форме (ДФ)* $\bigvee\limits_{i_1 < \dots < i_s} (y_{i_1} \wedge \dots \wedge y_{i_s})$, *где каждое* y_i *– либо переменная* x_i, *либо её отрицание* $\overline{x_i}$. *Эту дизъюнктивную форму иногда можно ещё более упростить, применяя законы поглощения* $A \vee (A \wedge B) \equiv A$, *удаления* $A \vee (\overline{A} \wedge B) \equiv A \vee B$ *и склейки* $(A \wedge B) \vee (A \wedge \overline{B}) \equiv A$.

5. *если считать, что* $\wedge$ *– аналог сложения, а* $\vee$ *– умножения, то раскрывая скобки (по дистрибутивности) и учитывая законы коммутативности* $A \vee B \equiv B \vee A$, $A \wedge B \equiv B \wedge A$, *идемпотентности* $A \vee A \equiv A$, $A \wedge A \equiv A$, *и правила действий с тавтологиями, получим конъюнктивную форму (КФ)* $\bigwedge\limits_{i_1 < \dots < i_s} (y_{i_1} \vee \dots \vee y_{i_s})$, *где каждое* y_i *– либо переменная* x_i, *либо её отрицание* $\overline{x_i}$. *Эту конъюнктивную форму можно ещё более упростить, применяя законы* $A \wedge (A \vee B) \equiv A$, $A \wedge (\overline{A} \vee B) \equiv A \wedge B$ *и* $(A \vee B) \wedge (A \vee \overline{B}) \equiv A$.

Пример: Привести формулу $x \to y \leftrightarrow \overline{\overline{x} \wedge \overline{y} \to z}$ к дизъюнктивной и конъюнктивной формам.

$$x \to y \leftrightarrow \overline{\overline{x} \wedge \overline{y} \to z} = (x \to y) \leftrightarrow \overline{(\overline{x} \wedge \overline{y}) \to z} \equiv (\overline{x} \vee y) \leftrightarrow \overline{\overline{(\overline{x} \wedge \overline{y})} \vee z} \equiv$$

$$\equiv (\overline{x} \vee y) \leftrightarrow \overline{x} \wedge \overline{y} \wedge \overline{z} \equiv ((\overline{x} \vee y) \wedge \overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (\overline{\overline{x \vee y}} \wedge \overline{\overline{x} \wedge \overline{y} \wedge \overline{z}}) \equiv$$

$$\equiv ((\overline{x} \vee y) \wedge \overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge (x \vee y \vee z)).$$

Дизъюнктивная форма (ДФ): $((\overline{x} \vee y) \wedge \overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge (x \vee y \vee z)) \equiv$

$$\equiv (((\overline{x} \wedge \overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (y \wedge \overline{x} \wedge \overline{y} \wedge \overline{z})) \vee (x \wedge \overline{y} \wedge (x \vee y \vee z)) \equiv$$

$$\equiv ((\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee \mathbf{0}) \vee (x \wedge \overline{y} \wedge (x \vee y \vee z)) \equiv$$

$$\equiv (\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge (x \vee y \vee z)) \equiv$$

$$\equiv (\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee ((x \wedge \overline{y} \wedge x) \vee (x \wedge \overline{y} \wedge y) \vee (x \wedge \overline{y} \wedge z)) \equiv$$

$$\equiv (\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee ((x \wedge \overline{y}) \vee (x \wedge \overline{y} \wedge z)) \equiv (\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge \overline{y}) \equiv$$

$$\equiv ((\overline{x} \wedge \overline{z}) \vee x) \wedge \overline{y} \equiv (x \vee \overline{z}) \wedge \overline{y} \equiv (x \wedge \overline{y}) \vee (\overline{y} \wedge \overline{z}) - ДФ.$$

Конъюнктивная форма (КФ): $((\overline{x} \vee y) \wedge \overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge (x \vee y \vee z)) \equiv$

$$\equiv ((\overline{x} \vee y) \vee x) \wedge ((\overline{x} \vee y) \vee \overline{y}) \wedge ((\overline{x} \vee y) \vee (x \vee y \vee z)) \wedge$$

$$\wedge (\overline{x} \vee x) \wedge (\overline{x} \vee \overline{y}) \wedge (\overline{x} \vee (x \vee y \vee z)) \wedge$$

$$\wedge (\overline{y} \vee x) \wedge (\overline{y} \vee \overline{y}) \wedge (\overline{y} \vee (x \vee y \vee z)) \wedge$$

$$\wedge (\overline{z} \vee x) \wedge (\overline{z} \vee \overline{y}) \wedge (\overline{z} \vee (x \vee y \vee z)) \equiv$$

$$\equiv (\mathbf{1} \wedge \mathbf{1} \wedge \mathbf{1}) \wedge (\mathbf{1} \wedge (\overline{x} \vee \overline{y}) \wedge \mathbf{1}) \wedge ((\overline{y} \vee x) \wedge \overline{y} \wedge \mathbf{1}) \wedge$$

$$\wedge ((\overline{z} \vee x) \wedge (\overline{z} \vee \overline{y}) \wedge \mathbf{1}) \equiv$$

$$\equiv (\overline{x} \vee \overline{y}) \wedge (\overline{y} \vee x) \wedge \overline{y} \wedge (\overline{z} \vee x) \wedge (\overline{z} \vee \overline{y}) \equiv$$

$$\equiv \overline{y} \wedge (\overline{z} \vee x) \wedge (\overline{z} \vee \overline{y}) \equiv (\overline{z} \vee x) \wedge \overline{y} \wedge (\overline{z} \vee \overline{y}) \equiv (\overline{z} \vee x) \wedge \overline{y} - КФ.$$

§ 5. Совершенные дизъюнктивная и конъюнктивная нормальные формы

Итак, любая формула $A(x_1, \dots, x_n)$ определяет таблицу истинности, в которой можно опустить столбцы с промежуточными вычислениями. При этом равносильным формулам $A(x_1, \dots, x_n) \equiv B(x_1, \dots, x_n)$ соответствуют одинаковые таблицы истинности (если предположить, что в первых n столбцах этих таблиц всевозможные наборы

x_1	…	x_n	$A(x_1, \dots, x_n)$
…	…	…	…
ε_1	…	ε_n	$A(\varepsilon_1, \dots, \varepsilon_n)$
…	…	…	…

значений пропозициональных переменных $x_1, \dots, x_n$ (интерпретации) перечислены в одном и том же порядке). Возникает вопрос: каждая ли таблица рассматриваемого вида будет таблицей истинности некоторой формулы ?

x_1	x_2	x_3	?
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Пример. Найти формулу со следующей таблицей истинности:

Если формула $A(x_1, x_2, x_3)$ – искомая, то

$$A(x_1, x_2, x_3) = 1 \Leftrightarrow$$

$$\Leftrightarrow (x_1 = 0 \wedge x_2 = 0 \wedge x_3 = 1) \vee (x_1 = 0 \wedge x_2 = 1 \wedge x_3 = 1) \vee$$

$$\vee (x_1 = 1 \wedge x_2 = 0 \wedge x_3 = 1) \Leftrightarrow$$

$$\Leftrightarrow (\overline{x_1} \wedge \overline{x_2} \wedge x_3 = 1) \vee (\overline{x_1} \wedge x_2 \wedge x_3 = 1) \vee$$

$$\vee (x_1 \wedge \overline{x_2} \wedge \overline{x_3} = 1) \Leftrightarrow$$

$$\Leftrightarrow (\overline{x_1} \wedge \overline{x_2} \wedge x_3) \vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge \overline{x_3}) = 1.$$

Таким образом, в качестве искомой формулы можно взять

$$A(x_1, x_2, x_3) = (\overline{x_1} \wedge \overline{x_2} \wedge x_3) \vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge \overline{x_3}).$$

Полученное в примере выражение для формулы $A(x_1, x_2, x_3)$ устроено регулярно: оно является дизъюнкцией выражений вида $y_1 \wedge y_2 \wedge y_3$, где каждое y_i является или переменной x_i или её отрицанием $\overline{x_i}$. Аналогичные построения можно применить и в общем случае, используя соответствующие общие обозначения, к описанию которых теперь и переходим.

Для пропозициональной переменной x и фиксированного значения $\varepsilon \in \{0, 1\}$ введём следующее обозначение $x^\varepsilon = \begin{cases} x, & \text{если } \varepsilon = 1, \\ \overline{x}, & \text{если } \varepsilon = 0 \end{cases}$. Выражение x^ε можно считать булевой функцией переменного x, вычисляя её значение при $x = \delta \in \{0, 1\}$ естественным образом: $\delta^\varepsilon = \begin{cases} \delta, & \text{если } \varepsilon = 1, \\ \overline{\delta}, & \text{если } \varepsilon = 0 \end{cases}$.

Найденная в предыдущем примере формула в этих обозначениях может быть записана так: $A(x_1, x_2, x_3) = (x_1^0 \wedge x_2^0 \wedge x_3^1) \vee (x_1^0 \wedge x_2^1 \wedge x_3^1) \vee (x_1^1 \wedge x_2^0 \wedge x_3^0)$. Следует заметить, что наборы степеней при переменных x_1, x_2, x_3, т.е. наборы $(0; 0; 1)$, $(0; 1; 1)$, $(1; 0; 0)$, – это в точности те интерпретации из исходной таблицы, при которых в последнем её столбце стоит значение 1:

$$A(x_1, x_2, x_3) = \bigvee_{\substack{(\varepsilon_1; \varepsilon_2; \varepsilon_3) \\ ?(\varepsilon_1; \varepsilon_2; \varepsilon_3) = 1}} (x_1^{\varepsilon_1} \wedge x_2^{\varepsilon_2} \wedge x_3^{\varepsilon_3}).$$

Лемма (о значениях выражения x^ε). *(1)* $x^\varepsilon = 1 \Leftrightarrow x = \varepsilon$.

(2) $\overline{x^{\varepsilon}} = x^{\bar{\varepsilon}}$.

(3) $x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n} = 1 \Leftrightarrow (x_1 = \varepsilon_1) \wedge \ldots \wedge (x_n = \varepsilon_n)$.

(4) $\overline{x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n}} = x_1^{\bar{\varepsilon}_1} \vee \ldots \vee x_n^{\bar{\varepsilon}_n}$.

Доказательство. Следующая таблица показывает, что $x^{\varepsilon} = 1$ тогда и только тогда, когда $x = \varepsilon$, а также, что $\overline{x^{\varepsilon}} = x^{\bar{\varepsilon}}$:

ε	формула x^{ε}	x	значение x^{ε}	$\bar{\varepsilon}$	формула $x^{\bar{\varepsilon}}$	x	значение $x^{\bar{\varepsilon}}$	значение $\overline{x^{\varepsilon}}$
0	$\bar{x}$	0	1	1	x	0	0	0
		1	0			1	1	1
1	x	0	0	0	$\bar{x}$	0	1	1
		1	1			1	0	0

Остальные утверждения отсюда следуют:

$$(x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n} = 1) \Leftrightarrow (x_1^{\varepsilon_1} = 1) \wedge \ldots \wedge (x_n^{\varepsilon_n} = 1) \Leftrightarrow (x_1 = \varepsilon_1 \wedge \ldots \wedge x_n = \varepsilon_n),$$

$$\overline{x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n}} = \overline{x_1^{\varepsilon_1}} \vee \ldots \vee \overline{x_n^{\varepsilon_n}} = x_1^{\bar{\varepsilon}_1} \vee \ldots \vee x_n^{\bar{\varepsilon}_n}.$$

Лемма доказана.

*Элементарной конъюнкцией (*соответственно *дизъюнкцией) от n пропозициональных переменных* $x_1, \ldots, x_n$ назовём формулу вида $x_{i_1}^{\varepsilon_{i_1}} \wedge \ldots \wedge x_{i_k}^{\varepsilon_{i_k}}$ *(*соответственно $x_{i_1}^{\varepsilon_{i_1}} \vee \ldots \vee x_{i_k}^{\varepsilon_{i_k}}$*),* где $k \le n$, $1 \le i_1 < \ldots < i_k \le n$, $\varepsilon_{i_j} \in \{0, 1\}$. Менее формально, элементарная конъюнкция (дизъюнкция) – это выражение $y_1 \wedge \ldots \wedge y_k$ *(*соответственно $y_1 \vee \ldots \vee y_k$*),* где каждое y_s является либо пропозициональной переменной, либо её отрицанием, причём переменные, участвующие в этом выражении упорядочены по возрастанию своих номеров. Если в элементарной конъюнкции (соответственно дизъюнкции) участвуют все переменные, т.е. $k = n$, то такая элементарная конъюнкция (соответственно дизъюнкция) называется *совершенной элементарной конъюнкцией* (соответственно *дизъюнкцией*) . Любая дизъюнкция различных элементарных конъюнкций (соответственно конъюнкция различных элементарных дизъюнкций) называется *дизъюнктивной нормальной формой* (соответственно *конъюнктивной нормальной формой*) . Любая дизъюнкция различных совершенных элементарных конъюнкций (соответственно конъюнкция различных совершенных элементарных дизъюнкций) называется *совершенной дизъюнктивной нормальной формой,* или кратко *СДНФ* (соответственно *совершенной конъюнктивной нормальной формой,* или кратко

СКНФ). Таким образом, *СДНФ* (соответственно *СКНФ*) может быть записана так: $\bigvee\limits_{(\varepsilon_1;\ldots;\varepsilon_n)} (x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n})$ (соответственно $\bigwedge\limits_{(\varepsilon_1;\ldots;\varepsilon_n)} (x_1^{\varepsilon_1} \vee \ldots \vee x_n^{\varepsilon_n})$).

Примеры: 1. конъюнкция $x \wedge \overline{x}$ не является элементарной конъюнкцией, т.к. одна переменная в ней участвует дважды – вначале без отрицания, а потом с отрицанием.

2. $x \wedge \overline{y}$ – совершенная элементарная конъюнкция от двух переменных x и y, но она не является совершенной элементарной конъюнкцией от трёх переменных x, y, z (т.к. переменная z не участвует в этом выражении). Эта формула будет совершенной дизъюнктивной нормальной формой от переменных x, y, но она не будет совершенной, если рассматривать её от трёх переменных.

3. $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$ – совершенная конъюнктивная нормальная форма от переменных x_1, x_2, x_3.

4. $(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$ – не является совершенной конъюнктивной нормальной формой от переменных x_1, x_2, x_3, т.к. содержит две одинаковые элементарные дизъюнкции.

5. Любая дизъюнктивная нормальная форма принимает значение *1* хотя бы на одном наборе пропозициональных переменных. Докажем это для совершенной дизъюнктивной нормальной формы – в общем случае рассуждения аналогичны. Действительно, формула $\bigvee\limits_{(\varepsilon_1;\ldots;\varepsilon_n)} (x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n})$ истинна тогда и только тогда, когда истинна хотя бы одна её элементарная конъюнкция $x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n}$. Ввиду леммы она истинна при $x_1 = \varepsilon_1, \ldots, x_n = \varepsilon_n$, что и требовалось доказать.

6. Как следует из предыдущего примера, для противоречий не существует *СДНФ*. Однако легко записать формулу от n переменных, равносильную противоречию: например, $x_1 \wedge \overline{x_1}$.

7. Любая конъюнктивная нормальная форма принимает значение *0* хотя бы на одном наборе пропозициональных переменных. Доказательство аналогично предыдущему.

8. Как следует из предыдущего примера, для законов логики не существует *СКНФ*. Однако, легко записать формулу от n переменных, равносильную закону логики: например, $x_1 \vee \overline{x_1}$.

Возвращаемся к общей задаче построения формулы с заданной таблицей истинности.

Теорема (о СДНФ и СКНФ). *(1) Для любой таблицы, последний столбец которой состоит не из одних нулей, существует СДНФ с этой таблицей истинности.*

(2) Эта СДНФ единственна с точностью до порядка совершенных элементарных конъюнкций.

(3) В частности, для любой формулы $A(x_1, \dots, x_n)$, не являющейся противоречием, существует единственная (с точностью до перестановки элементарных конъюнкций) равносильная ей СДНФ.

(1′) Для любой таблицы, последний столбец которой состоит не из одних единиц, существует СКНФ с этой таблицей истинности.

(2′) Эта СКНФ единственна с точностью до порядка совершенных элементарных дизъюнкций.

(3′) В частности, для любой формулы $A(x_1, \dots, x_n)$, не являющейся законом логики, существует единственная (с точностью до перестановки элементарных дизъюнкций) равносильная ей СКНФ.

x_1	…	x_n	$A(x_1, \dots, x_n)$
…	…	…	…
ε_1	…	ε_n	$A(\varepsilon_1, \dots, \varepsilon_n)$
…	…	…	…

Доказательство. *(1)* Вначале докажем существование *СДНФ* для таблицы слева с неизвестной формулой $A(x_1, \dots, x_n) \not\equiv \mathbf{0}$. Для этого по данной таблице образуем следующее выражение $Д(x_1, \dots, x_n) = \bigvee\limits_{\substack{(\varepsilon_1; \dots; \varepsilon_n) \\ A(\varepsilon_1; \dots; \varepsilon_n) = 1}} (x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n})$. Это – *СДНФ*, причём

$$(Д(\varepsilon_1, \dots, \varepsilon_n) = 1) \Leftrightarrow (\text{найдётся такая интерпретация } (\delta_1; \dots; \delta_n), \text{ что}$$

$$A(\delta_1, \dots, \delta_n) = 1, \text{ и } \delta_1^{\varepsilon_1} \wedge \dots \wedge \delta_n^{\varepsilon_n} = 1) \Leftrightarrow (\text{найдётся такая интерпретация}$$

$$(\delta_1; \dots; \delta_n), \text{ что } A(\delta_1, \dots, \delta_n) = 1, \text{ и } (\delta_1 = \varepsilon_1) \wedge \dots \wedge (\delta_n = \varepsilon_n)) \Leftrightarrow$$

$$\Leftrightarrow (A(\varepsilon_1, \dots, \varepsilon_n) = 1), \text{ что и требовалось.}$$

(2) Докажем теперь единственность (с точностью до перестановки элементарных конъюнкций) *СДНФ* с заданной таблицей истинности. Пусть нашлись две такие *СДНФ* $Д_1(x_1, \dots, x_n)$ и $Д_2(x_1, \dots, x_n)$, что $Д_1(x_1, \dots, x_n) \equiv Д_2(x_1, \dots, x_n)$. Будет показано, что любая элементарная конъюнкция формулы $Д_1(x_1, \dots, x_n)$ участвует и в $Д_2(x_1, \dots, x_n)$, и наоборот, любая элементарная конъюнкция формулы $Д_2(x_1, \dots, x_n)$ участвует в $Д_1(x_1, \dots, x_n)$. Таким образом, будет показано, что эти *СДНФ* состоят из одного и того же набора элементарных конъюнкций.

Пусть элементарная конъюнкция $x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n}$ участвует в $Д_1(x_1, \ldots, x_n)$. Тогда эта конъюнкция принимает значение 1 при $x_1 = \varepsilon_1, \ldots, x_n = \varepsilon_n$, а значит, $Д_1(\varepsilon_1, \ldots, \varepsilon_n) = 1$. Ввиду $Д_1(x_1, \ldots, x_n) \equiv Д_2(x_1, \ldots, x_n)$ имеем $Д_2(\varepsilon_1, \ldots, \varepsilon_n) = 1$. Значит, найдётся такая элементарная конъюнкция $x_1^{\delta_1} \wedge \ldots \wedge x_n^{\delta_n}$ в $Д_2(x_1, \ldots, x_n)$, что $\varepsilon_1^{\delta_1} \wedge \ldots \wedge \varepsilon_n^{\delta_n} = 1$. Однако, $(\varepsilon_1^{\delta_1} \wedge \ldots \wedge \varepsilon_n^{\delta_n} = 1) \Leftrightarrow (\delta_1 = \varepsilon_1 \wedge \ldots \wedge \delta_n = \varepsilon_n)$, т.е. элементарная конъюнкция $x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n}$ участвует и в формуле $Д_2(x_1, \ldots, x_n)$.

Аналогично доказывается, что любая элементарная конъюнкция формулы $Д_2(x_1, \ldots, x_n)$ участвует и в формуле $Д_1(x_1, \ldots, x_n)$, а значит, эти *СДНФ* состоят из одних и тех же совершенных элементарных конъюнкций (с точностью до их перестановки).

(3) следует из *(1)* и *(2)*: достаточно по заданной формуле $A(x_1, \ldots, x_n) \not\equiv \mathbf{0}$ построить таблицу истинности, и найти единственную *СДНФ* $Д(x_1, \ldots, x_n)$ с этой таблицей истинности. Тогда $A(x_1, \ldots, x_n) \equiv Д(x_1, \ldots, x_n)$.

(1′) выведем это из *(1)*. По условию, искомая формула $A(x_1, \ldots, x_n)$ не тождественно истинна, так что $\overline{A}(x_1, \ldots, x_n) \not\equiv \mathbf{0}$. По доказанному в *(1)*, найдётся *СДНФ* $Д(x_1, \ldots, x_n) = \bigvee\limits_{\overline{A}(\varepsilon_1; \ldots; \varepsilon_n) = 1} (\varepsilon_1; \ldots; \varepsilon_n)} (x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n}) \equiv \overline{A}(x_1, \ldots, x_n)$. Значит,

$$A(x_1, \ldots, x_n) \equiv \overline{\overline{A}}(x_1, \ldots, x_n) \equiv \overline{\bigvee\limits_{\overline{A}(\varepsilon_1; \ldots; \varepsilon_n) = 1} (\varepsilon_1; \ldots; \varepsilon_n)} (x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n})} \equiv \{\text{де Морган}\} \equiv$$

$$\equiv \bigwedge_{\overline{A}(\varepsilon_1; \ldots; \varepsilon_n) = 1} \overline{(x_1^{\varepsilon_1} \wedge \ldots \wedge x_n^{\varepsilon_n})} \equiv \bigwedge_{A(\varepsilon_1; \ldots; \varepsilon_n) = 0} (\overline{x_1^{\varepsilon_1}} \vee \ldots \vee \overline{x_n^{\varepsilon_n}}) \equiv \bigwedge_{A(\varepsilon_1; \ldots; \varepsilon_n) = 0} (x_1^{\overline{\varepsilon_1}} \vee \ldots \vee x_n^{\overline{\varepsilon_n}})$$

– искомая *СКНФ*.

(2′) Если найдены две равносильные *СКНФ* $K_1(x_1, \ldots, x_n) \equiv K_2(x_1, \ldots, x_n)$, то у формулы $\overline{A}(x_1, \ldots, x_n)$ существовали бы две *СДНФ* $\overline{K_1}(x_1, \ldots, x_n)$ и $\overline{K_2}(x_1, \ldots, x_n)$. По доказанному в *(1)*, $\overline{K_1}(x_1, \ldots, x_n)$ и $\overline{K_2}(x_1, \ldots, x_n)$ отличаются только порядком элементарных конъюнкций, а значит, $K_1(x_1, \ldots, x_n)$ и $K_2(x_1, \ldots, x_n)$ отличаются только порядком элементарных дизъюнкций, что и требовалось.

(3′) выводится из *(1′)* и *(2′)* аналогично тому, как *(3)* выведено из *(1)* и *(2)*.

Теорема доказана.

На практике *СКНФ* можно получать, как следует из приведённых при доказательстве теоремы вычислений, без привлечения отрицания формулы. По заданной таблице истинности формулы для каждого набора значений $(\varepsilon_1; \ldots; \varepsilon_n)$ со

свойством $A(\varepsilon_1, \dots, \varepsilon_n) = 0$ построим элементарную дизъюнкцию $x_1^{\overline{\varepsilon_1}} \vee \dots \vee x_n^{\overline{\varepsilon_n}}$ и конъюнкцию всех таких дизъюнкций: $\bigwedge\limits_{\substack{(\varepsilon_1;\dots;\varepsilon_n) \\ A(\varepsilon_1;\dots;\varepsilon_n)=0}} (x_1^{\overline{\varepsilon_1}} \vee \dots \vee x_n^{\overline{\varepsilon_n}})$, которая и будет *СКНФ* для исходной не тождественно истинной формулы $A(x_1, \dots, x_n)$.

Примеры: 1. Построить *СКНФ* для формулы $(x \to y) \wedge z \vee (y \to x) \wedge \overline{z}$.

x	y	z	$x \to y$	$(x \to y) \wedge z$	$y \to x$	$\overline{z}$	$(y \to x) \wedge \overline{z}$	A
0	0	0	1	0	1	1	1	1
0	0	1	1	1	1	0	0	1
0	1	0	1	0	0	1	0	0
0	1	1	1	1	0	0	0	1
1	0	0	0	0	1	1	1	1
1	0	1	0	0	1	0	0	0
1	1	0	1	0	1	1	1	1
1	1	1	1	1	1	0	0	1

Вначале строим таблицу истинности формулы. Далее, выбираем нулевые значения формулы с интерпретациями *(0; 1; 0)* и *(1; 0; 1)* соответственно и строим по этим наборам элементарные дизъюнкции

$x^{\overline{0}} \vee y^{\overline{1}} \vee z^{\overline{0}} = x^1 \vee y^0 \vee z^1 = x \vee \overline{y} \vee z$, $x^{\overline{1}} \vee y^{\overline{0}} \vee z^{\overline{1}} = x^0 \vee y^1 \vee z^0 = \overline{x} \vee y \vee \overline{z}$.

Таким образом, *СКНФ* такова: $K(x, y, z) = (x \vee \overline{y} \vee z) \wedge (\overline{x} \vee y \vee \overline{z})$.

2. Предыдущую задачу можно решить и без построения таблицы истинности, воспользовавшись основными равносильностями:

$$((x \to y) \wedge z) \vee ((y \to x) \wedge \overline{z}) \equiv ((\overline{x} \vee y) \wedge z) \vee ((\overline{y} \vee x) \wedge \overline{z}) \equiv \{\text{дистрибутивность}\} \equiv$$
$$\equiv ((\overline{x} \vee y) \vee ((\overline{y} \vee x) \wedge \overline{z}))) \wedge (z \vee ((\overline{y} \vee x) \wedge \overline{z}))) \equiv$$
$$\equiv ((\overline{x} \vee y) \vee (\overline{y} \vee x)) \wedge ((\overline{x} \vee y) \vee \overline{z}) \wedge (z \vee (\overline{y} \vee x)) \wedge (z \vee \overline{z}) \equiv$$
$$\equiv \{\overline{x} \vee y \vee \overline{y} \vee x \equiv \mathbf{1},\ z \vee \overline{z} \equiv \mathbf{1}\} \equiv (\overline{x} \vee y \vee \overline{z}) \wedge (x \vee \overline{y} \vee z) - \text{СКНФ}.$$

3. Построим *СДНФ* для формулы примера ***1***.

Выбираем все единичные значения формулы, которым отвечают интерпретации *(0; 0; 0), (1; 0; 0), (1; 1; 0), (0; 0; 1), (0; 1; 1)* и *(1; 1; 1)* соответственно. Строим по этим наборам элементарные конъюнкции $x^0 \wedge y^0 \wedge z^0 = \overline{x} \wedge \overline{y} \wedge \overline{z}$, $x^1 \wedge y^0 \wedge z^0 = x \wedge \overline{y} \wedge \overline{z}$, $x^1 \wedge y^1 \wedge z^0 = x \wedge y \wedge \overline{z}$, $x^0 \wedge y^0 \wedge z^1 = \overline{x} \wedge \overline{y} \wedge z$, $x^0 \wedge y^1 \wedge z^1 = \overline{x} \wedge y \wedge z$ и $x^1 \wedge y^1 \wedge z^1 = x \wedge y \wedge z$. Таким образом, *СДНФ* такова: $(\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge \overline{y} \wedge z) \vee (\overline{x} \wedge y \wedge z) \vee (x \wedge y \wedge z)$.

4. Предыдущую задачу можно решить и без построения таблицы истинности, воспользовавшись основными равносильностями:

$$((x \to y) \wedge z) \vee ((y \to x) \wedge \overline{z}) \equiv ((\overline{x} \vee y) \wedge z) \vee ((\overline{y} \vee x) \wedge \overline{z}) \equiv \{\text{дистрибутивность}\} \equiv (\overline{x} \wedge z) \vee (y \wedge z) \vee (\overline{y} \wedge \overline{z}) \vee (x \wedge \overline{z}) \equiv \{\text{склейка}\} \equiv$$

$$\equiv (\overline{x} \wedge y \wedge z) \vee (\overline{x} \wedge \overline{y} \wedge z) \vee (x \wedge y \wedge z) \vee (\overline{x} \wedge y \wedge z) \vee (x \wedge \overline{y} \wedge \overline{z}) \vee$$

$$\vee (\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge \overline{z}) \equiv \{\text{идемпотентность}\} \equiv$$

$$\equiv (\overline{x} \wedge y \wedge z) \vee (\overline{x} \wedge \overline{y} \wedge z) \vee (x \wedge y \wedge z) \vee (\overline{x} \wedge \overline{y} \wedge \overline{z}) \vee (x \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge \overline{z}).$$

Упражнение. Постройте *СДНФ* и *СКНФ* для следующих формул:

а) $a \vee b \to \overline{b} \wedge \overline{a}$, *б)* $a \leftrightarrow \overline{a}$, *в)* $\overline{a \vee b \wedge c} \to \overline{a \wedge b \vee c}$, *г)* $a \to b \wedge c \leftrightarrow c \wedge \overline{a}$,

д) $\overline{a \wedge b \to a \vee c \to \overline{a \leftrightarrow b \vee c}} \vee a \wedge b \vee \overline{b \to \overline{b \vee c \leftrightarrow a}}$, *е)* $(a \leftrightarrow b) \wedge c \to c \vee \overline{a \leftrightarrow b}$.

Зададимся следующим вопросом: сколько можно выписать подряд попарно неравносильных формул исчисления высказываний от n пропозициональных переменных ? С одной стороны, каждая формула имеет таблицу истинности. С другой стороны, в этом параграфе было доказано, что для каждой таблицы значений существует реализующая её формула исчисления высказываний. Поэтому максимальное количество попарно неравносильных формул равно количеству различных таблиц истинности (при фиксированном порядке перечисления наборов значений переменных в первых n столбцах этих таблиц).

Сколько же существует таблиц истинности ? Если зафиксировать один и тот же порядок перечисления наборов значений переменных в первых n столбцах этих таблиц, то каждая таблица полностью определяется своим последним столбцом, который является набором из нулей и единиц длины 2^n. Всего существует $2^{\left(2^n\right)}$ таких наборов, т.е. всего существует $2^{\left(2^n\right)}$ таблиц истинности, а значит, и $2^{\left(2^n\right)}$ попарно неравносильных формул от n переменных.

Поскольку каждая не тождественно ложная формула имеет однозначно определённую *СДНФ*, общее количество *СДНФ* (с точностью до перестановки их совершенных элементарных конъюнкций) равно $2^{\left(2^n\right)} - 1$. Столько же существует и различных *СКНФ* (с точностью до перестановки их совершенных элементарных дизъюнкций). Значит доказана

Теорема (о количестве неравносильных формул от n переменных). *(1) Максимальное количество попарно неравносильных формул исчисления высказываний от n пропозициональных переменных равно $2^{\left(2^n\right)}$.*

(2) Существует ровно $2^{\left(2^n\right)} - 1$ *неравносильных между собой СДНФ и столько же неравносильных между собой СКНФ.*

§ 6. Булевы функции

После того как каждой формуле $A(x_1, \dots, x_n)$ при любом наборе $x_1 = \varepsilon_1, \dots, x_n = \varepsilon_n$ $(\varepsilon_i \in \{0, 1\},\ 1 \le i \le n)$ значений её пропозициональных переменных приписано единственным образом некоторое значение $A(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}$, такую формулу можно рассматривать как функцию $A : \underbrace{B \times \dots \times B}_{n} \to B$ от n переменных $x_1, \dots, x_n \in B = \{0, 1\}$ со значениями во множестве B. Любая всюду определённая функция $f : \underbrace{B \times \dots \times B}_{n} \to B$ называется *булевой*. Таким образом, каждая формула исчисления высказываний является булевой функцией. При этом две формулы равносильны тогда и только тогда, когда совпадают определяемые ими булевы функции. С другой стороны, произвольная булева функция $f : \underbrace{B \times \dots \times B}_{n} \to B$ может быть задана с помощью таблицы, являющейся (в силу § 5) таблицей истинности некоторой формулы исчисления высказываний. Таким образом, доказана

x_1	…	x_n	$f(x_1, \dots, x_n)$
…	…	…	…
ε_1	…	ε_n	$f(\varepsilon_1, \dots, \varepsilon_n)$
…	…	…	…

Теорема (о реализации булевых функций формулами). *Любая булева функция реализуется формулой исчисления высказываний.*

Эту теорему можно было доказать иначе: подсчитав количество булевых функций от заданного числа переменных и сравнив его с максимальным количеством попарно не равносильных формул исчисления высказываний от тех же переменных. Булевых функций от n переменных $x_1, \dots, x_n$ будет столько же, сколько таблиц вышеприведённого вида, задающих эти функции, т.е. столько же, сколько таблиц истинности от тех же переменных, – а именно – $2^{\left(2^n\right)}$. Это совпадает с максимальным количеством попарно неравносильных формул исчисления высказываний от переменных $x_1, \dots, x_n$. Учитывая, что множество формул содержится во множестве функций, причём две формулы равносильны тогда и только тогда, когда совпадают определяемые ими булевы функции, получим, что булевых функций столько же, каково максимальное число попарно неравносиль-

ных формул исчисления высказываний. Значит, любая булева функция реализуется формулой исчисления высказываний.

Можно перечислить все булевы функции от заданного числа n аргументов. Например, следующие таблицы задают все $2^{(2^2)} = 16$ булевых функций от $n = 2$ аргументов:

x	y	$f_1 = 0$
0	0	0
1	0	0
0	1	0
1	1	0

x	y	$f_2 = x \wedge y$
0	0	0
1	0	0
0	1	0
1	1	1

x	y	$f_3 = \overline{x} \wedge y$
0	0	0
1	0	0
0	1	1
1	1	0

x	y	$f_4 = y$
0	0	0
1	0	0
0	1	1
1	1	1

x	y	$f_5 = x \wedge \overline{y}$
0	0	0
1	0	1
0	1	0
1	1	0

x	y	$f_6 = x$
0	0	0
1	0	1
0	1	0
1	1	1

x	y	$f_7 = x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

x	y	$f_8 = x \vee y$
0	0	0
1	0	1
0	1	1
1	1	1

x	y	$f_9 = \overline{x} \wedge \overline{y}$
0	0	1
1	0	0
0	1	0
1	1	0

x	y	$f_{10} = x \leftrightarrow y$
0	0	1
1	0	0
0	1	0
1	1	1

x	y	$f_{11} = \overline{x}$
0	0	1
1	0	0
0	1	1
1	1	0

x	y	$f_{12} = \overline{x} \vee y$
0	0	1
1	0	0
0	1	1
1	1	1

x	y	$f_{13} = \overline{y}$
0	0	1
1	0	1
0	1	0
1	1	0

x	y	$f_{14} = x \vee \overline{y}$
0	0	1
1	0	1
0	1	0
1	1	1

x	y	$f_{15} = \overline{x} \vee \overline{y}$
0	0	1
1	0	1
0	1	1
1	1	0

x	y	$f_{16} = 1$
0	0	1
1	0	1
0	1	1
1	1	1

Подписанные обозначения функций не единственны: их можно заменить на любые равносильные формулы. Здесь $x \oplus y = (x \wedge \overline{y}) \vee (\overline{x} \wedge y) \equiv \overline{x \leftrightarrow y}$ – операция *"исключающего или"*, называемая также *сложением по модулю 2* (т.к. с точки зрения программиста $x \oplus y = (x+y) \bmod 2$) . Специальные названия есть и у других важных функций. Например, функция f_{15}, подписанная $\overline{x} \vee \overline{y}$, носит название *штрих Шеффера* и обозначается $x \mid y$, а функция f_9 $(\overline{x} \wedge \overline{y})$ – *стрелка Пирса* и обозначается $x \downarrow y$.

Чтобы уяснить связь между булевыми функциями от разного количества аргументов докажем следующую лемму:

Лемма (о разложении булевой функции по k переменным). *Пусть $f: B^n \to B$ – булева функция от n аргументов. Тогда для любого k от 1 до n верна формула:*

$$f(x_1,\dots,x_n)=\bigvee_{(\varepsilon_1;\dots;\varepsilon_k)\in B^k}\left(f(\varepsilon_1,\dots,\varepsilon_k,x_{k+1},\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}\right),$$

где дизъюнкция берётся по <u>*всем*</u> *интерпретациям* $(\varepsilon_1;\dots;\varepsilon_k)\in B^k$.

Доказательство. Рассмотрим формулу $\Phi(x_1,\dots,x_k)=\bigvee_{(\varepsilon_1;\dots;\varepsilon_k)\in B^k}(x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k})$, где дизъюнкция берётся по <u>всем</u> интерпретациям $(\varepsilon_1;\dots;\varepsilon_k)\in B^k$, и проверим, что она тождественно истинна. Действительно, пусть $\varepsilon=(\varepsilon_1;\dots;\varepsilon_k)$ – произвольная интерпретация. Тогда совершенная элементарная конъюнкция $x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}$ от k переменных участвует в $\Phi(x_1,\dots,x_k)$, и по лемме о значениях выражения x^{ε} из прошлого параграфа имеем $(x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k})(\varepsilon_1,\dots,\varepsilon_k)=\varepsilon_1^{\varepsilon_1}\wedge\dots\wedge\varepsilon_k^{\varepsilon_k}=1$, и значит, будучи дизъюнкцией, $\Phi(\varepsilon_1,\dots,\varepsilon_k)=1$. Таким образом, $\Phi(x_1,\dots,x_k)\equiv\mathbf{1}$.

Теперь сразу получаем

$$f(x_1,\dots,x_n)\equiv f(x_1,\dots,x_n)\wedge\Phi(x_1,\dots,x_n)\equiv\bigvee_{(\varepsilon_1;\dots;\varepsilon_k)\in B^k}\left(f(x_1,\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}\right).$$

Остаётся доказать, что $f(x_1,\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}\equiv f(\varepsilon_1,\dots,\varepsilon_k,x_{k+1},\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}$. Для этого вычислим значения левой и правой частей при произвольной интерпретации $(\delta_1;\dots;\delta_n)\in B^n$: $(f(x_1,\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k})(\delta_1,\dots,\delta_n)=f(\delta_1,\dots,\delta_n)\wedge\delta_1^{\varepsilon_1}\wedge\dots\wedge\delta_k^{\varepsilon_k}=$

$$=\begin{cases}f(\varepsilon_1,\dots,\varepsilon_k,\delta_{k+1},\dots,\delta_n)\wedge 1=f(\varepsilon_1,\dots,\varepsilon_k,\delta_{k+1},\dots,\delta_n) & \text{при } \delta_1=\varepsilon_1,\dots,\delta_k=\varepsilon_k\\ f(\delta_1,\dots,\delta_k,\delta_{k+1},\dots,\delta_n)\wedge 0=0 & \text{в противном случае}\end{cases}.$$

Аналогично получим

$$(f(\varepsilon_1,\dots,\varepsilon_k,x_{k+1},\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k})(\delta_1,\dots,\delta_n)=f(\varepsilon_1,\dots,\varepsilon_k,\delta_{k+1},\dots,\delta_n)\wedge\delta_1^{\varepsilon_1}\wedge\dots\wedge\delta_k^{\varepsilon_k}=$$

$$=\begin{cases}f(\varepsilon_1,\dots,\varepsilon_k,\delta_{k+1},\dots,\delta_n)\wedge 1=f(\varepsilon_1,\dots,\varepsilon_k,\delta_{k+1},\dots,\delta_n) & \text{при } \delta_1=\varepsilon_1,\dots,\delta_k=\varepsilon_k\\ f(\varepsilon_1,\dots,\varepsilon_k,\delta_{k+1},\dots,\delta_n)\wedge 0=0 & \text{в противном случае}\end{cases}.$$

Таким образом, $f(x_1,\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}\equiv f(\varepsilon_1,\dots,\varepsilon_k,x_{k+1},\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}$, а значит, $f(x_1,\dots,x_n)=\bigvee_{(\varepsilon_1;\dots;\varepsilon_k)\in B^k}\left(f(\varepsilon_1,\dots,\varepsilon_k,x_{k+1},\dots,x_n)\wedge x_1^{\varepsilon_1}\wedge\dots\wedge x_k^{\varepsilon_k}\right)$.

Лемма доказана.

Эта лемма не только позволяет выражать булевы функции от n переменных через булевы функции от меньшего числа аргументов, но и открывает другой путь к получению *СДНФ*:

Следствие (о СДНФ). *Если* $f(x_1,\dots,x_n)$ *– не тождественно нулевая булева функция, то* $f(x_1,\dots,x_n)=\bigvee_{\substack{(\varepsilon_1;\dots;\varepsilon_n)\in B^n\\ f(\varepsilon_1;\dots;\varepsilon_n)=1}}(x_1^{\varepsilon_1}\wedge\dots\wedge x_n^{\varepsilon_n})$.

Доказательство: Из предыдущей теоремы при $k = n$ получаем разложение:

$$f(x_1, \dots, x_n) = \bigvee_{(\varepsilon_1;\dots;\varepsilon_n) \in B^n} (f(\varepsilon_1, \dots, \varepsilon_n) \wedge x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n}).$$

Если $f(\varepsilon_1, \dots, \varepsilon_n) = 0$, то конъюнкцию $f(\varepsilon_1, \dots, \varepsilon_n) \wedge x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n} \equiv 0$ в этой дизъюнктивной форме можно опустить. Таким образом, в правой части останутся только конъюнкции, в которых $f(\varepsilon_1, \dots, \varepsilon_n) = 1$, т.е. $f(\varepsilon_1, \dots, \varepsilon_n) \wedge x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n} \equiv$ $\equiv x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n}$, что и требовалось.

Следствие доказано.

Теорема о *СДНФ* и *СКНФ* показывает, что любую булеву функцию можно записать, используя только три логических связки: $\overline{\bullet}$ – отрицание, $\wedge$ – конъюнкцию и $\vee$ – дизъюнкцию. На самом деле, используя равносильности $(A \wedge B) \equiv$ $\equiv \overline{(\overline{A} \vee \overline{B})}$, $(A \vee B) \equiv \overline{(\overline{A} \wedge \overline{B})}$, можно обойтись и двумя связками – либо отрицанием и конъюнкцией, либо отрицанием и дизъюнкцией.

Примеры: 1. Записать формулу $x \vee \overline{y} \vee z$, используя только отрицание и конъюнкцию.

$$x \vee \overline{y} \vee z \equiv (x \vee \overline{y}) \vee z \equiv \overline{(\overline{x} \wedge y)} \vee z \equiv \overline{(\overline{x} \wedge y \wedge \overline{z})} = \overline{f_2(f_2(\overline{x}, y), \overline{z})}.$$

2. Записать $\overline{x} \wedge \overline{y} \wedge \overline{z}$, используя только отрицание и дизъюнкцию.

Имеем $\overline{x} \wedge \overline{y} \wedge \overline{z} \equiv \overline{(x \vee y \vee z)} = \overline{f_8(f_8(x, y), z)}$.

3. Функцию $f_1(x, y) = \mathbf{0}$ невозможно выразить, используя только конъюнкцию и дизъюнкцию. Действительно, любая формула $A(x_1, \dots, x_n)$, выразимая через конъюнкцию и дизъюнкцию, принимает значение 1 при $x_1 = \dots = x_n = 1$.

Таким образом, предыдущие примеры показывают, что через некоторые наборы функций можно выразить любую булеву функцию, а через некоторые – нельзя. Это приводит к следующему определению: множество булевых функций $\{f_1, \dots, f_k\}$ называется *полным*, если любую булеву функцию можно выразить через $f_1, \dots, f_k$, используя операцию подстановки значений одних функций и любых пропозициональных переменных в аргументы других функций этого множества (т.е. операцию образования сложных функций от произвольных переменных). Система булевых функций, не являющаяся полной, называется *неполной*.

Теорема (о полных и не полных системах булевых функций). *(1) Следующие системы булевых функций являются полными:* $\{\overline{x}, x \wedge y\}$, $\{\overline{x}, x \vee y\}$, $\{\overline{x}, x \to y\}$, $\{x \mid y\}$, $\{x \downarrow y\}$, $\{x \wedge y, x \oplus y, \mathbf{1}\}$.

(2) Следующие системы булевых функций являются неполными: $\{x \wedge y, x \vee y\}$, $\{\overline{x}, x \leftrightarrow y\}$, $\{x \wedge y, x \oplus y\}$.

Доказательство. Системы функций $\{\overline{x}, x \wedge y\}$, $\{\overline{x}, x \vee y\}$, $\{x \wedge y, x \vee y\}$ были исследованы выше.

Заметим теперь, что для доказательства полноты других систем достаточно выразить через функции этих систем все функции любой полной системы. Действительно, если все функции полной системы C выражаются через функции системы F, то произвольная функция f может быть выражена через функции системы C, а значит, и через функции системы F. Таким образом, система F оказывается полной.

Так для системы $\{\overline{x}, x \to y\}$ имеем $x \wedge y \equiv \overline{\overline{x} \vee \overline{y}} \equiv \overline{x \to \overline{y}}$, т.е. все функции полного множества $\{\overline{x}, x \wedge y\}$ выражаются через функции рассматриваемой системы, которая сама поэтому является полной.

Аналогично для системы $\{x \downarrow y\}$ имеем $x \downarrow y = \overline{x} \wedge \overline{y}$, и $\overline{x} \equiv x \downarrow x$, $x \vee y \equiv \overline{\overline{x} \wedge \overline{y}} \equiv (x \downarrow y) \downarrow (x \downarrow y)$.

Точно так же для системы $\{x \mid y\}$ получаем $x \mid y = \overline{x} \vee \overline{y}$, $\overline{x} \equiv x \mid x$, $x \wedge y \equiv \overline{\overline{x} \vee \overline{y}} \equiv (x \mid y) \mid (x \mid y)$.

Далее, $x \oplus y = (x \wedge \overline{y}) \vee (\overline{x} \wedge y)$, так что $\overline{x} \equiv (x \wedge \mathbf{0}) \vee (\overline{x} \wedge \overline{\mathbf{0}}) \equiv x \oplus \mathbf{1}$, откуда и следует полнота системы функций $\{x \wedge y, x \oplus y, \mathbf{1}\}$.

Неполнота системы $\{\overline{x}, x \leftrightarrow y\}$ доказывается более тонко, чем неполнота системы $\{x \wedge y, x \vee y\}$. Очевидно, что через функции рассматриваемой системы можно выразить $\mathbf{0} \equiv (x \leftrightarrow \overline{x})$, $\mathbf{1} \equiv (x \leftrightarrow x)$, $x \equiv \overline{\overline{x}}$, $y \equiv \overline{\overline{y}}$, $\overline{x}$, $\overline{y}$, $x \leftrightarrow y$, $\overline{x} \leftrightarrow y \equiv \overline{x \leftrightarrow y}$, а больше никаких новых функций не получится. Для проверки последнего утверждения достаточно показать, что выписанная система восьми функций замкнута относительно отрицаний (т.е. для любой из этих восьми функций f отрицание $\overline{f}$ снова будет одной из этих функций) и эквивалентность $f \leftrightarrow g$ любых двух функций этой системы равносильна одной из выписанных восьми функций (проделайте эти проверки самостоятельно !). Таким образом, $x \wedge y$ невозможно выразить через $\overline{x}$, $x \leftrightarrow y$, а значит, эти две функции образуют неполную систему.

Неполнота системы $\{x \wedge y, x \oplus y\}$ следует из того, что обе функции $x \wedge y$, $x \oplus y$ принимают значение 0 при $x = 0 = y$. Поэтому и все функции, выражаю-

щиеся через них обладают этим свойством. Действительно, если булевы функции $f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)$, $f(y_1, \dots, y_k)$ дают значение 0 при нулевых значениях аргументов: $f_i(0, \dots, 0) = 0 = f(0, \dots, 0)$ $(1 \le i \le k)$, то для функции $g(x_1, \dots, x_n) = f(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$ имеем

$$g(0, \dots, 0) = f(f_1(0, \dots, 0), \dots, f_k(0, \dots, 0)) = f(0, \dots, 0) = 0.$$

Таким образом, через функции $x \wedge y$, $x \oplus y$ невозможно выразить, например, $\overline{x}$, т.к. $\overline{x}(0) = 1 \neq 0$.

Теорема доказана полностью.

Отметим без доказательства следующую теорему, полностью решающую вопрос о полноте системы булевых функций:

Теорема (о полноте системы булевых функций). *Для полноты системы булевых функций S необходимо и достаточно, чтобы она целиком не содержалась ни в одном из следующих пяти классов булевых функций:*

1) класс функций, сохраняющих 0: $T_0 = \{f : B^n \to B \mid f(0, \dots, 0) = 0\}$,

2) класс функций, сохраняющих 1: $T_1 = \{f : B^n \to B \mid f(1, \dots, 1) = 1\}$,

3) класс самодвойственных функций:

$$S = \{f : B^n \to B \mid f(x_1, \dots, x_n) = \overline{f(\overline{x_1}, \dots, \overline{x_n})}\},$$

4) класс монотонных функций:

$M = \{f : B^n \to B \mid$ *при* $x_1 \le y_1, \dots, x_n \le y_n$ *верно* $f(x_1, \dots, x_n) \le f(y_1, \dots, y_n)\}$,

5) класс линейных функций:

$$L = \{f : B^n \to B \mid f(x_1, \dots, x_n) = c_1 \wedge x_1 \vee \dots \vee c_n \wedge x_n \vee b \ (c_i, b \in \{0, 1\})\}.$$

Упражнение: Докажите теорему о полных и неполных системах булевых функций, используя теорему о полноте системы булевых функций.

Наряду с обычными логическими связками в теории булевых функций важную роль играет полная система функций $\{x \wedge y, x \oplus y, \mathbf{1}\}$. Это обусловлено тем, что функции выражаются через неё наиболее простым и естественным образом. Для удобства обозначим конъюнкцию $x \wedge y$ через $x \otimes y$. Тогда имеет место следующая

Теорема (о свойствах операций $\otimes$, $\oplus$). *Для любых $x, y, z \in \{0, 1\}$ и формул A, B, C верны следующие свойства:*

(А $\oplus$): $(x \oplus y) \oplus z = x \oplus (y \oplus z)$

$(A \oplus B) \oplus C \equiv A \oplus (B \oplus C)$ *ассоциативность сложения,*

(К $\oplus$): $x \oplus y = y \oplus x$

$A \oplus B \equiv B \oplus A$ — *коммутативность сложения,*

(Н ⊕): $x \oplus 0 = x = 0 \oplus x$

$A \oplus \mathbf{0} \equiv A \equiv \mathbf{0} \oplus A$ — *существование нуля по сложению,*

(О ⊕): $x \oplus x = 0$ — *существование противоположного*

$A \oplus A \equiv \mathbf{0}$ — *элемента по сложению,*

(А⊗): $(x \otimes y) \otimes z = x \otimes (y \otimes z)$

$(A \otimes B) \otimes C \equiv A \otimes (B \otimes C)$ — *ассоциативность умножения,*

(К ⊗): $x \otimes y = y \otimes x$

$A \otimes B \equiv B \otimes A$ — *коммутативность умножения,*

(Н ⊗): $x \otimes 1 = x = 1 \otimes x$ — *существование единицы*

$A \otimes \mathbf{1} \equiv A \equiv \mathbf{1} \otimes A$ — *по умножению,*

(Д ⊕ ⊗): $(x \oplus y) \otimes z = x \otimes z \oplus y \otimes z$

$x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z$ — *дистрибутивность*

$(A \oplus B) \otimes C \equiv A \otimes C \oplus B \otimes C$ — *сложения и умножения.*

$A \otimes (B \oplus C) \equiv A \otimes B \oplus A \otimes C$

Доказательство равенств с переменными x, y, z состоит в простом вычислении. Соответствующие равносильности следуют из доказанных равенств.

Например, проверим свойства дистрибутивности $x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z$. Построим таблицу истинности, доказывающую это равенство.

x	y	z	$y \oplus z$	**л.ч.**	$x \otimes y$	$x \otimes z$	**п.ч.**
0	0	0	0	**0**	0	0	**0**
0	0	1	1	**0**	0	0	**0**
0	1	0	1	**0**	0	0	**0**
0	1	1	0	**0**	0	0	**0**
1	0	0	0	**0**	0	0	**0**
1	0	1	1	**1**	0	1	**1**
1	1	0	1	**1**	1	0	**1**
1	1	1	0	**0**	1	1	**0**

Закон дистрибутивности $A \otimes (B \oplus C) \equiv A \otimes B \oplus A \otimes C$ для формул следует из доказанного равенства с переменными. Действительно, при любой интерпретации $\varepsilon = (\varepsilon_1 ; \dots ; \varepsilon_n)$ для значений $A(\varepsilon)$, $B(\varepsilon)$, $C(\varepsilon)$ этих формул имеем $A(\varepsilon) \otimes (B(\varepsilon) \oplus C(\varepsilon)) \equiv A(\varepsilon) \otimes B(\varepsilon) \oplus A(\varepsilon) \otimes C(\varepsilon)$.

Теорема доказана.

Таким образом, рассматриваемые операции сложения и умножения наиболее естественны с точки зрения обычной арифметики.

Пусть $x_1, \dots, x_n$ – переменные. Назовём выражение вида $x_{i_1} \otimes \dots \otimes x_{i_k}$, где $1 \le i_1 < \dots < i_k \le n$ *мономом от переменных* $x_1, \dots, x_n$ степени k. Специально выделим моном степени 0 – число $\varepsilon \in \{0, 1\}$. Произвольную сумму мономов относительно операции $\oplus$ будем называть *многочленом (полиномом) Жегалкина*

от переменных $x_1, \dots, x_n$. Таким образом, полиномы Жегалкина имеют вид: $p(x_1, \dots, x_n) = \sum\limits_{k=0}^{n}{}^{\oplus} \sum\limits_{1 \le i_1 < \dots < i_k \le n} x_{i_1} \otimes \dots \otimes x_{i_k} \oplus \varepsilon$, где суммы вычисляются относительно операции $\oplus$ и могут, вообще говоря, отсутствовать (например, в случае постоянного полинома $p(x_1, \dots, x_n) = \varepsilon$). Постоянный многочлен Жегалкина $p(x_1, \dots, x_n) = 0$ называется *нулевым*.

Пример. Выпишем все полиномы Жегалкина от двух переменных степени не выше *2*.

степени *0*: $0, 1;$

степени 1: $x,\ y,\ x \oplus 1,\ y \oplus 1,\ x \oplus y,\ x \oplus y \oplus 1;$

степени 2: $x \otimes y,\ x \otimes y \oplus x,\ x \otimes y \oplus y,\ x \otimes y \oplus x \oplus y,\ x \otimes y \oplus 1,\ x \otimes y \oplus x \oplus 1,$
$x \otimes y \oplus y \oplus 1,\ x \otimes y \oplus x \oplus y \oplus 1.$

Получилось *16* полиномов Жегалкина от двух переменных.

Ясно, что любой многочлен Жегалкина является булевой функцией: при любых значениях $x_1 = \varepsilon_1, \dots, x_n = \varepsilon_n$ переменных можно однозначно вычислить значение $p(\varepsilon_1, \dots, \varepsilon_n) = \sum\limits_{k=0}^{n}{}^{\oplus} \sum\limits_{1 \le i_1 < \dots < i_k \le n} \varepsilon_{i_1} \otimes \dots \otimes \varepsilon_{i_k} \oplus \varepsilon$ полинома. Более интересно то, что любая булева функция представима в виде полинома Жегалкина.

Теорема (о полиномах Жегалкина). *Любая булева функция от* n *переменных равна единственному (с точностью до порядка слагаемых-мономов) полиному Жегалкина.*

Доказательство. Существование записи булевой функции в виде полинома Жегалкина следует из полноты системы функций $\{x \oplus y,\ x \otimes y,\ \mathbf{1}\}$: любое выражение, полученное с помощью этих функций, является полиномом Жегалкина.

На самом деле, достаточно уметь записать в виде полиномов Жегалкина, например, все *СДНФ*, т.к. любая булева функция либо тождественно ложна и поэтому равна $\mathbf{1} \oplus \mathbf{1} \equiv \mathbf{0}$, либо равна некоторой *СДНФ*. При записывании *СДНФ* в виде многочлена Жегалкина нужно использовать следующие равносильности: $\overline{a} \equiv a \oplus \mathbf{1},\ a \wedge b = a \otimes b,\ a \vee b \equiv a \oplus b \oplus a \otimes b,\ a \oplus a \equiv \mathbf{0},\ a \otimes a \equiv a$ (проверьте эти формулы, построив таблицы истинности для левых и правых частей).

Примеры: 1. Представить полиномом Жегалкина формулу

$$(\overline{x} \wedge \overline{y}) \vee (x \wedge y) \vee (\overline{x} \wedge y).$$

Для простоты будем использовать привычные знаки: $+$ вместо $\oplus$, и $\cdot$ вместо $\otimes$: $(\overline{x} \wedge \overline{y}) \vee (x \wedge y) \vee (\overline{x} \wedge y) \equiv (\overline{x} \wedge \overline{y}) \vee (\overline{x} \wedge y) \vee (x \wedge y) \equiv$

$$\equiv \overline{x} \vee (x \wedge y) \equiv (x + \mathbf{1}) \vee (x \cdot y) \equiv (x + \mathbf{1}) + (x \cdot y) + (x + \mathbf{1}) \cdot (x \cdot y) \equiv$$

$$\equiv x + (x \cdot y) + \mathbf{1} + x \cdot y + x \cdot y \equiv x \cdot y + x + \mathbf{1}.$$

2. Представить полиномом Жегалкина функцию

$$(x \wedge \overline{y} \wedge z) \vee (\overline{x} \wedge y \wedge \overline{z}) \vee (x \wedge y \wedge z).$$

$$(x \wedge \overline{y} \wedge z) \vee (\overline{x} \wedge y \wedge \overline{z}) \vee (x \wedge y \wedge z) \equiv (x \cdot (y + \mathbf{1}) \cdot z) \vee ((x + \mathbf{1}) \cdot y \cdot (z + \mathbf{1})) \vee (x \cdot y \cdot z) \equiv$$

$$\equiv (x \cdot y \cdot z + x \cdot z) \vee (x \cdot y \cdot z + y \cdot z + x \cdot y + y) \vee (x \cdot y \cdot z) \equiv$$

$$\equiv [(x \cdot y \cdot z + x \cdot z) + (x \cdot y \cdot z + y \cdot z + x \cdot y + y) + (x \cdot y \cdot z + x \cdot z) \cdot (x \cdot y \cdot z + y \cdot z + x \cdot y + y)] \vee (x \cdot y \cdot z) \equiv$$

$$\equiv [x \cdot z + y \cdot z + x \cdot y + y + x \cdot z \cdot (\mathbf{1} + y) \cdot y \cdot (\mathbf{1} + x) \cdot (\mathbf{1} + z)] \vee (x \cdot y \cdot z) \equiv$$

$$\equiv [x \cdot z + y \cdot z + x \cdot y + y + x \cdot z \cdot \mathbf{0} \cdot (1 + x) \cdot (1 + z)] \vee (x \cdot y \cdot z) \equiv$$

$$\equiv [x \cdot z + y \cdot z + x \cdot y + y] \vee (x \cdot y \cdot z) \equiv$$

$$\equiv [x \cdot z + y \cdot z + x \cdot y + y] + x \cdot y \cdot z + [x \cdot z + y \cdot z + x \cdot y + y] \cdot x \cdot y \cdot z \equiv$$

$$\equiv x \cdot y \cdot z + x \cdot z + y \cdot z + x \cdot y + y + [x \cdot y \cdot z + x \cdot y \cdot z + x \cdot y \cdot z + x \cdot y \cdot z] \equiv$$

$$\equiv x \cdot y \cdot z + x \cdot z + y \cdot z + x \cdot y + y.$$

Докажем единственность полинома Жегалкина, представляющего данную функцию. Проверим, что если для двух полиномов Жегалкина $p(x_1, \ldots, x_n)$ и $q(x_1, \ldots, x_n)$ выполняется условие $p(x_1, \ldots, x_n) \equiv q(x_1, \ldots, x_n)$, т.е. значения этих многочленов совпадают при любых наборах значений переменных, то $p(x_1, \ldots, x_n)$ и $q(x_1, \ldots, x_n)$ состоят из одних и тех же мономов. Прибавив к обеим частям этой равносильности $q(x_1, \ldots, x_n)$ и воспользовавшись тождеством $q(x_1, \ldots, x_n) \oplus q(x_1, \ldots, x_n) \equiv \mathbf{0}$, получим $p(x_1, \ldots, x_n) \oplus q(x_1, \ldots, x_n) \equiv \mathbf{0}$. Остаётся только доказать, что многочлен $p(x_1, \ldots, x_n) \oplus q(x_1, \ldots, x_n)$ не содержит ни одного монома.

Таким образом, утверждение о единственности полинома Жегалкина будет доказано, если понять, что в случае $p(x_1, \ldots, x_n) \equiv \mathbf{0}$ многочлен $p(x_1, \ldots, x_n)$ не содержит мономов, т.е. является нулевым многочленом. Это, очевидно, верно для постоянного многочлена $p(x_1, \ldots, x_n) = \varepsilon$. Пусть теперь $p(x_1, \ldots, x_n)$ – полином Жегалкина наименьшей степени, для которого доказываемое свойство не выполнено, т.е. $p(x_1, \ldots, x_n) \equiv \mathbf{0}$, но $p(x_1, \ldots, x_n)$ содержит мономы. Выберем переменную x_i, участвующую в одном из мономов многочлена и вынесем её из всех мономов, зависящих от x_i. Получим

$$p(x_1, \ldots, x_n) = x_i \otimes q(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \oplus r(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n),$$

где полиномы Жегалкина $q(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ и $r(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ не зависят от x_i. Поскольку $p(x_1, \dots, x_n) \equiv \mathbf{0}$, то $p(\varepsilon_1, \dots, \varepsilon_n) = 0$ для любых $x_1 = \varepsilon_1, \dots, x_i = \varepsilon_i, \dots, x_n = \varepsilon_n$. В частности, при $\varepsilon_i = 0$ имеем

$$0 = p(\varepsilon_1, \dots, \varepsilon_{i-1}, 0, \varepsilon_{i+1}, \dots, \varepsilon_n) =$$

$$= 0 \otimes q(\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n) \oplus r(\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n) =$$

$$= r(\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n)$$

для любых значений $x_1 = \varepsilon_1, \dots, x_{i-1} = \varepsilon_{i-1}, x_{i+1} = \varepsilon_{i+1}, \dots, x_n = \varepsilon_n$. Таким образом, получаем аналогичное исходному равенство $r(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \equiv \mathbf{0}$ для полинома Жегалкина меньшей степени, чем $p(x_1, \dots, x_n)$. По предположению, полином $r(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ не содержит мономов, т.е. имеет место равенство $p(x_1, \dots, x_n) = x_i \otimes q(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$. Теперь, аналогично предыдущему, при $\varepsilon_i = 1$ получаем $0 = p(\varepsilon_1, \dots, \varepsilon_{i-1}, 1, \varepsilon_{i+1}, \dots, \varepsilon_n) =$

$$= 1 \otimes q(\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n) = q(\varepsilon_1, \dots, \varepsilon_{i-1}, \varepsilon_{i+1}, \dots, \varepsilon_n).$$

Таким образом, $q(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \equiv \mathbf{0}$ для полинома Жегалкина меньшей степени, чем $p(x_1, \dots, x_n)$. Значит и $q(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ не содержит мономов, а следовательно, их не содержал и многочлен $p(x_1, \dots, x_n)$ – противоречие. Поэтому предположение о том, что $p(x_1, \dots, x_n) \neq 0$ было неверным, и на самом деле полином $p(x_1, \dots, x_n)$ мономов не содержит.

Теорема доказана.

§ 7. Логическое следование

Понятие логического следования является одним из важнейших в математической логике и имеет непосредственное отношение к жизни. Нам часто приходится обосновывать те или иные утверждения: это значит, что на основании нескольких высказываний $a_1, \dots, a_n$ – *посылок*, делается вывод: "следовательно, верно утверждение (*заключение*) a". Такой вывод является корректным в том и только том случае, если из истинности всех посылок следует истинность заключения, т.е. если истинно высказывание "*если* a_1 *и* a_2, *и* … , *и* a_n, *то* a". Это приводит к следующему определению *логического следствия*.

Пусть $A_1, \dots, A_n, A$ – формулы исчисления высказываний от переменных $x_1, \dots, x_k$, $\Gamma = \{A_1, \dots, A_n\}$. Говорят, что *формула* A *является логическим следствием множества формул* Γ *(или просто формул* $A_1, \dots, A_n$*)*, если при любых интерпретациях $\varepsilon = (\varepsilon_1; \dots; \varepsilon_k)$ со свойством $A_1(\varepsilon) = \dots = A_n(\varepsilon) = 1$ выполнено условие $A(\varepsilon) = 1$. В этом случае пишут $A_1, \dots, A_n \models A$ или кратко $\Gamma \models A$. По-

следнее обозначение используется и в случае $\Gamma = \varnothing$: пишут $\models A$, понимая под этим, что A – закон логики.

Примеры: 1. Будет ли $a \to b$ логическим следствием формул $\overline{a}$, b ?

a	b	$\overline{a}$	$a \to b$
0	0	1	1
1	0	0	0
0	1	1	1
1	1	0	1

Построим общую таблицу истинности для формул $\overline{a}$, b, $a \to b$ и проверим выполнение требований определения логического следования. Видно, что в таблице ровно при одной интерпретации $(a = 0, b = 1)$ обе формулы-посылки $\overline{a}$ и b принимают значение 1. При этом значение формулы $a \to b$ также равно 1, т.е. формула $a \to b$ является логическим следствием формул $\overline{a}$ и b.

2. Будет ли формула $a \leftrightarrow b \vee c$ логическим следствием формул $\overline{a}$, $a \to b$, $b \wedge c$?

Аналогично предыдущему, строим таблицу истинности и замечаем, что ровно при одной интерпретации $(a = 0, b = 1 = c)$ все формулы $\overline{a}$, $a \to b$, $b \wedge c$ принимают значение 1. Однако при этой интерпретации формула-заключение $a \leftrightarrow b \vee c$ принимает значение 0, так что она не является логическим следствием формул $\overline{a}$, $a \to b$ и $b \wedge c$.

a	b	c	$\overline{a}$	$a \to b$	$b \wedge c$	$b \vee c$	$a \leftrightarrow b \vee c$
0	0	0	1	1	0	0	1
0	0	1	1	1	0	1	0
0	1	0	1	1	0	1	0
0	1	1	1	1	1	1	0
1	0	0	0	0	0	0	0
1	0	1	0	0	0	1	1
1	1	0	0	1	0	1	1
1	1	1	0	1	1	1	1

Теорема (критерий логического следования). *Для формул $A_1, \dots, A_n$ и A условие $A_1, \dots, A_n \models A$ выполнено тогда и только тогда, когда формула $(A_1 \wedge \dots \wedge A_n) \to A$ является законом логики.*

Доказательство. Пусть выполнено $A_1, \dots, A_n \models A$. Докажем, что формула $(A_1 \wedge \dots \wedge A_n \to A)$ – закон логики. При каких интерпретациях $\varepsilon = (\varepsilon_1 ; \dots ; \varepsilon_k)$ рассматриваемая формула может быть ложна ? Только при тех, для которых верно $(A_1 \wedge \dots \wedge A_n)(\varepsilon) = 1$, но $A(\varepsilon) = 0$. Это значит, что $A_1(\varepsilon) = \dots = A_n(\varepsilon) = 1$, но $A(\varepsilon) = 0$ – противоречие с условием $A_1, \dots, A_n \models A$. Поэтому рассматриваемая формула $(A_1 \wedge \dots \wedge A_n \to A)$ не может принимать значения 0, т.е. является законом логики, что и требовалось.

Пусть теперь $(A_1 \wedge \dots \wedge A_n \to A)$ – закон логики. Рассмотрим любую интерпретацию $\varepsilon = (\varepsilon_1 ; \dots ; \varepsilon_k)$ со свойством $A_1(\varepsilon) = \dots = A_n(\varepsilon) = 1$. Тогда

$1 = (A_1 \wedge \ldots \wedge A_n \to A)(\varepsilon) = (A_1(\varepsilon) \wedge \ldots \wedge A_n(\varepsilon) \to A(\varepsilon)) = (1 \to A(\varepsilon))$,

и по аксиоме вычисления импликации $A(\varepsilon) = 1$. Таким образом, $A_1, \ldots, A_n \models A$.

Теорема доказана.

Теорема (о дедукции). *Для любого множества формул Γ и формул A, B условие $\Gamma, A \models B$ выполнено тогда и только тогда, когда $\Gamma \models A \to B$.*

Доказательство. Условие $\Gamma, A \models B$, где $\Gamma = \{A_1, \ldots, A_n\}$ $(n \geq 0)$, имеет место (по доказанной выше теореме) в случае, когда $(A_1 \wedge \ldots \wedge A_n \wedge A \to B)$ – закон логики. Имеем $((A_1 \wedge \ldots \wedge A_n \wedge A \to B) \equiv 1) \Leftrightarrow ((\overline{A_1 \wedge \ldots \wedge A_n \wedge A} \vee B) \equiv 1) \Leftrightarrow$ $\Leftrightarrow$ {*де Морган*} $\Leftrightarrow ((\overline{A_1 \wedge \ldots \wedge A_n} \vee \overline{A} \vee B) \equiv 1) \Leftrightarrow ((\overline{A_1 \wedge \ldots \wedge A_n} \vee (A \to B)) \equiv 1) \Leftrightarrow$ $\Leftrightarrow ((A_1 \wedge \ldots \wedge A_n \to (A \to B)) \equiv 1)$. Таким образом, $(A_1 \wedge \ldots \wedge A_n \wedge A \to B)$ – закон логики тогда и только тогда, когда законом логики является формула $(A_1 \wedge \ldots \wedge A_n \to (A \to B))$, а это (по критерию логического следования) и означает, что $\Gamma, A \models B$ имеет место тогда и только тогда, когда $\Gamma \models A \to B$.

Теорема доказана.

В течение тысячелетий человечеством накоплен опыт построения правильных выводов. Соответствующие правила на математическом языке обычно записывают так: $\frac{\mathcal{A}_1, \ldots, \mathcal{A}_n}{\mathcal{A}}$, где $\mathcal{A}_1, \ldots, \mathcal{A}_n$ – *посылки*, а $\mathcal{A}$ – *заключение*. Такое правило означает, что из справедливости посылок $\mathcal{A}_1, \ldots, \mathcal{A}_n$ логически следует справедливость заключения $\mathcal{A}$. На самом деле правила (логического) вывода представляют из зебя *схемы правил*: они зависят от переменных-параметров, вместо которых можно подставлять любые формулы исчисления высказываний. Эти параметры будем выделять курсивом.

Пример. Правило *modus ponens* – "мост ослов": $\frac{\mathcal{A},\ \mathcal{A} \to \mathcal{B}}{\mathcal{B}}$ [2].

Здесь $\mathcal{A}$, $\mathcal{B}$ – любые формулы языка исчисления высказываний. Докажем это правило. Для этого проверим, что $\mathcal{A}, \mathcal{A} \to \mathcal{B} \models \mathcal{B}$. Имеем $(\mathcal{A}, \mathcal{A} \to \mathcal{B} \models \mathcal{B}) \Leftrightarrow$ $\Leftrightarrow$ $(\mathcal{A} \to \mathcal{B},\ \mathcal{A} \models \mathcal{B}) \Leftrightarrow (\mathcal{A} \to \mathcal{B} \models \mathcal{A} \to \mathcal{B}) \Leftrightarrow (((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{B})) \equiv 1)$, что справедливо.

Знак $\Leftrightarrow$ здесь, как обычно, следует понимать как синоним выражения "*тогда и только тогда, когда*".

[2] Древние считали, что это правило отделяет "ослов" – не понимающих логики – от нормальных людей: тот, кто освоил это правило уже перешёл по мосту из разряда "ослов" в разряд нормальных людей.

Теорема (об основных правилах логического вывода). *Справедливы следующие основные правила логического вывода:*

$\dfrac{\Gamma \models \mathcal{A};\ \Gamma \models \mathcal{A}\to\mathcal{B}}{\Gamma \models \mathcal{B}}$ – расширение *modus ponens*, $\dfrac{\Gamma,\mathcal{A}\models\mathcal{B}}{\Gamma\models\mathcal{A}\to\mathcal{B}}$, $\dfrac{\Gamma\models\mathcal{A}\to\mathcal{B}}{\Gamma,\mathcal{A}\models\mathcal{B}}$ – *правила дедукции*, $\dfrac{\Gamma\models\mathcal{B}}{\Gamma,\mathcal{A}\models\mathcal{B}}$ – *правило расширения посылок*, $\dfrac{\Gamma\models\mathcal{A}\to(\mathcal{B}\to C)}{\Gamma\models\mathcal{B}\to(\mathcal{A}\to C)}$ – *правило перестановки посылок*, $\dfrac{\Gamma\models\mathcal{A}\to(\mathcal{B}\to C)}{\Gamma\models\mathcal{A}\wedge\mathcal{B}\to C}$, $\dfrac{\Gamma\models\mathcal{A}\wedge\mathcal{B}\to C}{\Gamma\models\mathcal{A}\to(\mathcal{B}\to C)}$ – *правила объединения и разделения посылок*, $\dfrac{\Gamma\models\mathcal{A}\wedge\mathcal{B}}{\Gamma\models\mathcal{A}}$, $\dfrac{\Gamma\models\mathcal{A}\wedge\mathcal{B}}{\Gamma\models\mathcal{B}}$ – *правила удаления конъюнкции*, $\dfrac{\Gamma\models\mathcal{A}}{\Gamma\models\mathcal{A}\vee\mathcal{B}}$, $\dfrac{\Gamma\models\mathcal{B}}{\Gamma\models\mathcal{A}\vee\mathcal{B}}$ – *правила введения дизъюнкции*, $\dfrac{\Gamma\models\mathcal{A};\ \Gamma\models\mathcal{B}}{\Gamma\models\mathcal{A}\wedge\mathcal{B}}$ – *правило введения конъюнкции*, $\dfrac{\Gamma\models\mathcal{B};\ \mathcal{B}\models C}{\Gamma\models C}$, $\dfrac{\Gamma,\mathcal{A}\models\mathcal{B};\ \Gamma,\mathcal{B}\models C}{\Gamma,\mathcal{A}\models C}$ – *правила силлогизма*, $\dfrac{\Gamma,\mathcal{A}\models\mathcal{B};\ \Gamma\models\overline{\mathcal{B}}}{\Gamma\models\overline{\mathcal{A}}}$ – *modus tollens*[3], $\dfrac{\Gamma,\mathcal{A}\models\mathcal{B};\ \Gamma,\mathcal{A}\models\overline{\mathcal{B}}}{\Gamma\models\overline{\mathcal{A}}}$ – *правило опровержения*, $\dfrac{\Gamma,\mathcal{A}\models\mathcal{B}}{\Gamma,\overline{\mathcal{B}}\models\overline{\mathcal{A}}}$ – *правило контрапозиции*, $\dfrac{\Gamma\models\mathcal{A}\vee\mathcal{B};\ \Gamma\models C\vee\overline{\mathcal{B}}}{\Gamma\models\mathcal{A}\vee C}$ – *правило резолюций.*

Доказательство. Правила расширение *modus ponens* доказывается аналогично его основному варианту. Правило дедукции уже доказано в теореме о дедукции. Остальные правила доказываются примерно так же.

Правило расширения посылок $\dfrac{\Gamma\models\mathcal{B}}{\Gamma,\mathcal{A}\models\mathcal{B}}$. Действительно, условие $\Gamma\models\mathcal{B}$ означает, что формула $\mathcal{B}$ принимает значение *1* на всех наборах значений переменных, при которых все формулы из Γ имеют значения *1*. Значит $\mathcal{B}$ принимает значение *1* и на всех наборах значений переменных, при которых имеют значения *1* формула $\mathcal{A}$ и все формулы из Γ, т.е. $\Gamma,\mathcal{A}\models\mathcal{B}$, что и требовалось доказать.

Правило перестановки посылок: $\dfrac{\Gamma\models\mathcal{A}\to(\mathcal{B}\to C)}{\Gamma\models\mathcal{B}\to(\mathcal{A}\to C)}$. Дано $\Gamma\models\mathcal{A}\to(\mathcal{B}\to C)$, т.е. (по теореме о дедукции) $\Gamma,\ \mathcal{A}\models\mathcal{B}\to C$ или $\Gamma,\mathcal{A},\mathcal{B}\models C$, что равносильно утверждению $\Gamma,\mathcal{B},\mathcal{A}\models C$. По теореме о дедукции, получим $\Gamma,\ \mathcal{B}\models\mathcal{A}\to C$, и далее $\Gamma\models\mathcal{B}\to(\mathcal{A}\to C)$, что и требовалось.

[3] Буду благодарен тому, кто сообщит, что бы это значило (*мера терпения* ?!).

Правило объединения и разделения посылок $\dfrac{\Gamma \models \mathcal{A} \to (\mathcal{B} \to C)}{\Gamma \models \mathcal{A} \wedge \mathcal{B} \to C}$, $\dfrac{\Gamma \models \mathcal{A} \wedge \mathcal{B} \to C}{\Gamma \models \mathcal{A} \to (\mathcal{B} \to C)}$.

Можно рассудить иначе, чем раньше: нетрудно заметить, что $\mathcal{A} \to (\mathcal{B} \to C) \equiv$ $\equiv (\mathcal{A} \wedge \mathcal{B}) \to C$. Поэтому если любая из этих формул истинна при любых значениях пропозициональных переменных, при которых истинны все формулы множества Γ, то это же верно и для второй формулы. Таким способом можно доказать и предыдущее правило вывода.

Правила удаления конъюнкции $\dfrac{\Gamma \models \mathcal{A} \wedge \mathcal{B}}{\Gamma \models \mathcal{A}}$, $\dfrac{\Gamma \models \mathcal{A} \wedge \mathcal{B}}{\Gamma \models \mathcal{B}}$. Если при любых значениях пропозициональных переменных, при которых истинны все формулы множества Γ, истинна формула $\mathcal{A} \wedge \mathcal{B}$, то это верно и для формул $\mathcal{A}$ и $\mathcal{B}$.

Правила введения дизъюнкции $\dfrac{\Gamma \models \mathcal{A}}{\Gamma \models \mathcal{A} \vee \mathcal{B}}$, $\dfrac{\Gamma \models \mathcal{B}}{\Gamma \models \mathcal{A} \vee \mathcal{B}}$ и *введения конъюнкции* $\dfrac{\Gamma \models \mathcal{A};\ \Gamma \models \mathcal{B}}{\Gamma \models \mathcal{A} \wedge \mathcal{B}}$ докажите самостоятельно.

Правила силлогизма: $\dfrac{\Gamma \models \mathcal{B};\ \mathcal{B} \models C}{\Gamma \models C}$, $\dfrac{\Gamma, \mathcal{A} \models \mathcal{B};\ \Gamma, \mathcal{B} \models C}{\Gamma, \mathcal{A} \models C}$. Первое из правил следует из того, что если $\Gamma \models \mathcal{B}$ и $(\mathcal{B} \to C)$ – закон логики, то при любых наборах значений пропозициональных переменных, при которых истинны все формулы из множества Γ, истинны $\mathcal{B}$ и $\mathcal{B} \to C$, а значит и C, что и требовалось.

Второе правило можно вывести так: если $\Gamma, \mathcal{A} \models \mathcal{B}$ и $\Gamma, \mathcal{B} \models C$, то (по теореме о дедукции) $\Gamma \models \mathcal{A} \to \mathcal{B}$ и $\Gamma \models \mathcal{B} \to C$, и по правилу введения конъюнкции верно $\Gamma \models (\mathcal{A} \to \mathcal{B}) \wedge (\mathcal{B} \to C)$. Закон логики $(\mathcal{A} \to \mathcal{B}) \wedge (\mathcal{B} \to C) \to (\mathcal{A} \to C)$ позволяет по первому правилу силлогизма (?!) получить $\Gamma \models \mathcal{A} \to C$, а значит, $\Gamma, \mathcal{A} \models C$ по теореме о дедукции, что и требовалось.

Правило modus tollens $\dfrac{\Gamma, \mathcal{A} \models \mathcal{B};\ \Gamma \models \overline{\mathcal{B}}}{\Gamma \models \overline{\mathcal{A}}}$. Действительно, из $\Gamma \models \mathcal{A} \to \mathcal{B}$ и $\Gamma \models \overline{\mathcal{B}}$ по правилу введения конъюнкции следует $\Gamma \models (\mathcal{A} \to \mathcal{B}) \wedge \overline{\mathcal{B}}$. Учитывая закон логики $(\mathcal{A} \to \mathcal{B}) \wedge \overline{\mathcal{B}} \to \overline{\mathcal{A}}$, по первому правилу силлогизма получаем (?!) $\Gamma \models \overline{\mathcal{A}}$, что и требовалось.

Правило опровержения $\dfrac{\Gamma, \mathcal{A} \models \mathcal{B};\ \Gamma, \mathcal{A} \models \overline{\mathcal{B}}}{\Gamma \models \overline{\mathcal{A}}}$ можно вывести из $\Gamma \models \mathcal{A} \to \mathcal{B}$, $\Gamma \models \mathcal{A} \to \overline{\mathcal{B}}$ и равносильности $(\mathcal{A} \to \mathcal{B}) \wedge (\mathcal{A} \to \overline{\mathcal{B}}) \equiv \overline{\mathcal{A}}$ (восстановите детали самостоятельно).

Правило контрапозиции $\dfrac{\Gamma, \mathcal{A} \models \mathcal{B}}{\Gamma, \overline{\mathcal{B}} \models \overline{\mathcal{A}}}$ следует из $\Gamma \models \mathcal{A} \to \mathcal{B}$, теоремы о дедукции и закона контрапозиции.

Правило резолюций $\dfrac{\Gamma \models \mathcal{A} \vee \mathcal{B};\ \ \Gamma \models C \vee \overline{\mathcal{B}}}{\Gamma \models \mathcal{A} \vee C}$: если оно не верно, то для некоторой интерпретации $x_1 = \varepsilon_1, \ldots, x_n = \varepsilon_n$, при которой все формулы из Γ имеют значение 1, будет $\mathcal{A}(\varepsilon) = 0 = C(\varepsilon)$, что немедленно ведёт к противоречию: $\mathcal{B}(\varepsilon) = (\mathcal{A}(\varepsilon) \vee \mathcal{B}(\varepsilon)) = 1 = (C(\varepsilon) \vee \overline{\mathcal{B}}\,(\varepsilon)) = \overline{\mathcal{B}}\,(\varepsilon)$.

Теорема доказана.

Упражнение: Докажите все правила логического вывода при $\Gamma = \varnothing$.

§ 8. Некоторые применения алгебры высказываний

I. Анализ логических рассуждений. Рассмотрим несколько примеров, которые используют понятие логического следования.

Примеры: 1. Правильно ли следующее логическое рассуждение: *"Когда выпадает снег, птицы улетают на юг. Если птицы улетели на юг, то скоро наступит зима. Зима наступила. Следовательно, либо выпал снег, либо птицы улетели на юг"*.

a	b	c	$a \to b$	$b \to c$	$b \vee a$
0	0	0	1	1	0
0	0	1	1	1	**0**
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	1	1
1	0	1	0	1	1
1	1	0	1	0	1
1	1	1	1	1	1

Обозначим элементарные высказывания буквами: a := *"Выпал снег"*, b := *"Птицы улетели на юг"*, c := *"Наступила зима"*. Тогда получим *схему рассуждения*: $a \to b,\ b \to c,\ c \models b \vee a$. Проверим, так ли это, по таблице истинности. Как видно из таблицы, формула $b \vee a$ не является логическим следствием формул $a \to b,\ b \to c,\ c$: именно, она ложна при $a = 0 = b,\ c = 1$, когда все посылки рассматриваемого логического следования истинны. Другими словами, в ситуации, когда зима наступила, но снег не выпал и птицы не улетели на юг, приведённый вывод не корректен.

2. Оцените правильность логического вывода: *"Если* $a < b$, *то* $b - a > 0$. *Если* $a \geq b$, *то* $a - b \geq 0$. *Либо* $a < b$, *либо* $a - b \geq 0$. *Следовательно, либо неверно, что* $a - b < 0$, *либо неверно, что* $b - a \leq 0$*"*.

Обозначая элементарные высказывания буквами, получим: $x :=$ "$a < b$", $y :=$ "$b - a > 0$", $z :=$ "$a \geq b$", $t :=$ "$a - b \geq 0$". Тогда $\overline{t}$ = "$a - b < 0$", $\overline{y}$ = "$b - a \leq 0$", и нужно схема рассуждения $x \to y,\ z \to t,\ x \vee t \models \overline{t} \vee \overline{y}$, т.е. $x \to y,\ z \to t,\ x \vee t \models t \vee y$. Формула $t \vee y$ ложна только при $t = 0 = y$, но при этих значениях все три формулы $x \to y,\ z \to t,\ x \vee t$ не могут быть одновременно истинны: для формулы $x \vee t$ условие истинности при $t = 0$ означает $x = 1$, что влечёт ложность значения формулы $x \to y$. Итак, заключение не может быть ложным при истинности всех посылок, т.е. рассуждение правильное.

Замечание: С точки зрения математики в целом все посылки и заключение в исследованном рассуждении истинны.

3. Оцените правильность логического вывода: *"Если число, составленное из двух младших цифр числа чётно, то само число делится на 2. Если сумма всех цифр числа делится на 3, то само число делится на 3. Сумма цифр трёхзначного числа равна 27. Число 27 делится на 3. Значит, это трёхзначное число не делится на 2"*.

Аналогично предыдущему, $a :=$ *"число, составленное из двух младших цифр числа n чётно"*, $b :=$ *"число n делится на 2"*, $c :=$ *"сумма всех цифр числа n делится на 3"*, $d :=$ *"число n делится на 3"*, $e :=$ *"число n трёхзначно"*, $f :=$ *"сумма цифр числа n равна 27"*, $g :=$ *"27 делится на 3"*.

Исследуем логическое следование $a \to b,\ c \to d,\ e \wedge f,\ g \models e \wedge \overline{b}$. Очевидно, что в таком общем виде оно не имеет места (?!), хотя рассматриваемое рассуждение верно с общематематической точки зрения: если при сформулированных условиях $\overline{xyz} \ \vdots\ 2$, то цифра z чётна, и $x + y + z = 27$ влечёт $x = y = z = 9$ – противоречие.

Однако, **с точки зрения логики, в этом верном математическом рассуждении есть пробелы**: заключение невозможно вывести из сформулированных посылок, используя только правила логического вывода – мы привлекли для обоснования заключения арифметическое свойство трёхзначных чисел. Этот пример показывает, что **математика не сводится к логике**, хотя и не может без неё обойтись. Придумайте более простые примеры, иллюстрирующие этот вывод.

II. Оптимизация логики условных переходов в программах. В сложных программах может использоваться много логических переменных, которые, причудливо сплетаясь и нагромождаясь друг на друга в условных операторах, способны запутать даже опытного программиста.

Примеры. 1. Следующий фрагмент программы чудовищен:

```
if (not(a and b) or (a and b)) then
   P
else
  if (not(a or b) and not(b)) then
     Q
  else
     R;
```

Действительно, стоит только упростить логическое выражение

$$\overline{a \wedge b} \vee (a \wedge b) \equiv \overline{a} \vee \overline{b} \vee (a \wedge b) \equiv (\overline{a} \vee (a \wedge b)) \vee \overline{b} \equiv$$

$$\equiv ((\overline{a} \vee a) \wedge (\overline{a} \vee b)) \vee \overline{b} \equiv (\mathbf{1} \wedge (\overline{a} \vee b)) \vee \overline{b} \equiv \overline{a} \vee (b \vee \overline{b}) \equiv \overline{a} \vee \mathbf{1} \equiv \mathbf{1},$$

как выяснится, что никаких условных операторов вообще не нужно: приведённый фрагмент программы равносилен просто выполнению группы операторов P.

2. Не лучше и такой фрагмент:

```
if (not(a and b) or (not(a or c) and not(b) and  c)) then
   P
else
   if (not(a or b) and not(b or c)) then
      Q
   else
      R;
```

Первое условие – для группы операторов P – оптимизируется так:

$$\overline{a \wedge b} \vee (\overline{a \vee c} \wedge \overline{b} \wedge c) \equiv \overline{a} \vee \overline{b} \vee (\overline{a} \wedge \overline{c} \wedge \overline{b} \wedge c) \equiv$$

$$\equiv \overline{a} \vee \overline{b} \vee (\overline{b} \wedge \overline{a} \wedge \overline{c} \wedge c) \equiv \overline{a} \vee \overline{b} \equiv \overline{a \wedge b}.$$

Условие для группы операторов Q таково:

$$\overline{\overline{a \wedge b}} \wedge \overline{a \vee b} \wedge \overline{b \vee c} \equiv a \wedge b \wedge \overline{a \vee b} \wedge \overline{b \vee c} \equiv a \wedge b \wedge \overline{a} \wedge \overline{b} \wedge \overline{b \vee c} \equiv \mathbf{0},$$

так что операторы группы Q не выполняются никогда, а условие для группы операторов R принимает вид $a \wedge b$. Поэтому весь рассматриваемый фрагмент программы равносилен такому:

```
if not(a and b) then
   P
else
   R;
```

Однако его лучше (?!) переписать следующим образом:

```
if (a and b) then
   R
else
   P;
```

Упражнения: 1. Почему в программах лучше писать *not(a and b)*, нежели *not(a) or not(b)*, хотя по закону де Моргана эти операторы равносильны ?

2. Оптимизируйте фрагмент программы:

```
if (not(a or b and c) or not(b or c)) then
   P
else
   if (b and not(a and c)) then
      Q
   else
      R;
```

3. Приведите ещё пару-тройку логических несуразностей из собственных программ.

III. Автоматизированный логический вывод формул. Пусть заданы формулы $A_1, \dots, A_n, A$ от некоторого набора пропозициональных переменных и нужно понять, верно ли, что $A_1, \dots, A_n \models A$. Оказывается, что для машинной проверки удобно использовать *правило резолюций* в виде $\dfrac{\mathcal{B} \vee \mathcal{A};\ C \vee \overline{\mathcal{A}}}{\mathcal{B} \vee C}$ или в терминах логического следования $\mathcal{A} \vee \mathcal{B},\ \overline{\mathcal{A}} \vee C \models \mathcal{B} \vee C$.

Привычное человеку правило *modus ponens* является частным случаем этого правила резолюций при $\mathcal{B} \equiv \mathbf{0}$: ввиду $\mathcal{A} \vee \mathcal{B} \equiv \mathcal{A}$, $\overline{\mathcal{A}} \vee C \equiv \mathcal{A} \to C$, $\mathcal{B} \vee C \equiv C$ правило резолюций принимает знакомый вид $\dfrac{\mathcal{A},\ \mathcal{A} \to C}{C}$ – *modus ponens*.

Как было доказано, логическое следование $A_1, \dots, A_n \models A$ имеет место тогда и только тогда, когда $(A_1 \wedge \dots \wedge A_n \to A) \equiv \mathbf{1}$. Удобнее перейти к отрицаниям:

$$\mathbf{0} \equiv \overline{A_1 \wedge \dots \wedge A_n \to A} \equiv \overline{\overline{A_1 \wedge \dots \wedge A_n} \vee A} \equiv \overline{\overline{A_1 \wedge \dots \wedge A_n} \wedge \overline{A}} \equiv A_1 \wedge \dots \wedge A_n \wedge \overline{A}.$$

Значит нужно понять, что $A_1 \wedge \dots \wedge A_n \wedge \overline{A} \equiv \mathbf{0}$, т.е. $A_1 \wedge \dots \wedge A_n \wedge \overline{A} \equiv \Phi \wedge \overline{\Phi}$ для некоторой формулы Φ, т.е. $A_1, \dots, A_n, \overline{A} \models \Phi \wedge \overline{\Phi}$ (этого достаточно ?!).

Запишем посылки $A_1, \dots, A_n, \overline{A}$ в *КНФ* и обозначим множество всех элементарных дизъюнкций, участвующих в этих *КНФ* через $\Delta = \{D_1, \dots, D_m\}$. Тогда каждая посылка, будучи конъюнкцией некоторых элементов множества Δ, является логическим следствием множества формул Δ (по правилу введения конъюнкции), т.е. $\Delta \models A_1, \dots, \Delta \models A_n, \Delta \models \overline{A}$. Поэтому $\Delta \models A_1 \wedge \dots \wedge A_n \wedge \overline{A}$ и $\Delta \models \Phi \wedge \overline{\Phi}$. Обратно, если $\Delta \models \Phi \wedge \overline{\Phi}$, то $D_1 \wedge \dots \wedge D_m \to \Phi \wedge \overline{\Phi}$ – закон логики, причём $D_1 \wedge \dots \wedge D_m \equiv A_1 \wedge \dots \wedge A_n \wedge \overline{A}$, т.к. каждая формула в правой части является конъюнкцией некоторых элементарных дизъюнкций из левой части, а каждая дизъюнкция из левой части встречается в одной из формул правой части. Итак, задача о проверке следования $A_1, \dots, A_n, \overline{A} \models \Phi \wedge \overline{\Phi}$ сводит-

ся к проверке следования $\Delta \models \Phi \wedge \overline{\Phi}$ для заданного конечного множества Δ элементарных дизъюнкций.

Возникшую редуцированную задачу будем решать *методом резолюций*, который можно описать так:

- перебираем дизъюнкции из множества Δ, пока не найдём пару вида $D_i = x_1^{\varepsilon_1} \vee ... \vee x_{k-1}^{\varepsilon_{k-1}} \vee x_k^{\varepsilon_k} \vee x_{k+1}^{\varepsilon_{k+1}} \vee ... \vee x_s^{\varepsilon_s}$, $D_j = x_1^{\delta_1} \vee ... \vee x_{k-1}^{\delta_{k-1}} \vee x_k^{\overline{\varepsilon_k}} \vee x_{k+1}^{\delta_{k+1}} \vee ... \vee x_s^{\delta_s}$, где ε_λ, $\delta_\mu \in \{0, 1, \varnothing\}$ $(1 \le \begin{matrix}\lambda \\ \mu\end{matrix} \le s)$, а запись $x_\lambda^{\varnothing}$ означает, что переменная x_λ не участвует в соответствующей дизъюнкции. Таким образом, в D_i и D_j переменная x_k (для некоторого k) встречается в одной дизъюнкции с отрицанием, а в другой – без отрицания.
- к этой паре применяем правило резолюций: если обозначить

  $$d_i = x_1^{\varepsilon_1} \vee ... \vee x_{k-1}^{\varepsilon_{k-1}} \vee x_{k+1}^{\varepsilon_{k+1}} \vee ... \vee x_s^{\varepsilon_s}, \quad d_j = x_1^{\delta_1} \vee ... \vee x_{k-1}^{\delta_{k-1}} \vee x_{k+1}^{\delta_{k+1}} \vee ... \vee x_s^{\delta_s},$$

  то $x_k^{\varepsilon_k} \vee d_i$; $x_k^{\overline{\varepsilon_k}} \vee d_j \models d_i \vee d_j$, причём $x_k^{\varepsilon_k} \vee d_i \equiv D_i$, $x_k^{\overline{\varepsilon_k}} \vee d_j \equiv D_j$, т.е. дизъюнкция $d_i \vee d_j$ будет логическим следствием формул D_i, D_j, а значит и следствием множества Δ.

  Возможен случай, когда $x_k^{\varepsilon_k} = D_i$, $x_k^{\overline{\varepsilon_k}} = D_j$, т.е. дизъюнкции d_i и d_j пустые. Тогда очевидно, что $\Delta \models x_k \wedge \overline{x_k}$, т.е. можно взять $\Phi = x_k$.

  Если же $d_i \vee d_j \equiv \mathbf{1}$, то рассматриваемое следствие тривиально и такую резолюцию можно не делать. Так будет, например, когда $\varepsilon_\lambda = \overline{\delta_\lambda} \in \{0, 1\}$. ***Таким образом, можно ограничиться рассмотрением дизъюнкций D_i и D_j, в которых x_k – единственная переменная, встречающаяся в одной из них с отрицанием, а в другой – без отрицания.*** Это ограничение существенно сокращает перебор возможных резолюций.
- расширяем множество Δ до Δ', присоединяя к Δ все дизъюнкции $\partial_1, \dots, \partial_m$ из *КНФ* для $d_i \vee d_j$: $\Delta' = \Delta \cup \{\partial_1, \dots, \partial_m\}$, $d_i \vee d_j \equiv \partial_1 \wedge \dots \wedge \partial_m$. Теперь $\Delta \models \Phi \wedge \overline{\Phi}$ тогда и только тогда, когда $\Delta' \models \Phi \wedge \overline{\Phi}$. Действительно, если противоречие $\Phi \wedge \overline{\Phi}$ следует из множества Δ, то оно следует и из большего множества Δ'. Если же это противоречие следует из множества Δ', то оно следует и из Δ, т.к. каждый элемент Δ' является логическим следствием множества Δ.
- процесс построения резолюций можно ещё более сократить, если учесть, что

при появлении во множестве Δ' двух дизъюнкций вида $Д$ и $Д \vee D$ можно оставить только одну из них – более короткую $Д$, т.к. $Д \models Д \vee D$.

Описанный алгоритм последовательного расширения множества Δ называется *замыканием этого множества относительно резолюций*. На некотором шаге ввиду конечности числа всех дизъюнкций (от фиксированного конечного числа переменных) либо получится вывод искомого противоречия $\Delta \models x_k \wedge \overline{x_k}$, либо множество дизъюнкций, *замкнутое относительно резолюций*, т.е. такое множество, которое описанный выше процесс не расширяет: дизъюнкций D_i, D_j описанного выше вида в нём нет. В первом случае получим $A_1, \ldots, A_n \models A$ для исходных формул, а во втором формула A не является логическим следствием формул $A_1, \ldots, A_n$.

Примеры: 1. Проверить, следует ли формула $A = y$ из

$$A_1 = (x \vee y \vee \overline{z}) \wedge (\overline{x} \vee y \vee z),\ A_2 = (x \vee \overline{y} \vee \overline{z}) \wedge (\overline{x} \vee \overline{y} \vee z).$$

Имеем $\overline{A} = \overline{y}$, $\Delta = \{x \vee y \vee \overline{z},\ \overline{x} \vee y \vee z,\ x \vee \overline{y} \vee \overline{z},\ \overline{x} \vee \overline{y} \vee z,\ \overline{y}\}$. Из этого множества сразу можно удалить все дизъюнкции, строго содержащие $\overline{y}$ (они следуют из $\overline{y}$). Таким образом, $\Delta = \{ x \vee y \vee \overline{z},\ \overline{x} \vee y \vee z,\ \overline{y}\}$.

Процесс замыкания относительно резолюций таков:

- $x \vee \mathbf{y} \vee \overline{z},\ \overline{\mathbf{y}} \models x \vee \overline{z}$, и $\Delta' = \{ x \vee y \vee \overline{z},\ \overline{x} \vee y \vee z,\ \overline{y},\ x \vee \overline{z}\}$.

Из этого множества можно удалить все дизъюнкции, строго содержащие $x \vee \overline{z}$, т.е. оставить $\Delta' = \{\overline{x} \vee y \vee z,\ \overline{y},\ x \vee \overline{z}\}$.

- $\overline{x} \vee \mathbf{y} \vee z,\ \overline{\mathbf{y}} \models \overline{x} \vee z$, так что $\Delta'' = \{\overline{x} \vee y \vee z,\ \overline{y},\ x \vee \overline{z},\ \overline{x} \vee z\}$ и после удаления дизъюнкций, строго содержащих $\overline{x} \vee z$, $\Delta'' = \{\overline{y}, x \vee \overline{z},\ \overline{x} \vee z\}$.

Других нетривиальных резолюций нет, Δ'' замкнуто относительно резолюций, поэтому формула A не является логическим следствием формул A_1 и A_2.

Этот результат можно, конечно, получить, построив таблицы истинности:

x	y	z	$x \vee y \vee \overline{z}$	$\overline{x} \vee y \vee z$	$\overline{x} \vee \overline{y} \vee z$	$x \vee \overline{y} \vee \overline{z}$	A_1	A_2	A
0	0	0	1	1	1	1	1	1	0
0	0	1	0	1	1	1	0	1	0
0	1	0	1	1	1	1	1	1	1
0	1	1	1	1	1	0	1	0	1
1	0	0	1	0	1	1	0	1	0
1	0	1	1	1	1	1	1	1	0
1	1	0	1	1	0	1	1	0	1
1	1	1	1	1	1	1	1	1	1

2. Верно ли, что $(x \vee y \vee \overline{z}) \wedge (\overline{x} \vee y \vee z),\ x \to y \wedge z \models y \vee \overline{x} \wedge \overline{z}$?

Здесь $A = y \vee \overline{x} \wedge \overline{z}$, $A_1 = (x \vee y \vee \overline{z}) \wedge (\overline{x} \vee y \vee z)$, $A_2 = x \to y \wedge z \equiv$ $\equiv \overline{x} \vee (y \wedge z) \equiv (\overline{x} \vee y) \wedge (\overline{x} \vee z)$. При этом $\overline{A} \equiv \overline{y} \wedge (x \vee z)$. Поэтому

$$\Delta = \{ x \vee y \vee \overline{z},\ \overline{x} \vee y \vee z,\ \overline{x} \vee y,\ \overline{x} \vee z,\ \overline{y},\ x \vee z \},$$

и после удаления всех дизъюнкций, строго содержащих $\overline{x} \vee z$, получим

$$\Delta = \{ x \vee y \vee \overline{z},\ \overline{x} \vee y,\ \overline{x} \vee z,\ \overline{y},\ x \vee z \}.$$

Теперь считаем нетривиальные резолюции:

- $\boldsymbol{x} \vee y \vee \overline{z},\ \overline{\boldsymbol{x}} \vee y \models (y \vee \overline{z}) \vee y \equiv y \vee \overline{z}$, поэтому

$$\Delta' = \{ x \vee y \vee \overline{z},\ \overline{x} \vee y,\ \overline{x} \vee z,\ \overline{y},\ x \vee z,\ y \vee \overline{z} \},$$

$$\Delta' = \{ \overline{x} \vee y,\ \overline{x} \vee z,\ \overline{y},\ x \vee z,\ y \vee \overline{z} \}.$$

- $\overline{x} \vee \boldsymbol{y},\ \overline{\boldsymbol{y}} \models \overline{x}$, и $\Delta'' = \{ \overline{y},\ x \vee z,\ y \vee \overline{z},\ \overline{x} \}$.
- $\overline{\boldsymbol{y}},\ \boldsymbol{y} \vee \overline{z} \models \overline{z}$, т.е. $\Delta''' = \{ \overline{y},\ x \vee z,\ \overline{x},\ \overline{z} \}$.
- $\boldsymbol{x} \vee z,\ \overline{\boldsymbol{x}} \models z$, поэтому $\Delta^{(4)} = \{ \overline{y},\ \overline{x},\ \overline{z},\ z \}$, и $\Delta^{(4)} \models z \wedge \overline{z}$.

Итак, $A_1, A_2 \models A$. Проверьте этот результат с помощью таблиц истинности.

Изложенный алгоритм допускает программную реализацию, эффективность которой зависит от удобства организации представления данных в ЭВМ и порядка вычисления резолюций.

IV. Проектирование, анализ и оптимизация релейно-контактных и больших интегральных схем. Рассмотрим лишь некоторые модельные задачи, иллюстрирующие методы этой важной и необъятной области современных технологий.

Задача 1. *Разработать схему для предварительного отбора участников соревнований в следующий тур. Перед каждым из четырёх членов жюри находится выключатель, который включается, если этот член жюри считает участника достойным прохождения в следующий тур. На табло должна загораться лампочка, если большинством голосов, обязательно включая председателя, имеющего два голоса, жюри высказалось за прохождение участника в следующий тур.*

Решение. Процесс проектирования проведём в несколько шагов:

1. ***Анализ логики задачи.*** Составим таблицу всех случаев, в которых должна загораться лампочка:

x_1	x_2	x_3	x_4	$Л$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

Здесь x_1 , x_2 , x_3 , x_4 – члены жюри, причём x_1 – председатель, а равенство $x_i = 1$ означает, что i-й судья нажал свою кнопку. Лампочка же включается тогда и только тогда, когда $Л = 1$, что происходит только при условии $(x_1 = 1) \wedge (x_2 + x_3 + x_4) \geq 1$.

2. ***Получение функции проводимости схемы.*** По таблице истинности напишем логическую функцию – *функцию проводимости схемы*:

$$Л(x_1 , x_2 , x_3 , x_4) = (x_1 \wedge \overline{x_2} \wedge \overline{x_3} \wedge x_4) \vee$$
$$\vee (x_1 \wedge \overline{x_2} \wedge x_3 \wedge \overline{x_4}) \vee (x_1 \wedge \overline{x_2} \wedge x_3 \wedge x_4) \vee$$
$$\vee (x_1 \wedge x_2 \wedge \overline{x_3} \wedge \overline{x_4}) \vee (x_1 \wedge x_2 \wedge \overline{x_3} \wedge x_4) \vee$$
$$\vee (x_1 \wedge x_2 \wedge x_3 \wedge \overline{x_4}) \vee (x_1 \wedge x_2 \wedge x_3 \wedge x_4).$$

3. ***Упрощение функции проводимости.*** Для того, чтобы схема получилась более компактной, эту функцию нужно упростить с помощью равносильных преобразований:

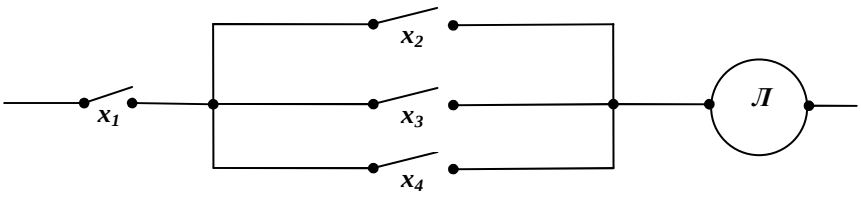
$$Л(x_1 , x_2 , x_3 , x_4) = (x_1 \wedge \overline{x_2} \wedge \overline{x_3} \wedge x_4) \vee (x_1 \wedge \overline{x_2} \wedge x_3 \wedge \overline{x_4}) \vee$$
$$\vee (x_1 \wedge \overline{x_2} \wedge x_3 \wedge x_4) \vee (x_1 \wedge x_2 \wedge \overline{x_3} \wedge \overline{x_4}) \vee$$
$$\vee (x_1 \wedge x_2 \wedge \overline{x_3} \wedge x_4) \vee (x_1 \wedge x_2 \wedge x_3 \wedge \overline{x_4}) \vee (x_1 \wedge x_2 \wedge x_3 \wedge x_4) \equiv$$
$$\equiv x_1 \wedge [(\overline{x_2} \wedge \overline{x_3} \wedge x_4) \vee (\overline{x_2} \wedge x_3 \wedge \overline{x_4}) \vee (\overline{x_2} \wedge x_3 \wedge x_4) \vee (x_2 \wedge \overline{x_3} \wedge \overline{x_4}) \vee$$
$$\vee (x_2 \wedge \overline{x_3} \wedge x_4) \vee (x_2 \wedge x_3 \wedge \overline{x_4}) \vee (x_2 \wedge x_3 \wedge x_4)] \equiv$$
$$\equiv x_1 \wedge [(\overline{x_2} \wedge \overline{x_3} \wedge x_4) \vee (\overline{x_2} \wedge x_3) \vee (x_2 \wedge \overline{x_3}) \vee (x_2 \wedge x_3)] \equiv$$
$$\equiv x_1 \wedge [(\overline{x_2} \wedge \overline{x_3} \wedge x_4) \vee x_3 \vee (x_2 \wedge \overline{x_3})] \equiv$$
$$\equiv x_1 \wedge [(\overline{x_2} \wedge \overline{x_3} \wedge x_4) \vee (x_2 \vee x_3)] \equiv x_1 \wedge [(\overline{x_2 \vee x_3} \wedge x_4) \vee (x_2 \vee x_3)] \equiv$$
$$\equiv x_1 \wedge (x_2 \vee x_3 \vee x_4).$$

Конечно, о таком результате в этой простейшей задаче можно было бы догадаться, внимательно прочитав условие. В случае сложных схем этапы генерации и упрощения логической функции можно автоматизировать.

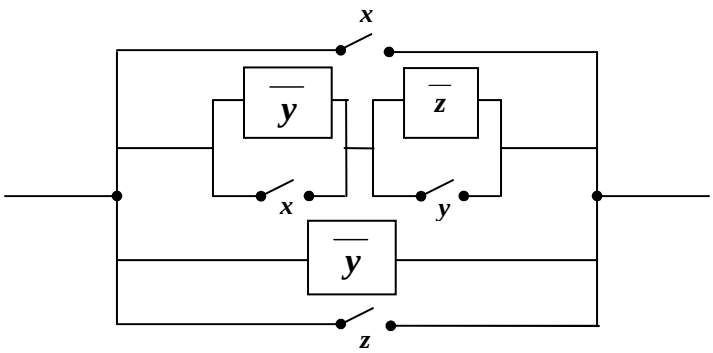
4. ***Изображение схемы.*** Теперь можно нарисовать искомую релейно-контактную схему, используя следующие условные обозначения, позволяющие строить электрическую схему по логической функции:

Обозначения	
логические	***релейно-контактные***
0	*цепь разомкнута*
1	*цепь замкнута*
$\overline{x}$	$\overline{x}$ *инверсия*
$x \wedge y$	x y *последовательное соединение*
$x \vee y$	x y *параллельное соединение*

Таким образом, проектируемая схема выглядит так:



Задача 2. *Упростить релейно-контактную схему, приведённую ниже.*



Учитывая реализацию последовательных и параллельных соединений в электрической схеме логическими связками конъюнкции и дизъюнкции соответственно, получаем функцию проводимости

$$f(x, y, z) = x \vee [(\overline{y} \vee x) \wedge (\overline{z} \vee y)] \vee \overline{y} \vee z\ .$$

После упрощения $f(x, y, z) = x \vee [(\overline{y} \vee x) \wedge (\overline{z} \vee y)] \vee \overline{y} \vee z \equiv$

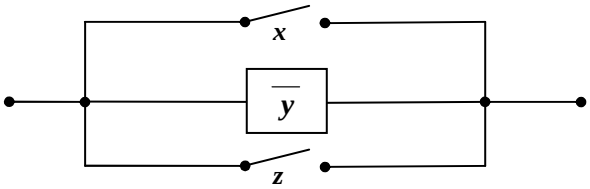
$$\equiv x \vee [\overline{y} \wedge \overline{z} \vee x \wedge \overline{z} \vee \overline{y} \wedge y \vee x \wedge y] \vee \overline{y} \vee z \equiv$$

$$\equiv x \vee (\overline{y} \wedge \overline{z}) \vee (x \wedge \overline{z}) \vee (x \wedge y) \vee \overline{y} \vee z \equiv$$

$$\equiv (x \vee x \wedge \overline{z} \vee x \wedge y) \vee (\overline{y} \wedge \overline{z} \vee \overline{y}) \vee z \equiv$$

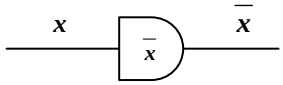
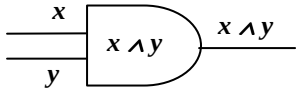
$$\equiv x \wedge (1 \vee \overline{z} \vee y) \vee \overline{y} \wedge (\overline{z} \vee 1) \vee z \equiv x \vee \overline{y} \vee z$$

рисуем новую схему:

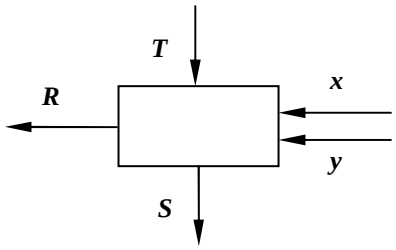


Отличие электронных *интегральных схем* от обычных электрических состоит, во-первых, в том, что они позволяют использовать транзисторы, с помощью которых более просто и компактно проектируются стандартные электронные устройства (*вентили*), реализующие те или иные логические функции. Во-вторых, технология изготовления интегральных схем позволяет размещать на малой площади изготавливаемого кристалла большое количество элементов, обеспечивающих его многофункциональность.

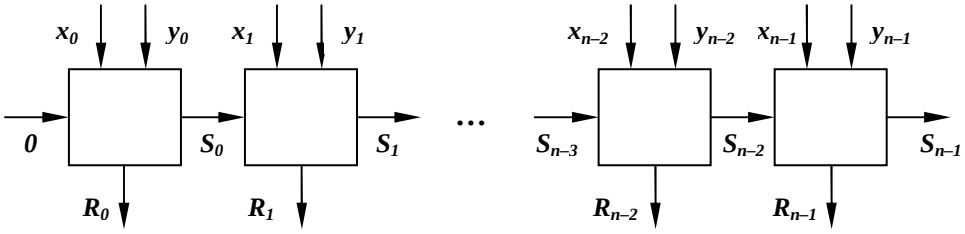
С логической точки зрения процесс разработки интегральной схемы ничем не отличается от этапов построения электрической схемы: вначале выписывается булева функция проводимости, которая минимизируется и реализуется в схеме с использованием доступной элементной базы. Конечно, при этом необходимо ещё учесть технологические ограничения, которые, грубо говоря, не позволяют “лепить” слишком много элементов и “проводов” на ограниченном участке печатной платы. Эти ограничения здесь рассматриваться не будут, хотя и очень важны при реальном проектировании интегральных схем.

Обозначения	
логические	***интегральных схем***
0	*сигнал низкого уровня*
1	*сигнал высокого уровня*
$\overline{x}$	 *вентиль “НЕ”*
$x \wedge y$	 *вентиль “И”*
$x \vee y$	 *вентиль “ИЛИ”*

Рассмотрим пример проектирования *сумматора* – реального электронного устройства, складывающего два n-разрядных двоичных числа. При сложении чисел “в столбик” цифры результата получаются последовательно: справа налево. Для получения очередной цифры нужно сложить две текущие цифры слагаемых и учесть полученный на предыдущем шаге перенос. Таким образом, сумматор можно проектировать *на основе конвейерной технологии*, часто используемой при создании разнообразных сложных интегральных схем. Именно, достаточно создать более простое устройство – *одноразрядный сумматор*:



получающий на входах очередные суммируемые цифры x, y а также бит переноса T, и дающий на выходах очередную цифру результата R и новый бит переноса S.



Если такое устройство создано, то n-разрядный сумматор можно построить в соответствии со следующей схемой. Здесь начальный бит переноса S_{-1} равен 0, и вырабатываемые в дальнейшем биты переноса передаются “по конвейеру”. Последний бит переноса S_{n-1} даёт информацию о *переполнении*: он равен единице в том и только том случае, если результат сложения не помещается в n разрядов.

Итак, спроектируем одноразрядный сумматор. Его естественная логика работы реализована в следующей таблице, из которой получаем дизъюнктивные формы логических функций $S(x, y, T)$ и $R(x, y, T)$:

x	y	T	S	R
0	0	0	0	0
1	0	0	0	1
0	1	0	0	1
1	1	0	1	0
0	0	1	0	1
1	0	1	1	0
0	1	1	1	0
1	1	1	1	1

$$S(x, y, T) = (x \wedge y \wedge \overline{T}) \vee (x \wedge \overline{y} \wedge T) \vee$$
$$\vee (\overline{x} \wedge y \wedge T) \vee (x \wedge y \wedge T),$$
$$R(x, y, T) = (x \wedge \overline{y} \wedge \overline{T}) \vee (\overline{x} \wedge y \wedge \overline{T}) \vee$$
$$\vee (\overline{x} \wedge \overline{y} \wedge T) \vee (x \wedge y \wedge T).$$

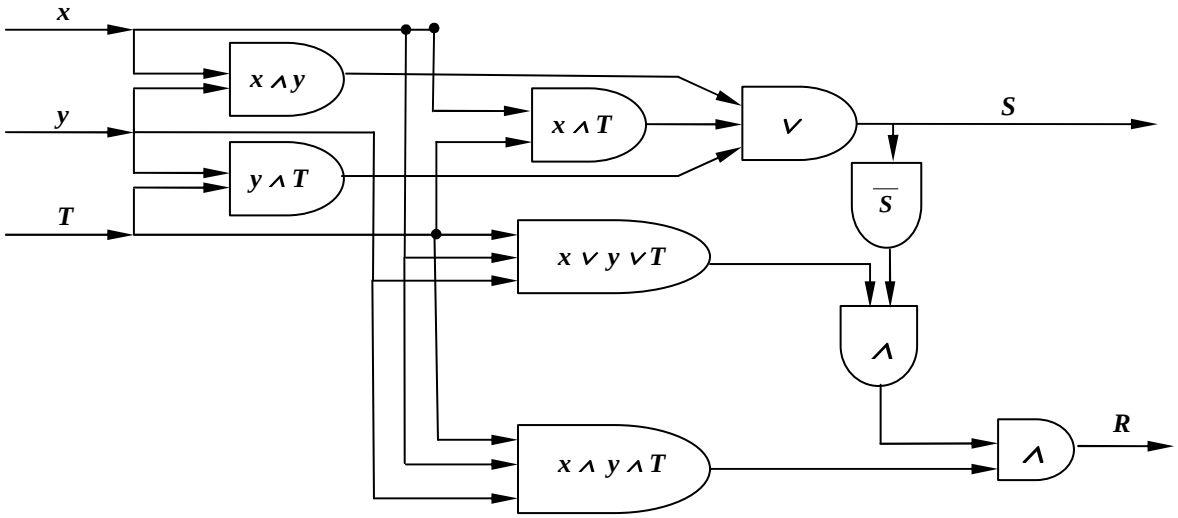
Теперь эти функции нужно упростить. Оказывается,

$$S(x, y, T) \equiv (x \wedge y) \vee (x \wedge T) \vee (y \wedge T),$$
$$R(x, y, T) \equiv (x \wedge y \wedge T) \vee \overline{S(x, y, T)} \wedge (x \vee y \vee T),$$

что следует из таблицы истинности правых частей r и s этих равенств.

x	y	T	R	S	$\overline{S}$	$x \wedge y \wedge T$	$x \vee y \vee T$	r	$x \wedge y$	$x \wedge T$	$y \wedge T$	s
0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	0	1	0	1	0	1	1	0	0	0	0
0	1	0	1	0	1	0	1	1	0	0	0	0
1	1	0	0	1	0	0	1	0	1	0	0	1
0	0	1	1	0	1	0	1	1	0	0	0	0
1	0	1	0	1	0	0	1	0	0	1	0	1
0	1	1	0	1	0	0	1	0	0	0	1	1
1	1	1	1	1	0	1	1	1	1	1	1	1

Таким образом, можно построить следующую схему одноразрядного сумматора, где вентили конъюнкции и дизъюнкции трёх величин можно получить, два раза выполнив соответствующие операции с двумя аргументами.



ГЛАВА II. АЛГЕБРА ПРЕДИКАТОВ

§ 1. Предикаты и кванторы

Каждая наука имеет дело со специфическими объектами, совокупность которых образует *объектную (или предметную) область* данной науки. Об этих объектах можно формулировать высказывания, которые могут быть истинными или ложными. При этом удобно использовать не одиночные высказывания, а "высказывания" с переменными, вместо которых можно подставлять те или иные конкретные объекты.

Примеры: 1. Высказывание "Волга впадает в Каспийское море" является истинным и говорит об одной конкретной реке Волге. Можно рассмотреть следующее "высказывание" с переменной x: "Река x впадает в Каспийское море", которое позволяет вместо переменной x подставлять любую реку и получать осмысленные высказывания. Например, при $x =$ *Иртыш* получим ложное высказывание.

2. "*3 – простое число*" – истинное высказывание об одном числе *3*, а "*y – простое число*" – это "высказывание с переменной" y, вместо которой можно подставлять любые целые числа и получать осмысленные высказывания. Например, при $y = 17$ получим истинное высказывание, а при $y = 6, -7$ – ложные.

Точно так же можно образовывать "высказывания " и от нескольких переменных. Например, "$x > y$" – "высказывание" от двух переменных x и y, вместо которых можно подставлять любые действительные числа, "$x^2 + y^2 = z^2$" – "высказывание" от трёх переменных x, y и z, принимающих числовые значения.

Пусть A – произвольное непустое множество, $x_1, \dots, x_n$ – переменные. Повествовательное предложение, в котором участвуют переменные $x_1, \dots, x_n$, обращающееся в высказывание при подстановке вместо $x_1, \dots, x_n$ произвольных элементов $a_1, \dots, a_n \in A$, называется *предикатом от n переменных* $x_1, \dots, x_n$ *на* A. Следует отметить, что для простоты будут, как правило, рассматриваться предикаты, всюду определённые на A.

Замечание: Само "повествовательное предложение, в котором участвуют переменные $x_1, \dots, x_n$" **высказыванием не является**. Например, предложение "Река x впадает в Каспийское море" бессмысленно, т.к. x – это переменная, а не

название реки. Но оно становится высказыванием после подстановки вместо x произвольного названия реки.

Можно дать другое определение предиката, не ссылающееся на неопределяемое понятие высказывания: *предикат* $P(x_1, \dots, x_n)$ *от* n *переменных* $x_1, \dots, x_n$ *на* A – это произвольное отображение (т.е. всюду определённая функция) $P: A^n \to B = \{0, 1\}$, где значения 1 и 0 интерпретируются как обычно – *истина* и *ложь*.

Примеры: 1. "$x \vdots 3$" (x делится нацело на 3) – предикат от одного переменного x на $\mathbf{Z}$ – множестве всех целых чисел – представляет функцию $P: \mathbf{Z} \to B$, где $P(x) = 1$ тогда и только тогда, когда x делится на 3.

2. "$x > \dfrac{x-1}{y}$" – предикат от двух переменных x, y на $A = \mathbf{R} \setminus \{0\}$, но не на $\mathbf{R}$ (?!). Его можно рассматривать как функцию $P: A \times A \to B$ двух переменных, где $P(x, y) = 0$ в том и только том случае, если $x \le \dfrac{x-1}{y}$.

Если $P(x_1, \dots, x_n)$ – предикат от n переменных на A, то множество $D(P) = \underbrace{A \times \dots \times A}_{n}$ (декартово произведение n экземпляров множества A, обозначаемое также A^n) называют *областью определения предиката* $P(x_1, \dots, x_n)$. Множество $D_1(P) = \{(a_1; \dots; a_n) \in D(P) \mid P(a_1, \dots, a_n) = 1\}$ называют *областью истинности этого предиката*, а множество $D_0(P) = D(P) \setminus D_1(P)$ – *областью ложности предиката* $P(x_1, \dots, x_n)$. Ясно, что

$$D_0(P) = \{(a_1; \dots; a_n) \in D(P) \mid P(a_1, \dots, a_n) = 0\}.$$

Сведения о простейших понятиях теории множеств даны в § 1 приложения.

Примеры: 1. Для предиката $P(x) =$ "$x \vdots 3$" в соответствии с определениями

$$D(P) = \mathbf{Z},\ D_1(P) = \{x \in \mathbf{Z} \mid x \vdots 3\} = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$D_0(P) = \mathbf{Z} \setminus D_1(P) = \{\dots -8, -7, -5, -4, -2, -1, 1, 2, 4, 5, 7, 8, \dots\}.$$

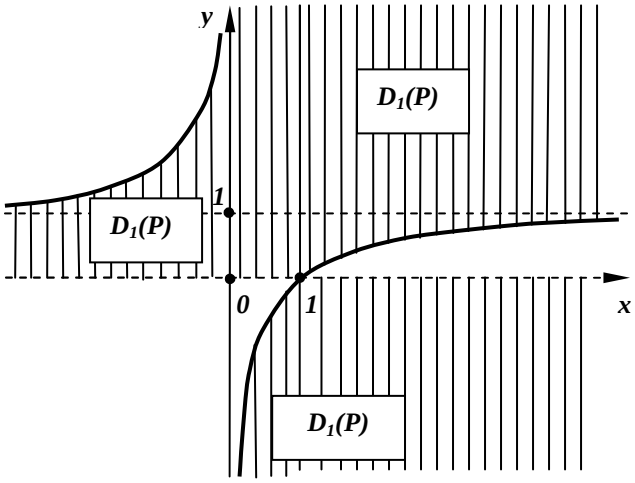
2. Для предиката $P(x) =$ "$x^2 > x$" имеем $D(P) = \mathbf{R}$, $D_1(P) = \{x \in \mathbf{R} \mid x^2 > x\} = (-\infty; 0) \cup (1; +\infty)$, $D_0(P) = \{x \in \mathbf{R} \mid x^2 \le x\} = [0; 1]$.

3. Для предиката $P(x, y) =$ "$x > \dfrac{x-1}{y}$" получим $D(P) = (\mathbf{R} \setminus \{0\}) \times (\mathbf{R} \setminus \{0\}) = (\mathbf{R} \setminus \{0\})^2$. Вычислим области истинности и ложности предиката:

$$D_1(P) = \{(x; y) \in D(P) \mid x > \frac{x-1}{y}\}, \quad D_0(P) = \{(x; y) \in D(P) \mid x \le \frac{x-1}{y}\}.$$

Для этого решим неравенство $x > \frac{x-1}{y}$:

$$x > \frac{x-1}{y} \Leftrightarrow \frac{x\cdot y - x + 1}{y} > 0 \Leftrightarrow y\cdot(x\cdot y - x + 1) > 0.$$



Если $y > 0$, то $x\cdot y - x + 1 > 0$. Это выполнено при $x = 0$, при $y > \frac{x-1}{x} = 1 - \frac{1}{x}$ (для $x > 0$) и при $0 < y < 1 - \frac{1}{x}$ (для $x < 0$).

Для $y < 0$ получаем условие $x\cdot y - x + 1 < 0$. Это верно при $y < 1 - \frac{1}{x}$ (для $x > 0$).

Полученные множества $D_1(P)$ и $D_0(P)$ изображены на рисунке: множество $D_1(P)$ заштриховано, а $D_0(P)$ – нет.

Логические операции над предикатами

Если заданы два предиката $P(x_1, \dots, x_n)$ и $Q(x_1, \dots, x_n)$ с одной и той же областью определения A^n и одним и тем же набором переменных, то можно рассмотреть предикаты $\overline{P}(x_1, \dots, x_n)$, $(P \wedge Q)(x_1, \dots, x_n)$, $(P \vee Q)(x_1, \dots, x_n)$, $(P \to Q)(x_1, \dots, x_n)$, $(P \leftrightarrow Q)(x_1, \dots, x_n)$, называемые соответственно *отрицанием предиката* P, а также *конъюнкцией, дизъюнкцией, импликацией и эквивалентностью предикатов* P *и* Q. Эти новые предикаты определяются следующим образом: для любых $a_1, \dots, a_n \in A$ положим $\overline{P}(a_1, \dots, a_n) = \overline{P(a_1, \dots, a_n)}$ и при $\omega \in \{\wedge, \vee, \to, \leftrightarrow\}$ $(P\,\omega\,Q)(a_1, \dots, a_n) = (P(a_1, \dots, a_n)\ \omega\ Q(a_1, \dots, a_n))$.

Примеры: 1. Пусть на $\boldsymbol{R}$ заданы два предиката: $P(x) =$ "$x > 3$" и $Q(x) =$ "$x \le 5$". Тогда для любого $a \in \boldsymbol{R}$ имеем

$$\overline{P}(a) = \overline{"a > 3"} = "a \le 3",\quad \overline{Q}(a) = \overline{"a \le 5"} = "a > 5",$$

$$(P \wedge Q)(a) = "a > 3" \wedge "a \le 5" = "3 < a \le 5",$$

$$(P \vee Q)(a) = "a > 3" \vee "a \le 5" = "a \in \boldsymbol{R}" = 1,$$

$$(P \to Q)(a) = "a > 3" \to "a \le 5" \equiv \overline{"a > 3"} \vee "a \le 5" = "a \le 3" \vee "a \le 5" = "a \le 5",$$

$$(P \leftrightarrow Q)(a) = "a > 3" \leftrightarrow "a \le 5" \equiv (\overline{"a > 3"} \wedge \overline{"a \le 5"}) \vee ("a > 3" \wedge "a \le 5") =$$

$$= ("a \le 3" \wedge "a > 5") \vee "3 < a \le 5" \equiv \boldsymbol{0} \vee "3 < a \le 5" \equiv "3 < a \le 5".$$

Ясно, что в этом примере верны следующие равенства множеств:

$$D_1(\overline{P}) = D_0(P),\ D_0(\overline{P}) = D_1(P),\ D_1(P \wedge Q) = D_1(P) \cap D_1(Q),$$

$$D_0(P \wedge Q) = D_0(P) \cup D_0(Q),\ D_1(P \vee Q) = D_1(P) \cup D_1(Q),\ D_1(P \to Q) = D_0(P) \cup D_1(Q),$$

$$D_1(P \leftrightarrow Q) = (D_1(P) \cap D_1(Q)) \cup (D_0(P) \cap D_0(Q))$$ (проверьте !!).

2. Пусть $P(x, y) =$ "$x^2 < y$", $Q(x, y) =$ "$y \le x$" – два предиката на $\mathbf{Z}$. Вычислим предикат $P \to Q$ и его область истинности.

По определению для любых $a, b \in \mathbf{Z}$: $(P \to Q)(a, b) = (P(a, b) \to Q(a, b)) =$ $= $ "$a^2 < b$" $\to$ "$b \le a$" $\equiv$ $\overline{"a^2 < b"} \vee$ "$b \le a$" $\equiv$ "$a^2 \ge b$" $\vee$ "$b \le a$". Когда истинна последняя дизъюнкция ? Она истинна, если $b \le a$. Но учитывая, что $a \in \mathbf{Z}$, имеем $a \le a^2$, так что из $b \le a$ следует $b \le a^2$, и $(P \to Q)(a, b) \equiv$ "$b \le a$".

Как и ранее, нетрудно понять, что $D_1(P \to Q) = D_0(P) \cup D_1(Q)$.

Оказывается, что отмеченные в этих примерах соотношения, связывающие множества $D_1(P \ \omega Q)$ и $D_1(P), D_1(Q), D_0(P), D_0(Q)$, справедливы всегда.

Лемма (об областях истинности). *Пусть $P(x_1, \dots, x_n)$, $Q(x_1, \dots, x_n)$ – два предиката на множестве A. Тогда верны равенства множеств:*

$D_1(\overline{P}) = D_0(P) = D(P) \setminus D_1(P)$,

$D_1(P \wedge Q) = D_1(P) \cap D_1(Q)$,

$D_1(P \vee Q) = D_1(P) \cup D_1(Q)$,

$D_1(P \to Q) = D_0(P) \cup D_1(Q)$,

$D_1(P \leftrightarrow Q) = (D_1(P) \cap D_1(Q)) \cup (D_0(P) \cap D_0(Q))$.

Доказательство. Все равенства доказываются однообразно, исходя из определения области истинности и логических операций над предикатами. Например,

$$D_1(\overline{P}) = \{(a_1; \dots; a_n) \in A^n \mid \overline{P}(a_1, \dots, a_n) = 1\} =$$

$$= \{(a_1; \dots; a_n) \in A^n \mid P(a_1, \dots, a_n) = 0\} = D_0(P) = D(P) \setminus D_1(P) = A^n \setminus D_1(P),$$

что и требовалось.

Аналогично доказываются и остальные равенства множеств (в приводимых ниже вычислениях для краткости полагаем $\mathbf{a} = (a_1; \dots; a_n)$, $P(\mathbf{a}) = P(a_1; \dots; a_n)$):

$$D_1(P \wedge Q) = \{(a_1; \dots; a_n) \in A^n \mid (P \wedge Q)(a_1, \dots, a_n) = 1\} =$$

$$= \{\mathbf{a} \in A^n \mid (P(\mathbf{a}) \wedge Q(\mathbf{a})) = 1\} = \{\mathbf{a} \in A^n \mid (P(\mathbf{a}) = 1) \wedge (Q(\mathbf{a}) = 1)\} =$$

$$= \{\mathbf{a} \in A^n \mid P(\mathbf{a}) = 1\} \cap \{\mathbf{a} \in A^n \mid Q(\mathbf{a}) = 1\} = D_1(P) \cap D_1(Q),$$

$$D_1(P \leftrightarrow Q) = \{\mathbf{a} \in A^n \mid (P \leftrightarrow Q)(\mathbf{a}) = 1\} = \{\mathbf{a} \in A^n \mid (P(\mathbf{a}) \leftrightarrow Q(\mathbf{a})) = 1\} =$$

$$= \{\mathbf{a} \in A^n \mid ((P(\mathbf{a}) \wedge Q(\mathbf{a})) \vee (\overline{P(\mathbf{a})} \wedge \overline{Q(\mathbf{a})})) = 1)\} =$$

$$= \{\mathbf{a} \in A^n \mid (P(\mathbf{a}) \wedge Q(\mathbf{a}) = 1) \vee (\overline{P(\mathbf{a})} \wedge \overline{Q(\mathbf{a})} = 1)\} =$$

$$= \{ \boldsymbol{a} \in A^n \mid P(\boldsymbol{a}) \wedge Q(\boldsymbol{a}) = 1\} \cup \{ \boldsymbol{a} \in A^n \mid \overline{P(\boldsymbol{a})} \wedge \overline{Q(\boldsymbol{a})} = 1\} =$$

$$= (\{ \boldsymbol{a} \in A^n \mid P(\boldsymbol{a}) = 1\} \cap \{ \boldsymbol{a} \in A^n \mid Q(\boldsymbol{a}) = 1\}) \cup$$

$$\cup (\{ \boldsymbol{a} \in A^n \mid \overline{P(\boldsymbol{a})} = 1\} \cap \{ \boldsymbol{a} \in A^n \mid \overline{Q(\boldsymbol{a})} = 1\}) =$$

$$= (D_1(P) \cap D_1(Q)) \cup (\{ \boldsymbol{a} \in A^n \mid P(\boldsymbol{a}) = 0\} \cap \{ \boldsymbol{a} \in A^n \mid Q(\boldsymbol{a}) = 0\}$$

$$= (D_1(P) \cap D_1(Q)) \cup (D_0(P) \cap D_0(Q)).$$

Лемма доказана.

Упражнения: 1. Вычислите области истинности предикатов P, Q, $\overline{P}$, $\overline{Q}$, $P \wedge Q$, $P \vee Q$, $P \to Q$, $P \leftrightarrow Q$, где $P(x)$ = "$x^2 > x$", $Q(x)$ = "$x^2 - 4 \cdot x + 3 < 0$".

2. Прочувствуйте аналогию между логическими операциями над предикатами и операциями над множествами. Сформулируйте общее правило вычисления области истинности предиката, полученного с помощью логических связок из известных предикатов.

3. Сформулируйте и докажите лемму об областях ложности.

Рассмотренные логические операции над предикатами позволяют по заданным на множестве A предикатам строить новые предикаты. Другой способ построения новых предикатов дают *кванторы*. *Квантор существования* $\exists$ и *квантор всеобщности* $\forall$ – это специальные математические знаки, служащие для сокращённого обозначения выражений *"существует"* и *"для любого"* соответственно.

Примеры: 1. Фразу *"квадрат любого действительного числа неотрицателен"* математики записывают так: $\forall\, x \in \boldsymbol{R}\ \ x^2 \geq 0$ (читается: *для любого действительного числа* x *выполнено свойство* $x^2 \geq 0$).

2. Запись $\forall m \in \boldsymbol{Z}\ \ (\exists n \in \boldsymbol{Z}\ \ n < m)$ (читается: *для любого целого числа* m *существует целое число* n *со свойством* $n < m$) выражает тот факт, что у любого целого числа есть предшествующие ему целые числа.

В приведённых примерах написанные с помощью кванторов формулы являлись высказываниями. Оба этих высказывания были истинны, но не следует думать, что все высказывания, записанные с помощью кванторов истинны: почувствуйте разницу, прочитав и осмыслив следующие высказывания $\forall\, x \in \boldsymbol{Z}\ \ x \geq 0$, $\forall m \in \boldsymbol{N}\ \ (\exists n \in \boldsymbol{N}\ \ n < m)$, $\forall\, x \in \boldsymbol{R}\ \ (\exists y \in \boldsymbol{R}\ \ |x - y| < x)$.

Пусть теперь $P(x)$ – предикат от одной переменной на множестве A. Тогда записи $\forall x \in A\ \ P(x)$ (для любого $x \in A$ выполнено свойство $P(x)$) и $\exists x \in A\ \ P(x)$ (существует $x \in A$ со свойством $P(x)$) являются высказываниями, не зависящими от переменной x. Говорят, что эти высказывания получены *связыванием*

переменной x *с помощью квантора всеобщности* $\forall$ *(и квантора существования* $\exists$*)* соответственно. При этом высказывание $\forall x \in A\ P(x)$ *истинно* тогда и только тогда, когда ***любой объект*** a ***из множества*** A ***принадлежит области истинности предиката*** $P(x)$, оно *ложно* тогда и только тогда, когда ***хотя бы один объект*** a ***из множества*** A ***принадлежит области ложности предиката*** $P(x)$. Высказывание $\exists x \in A\ P(x)$ *истинно* тогда и только тогда, когда ***хотя бы один объект*** a ***из множества*** A ***принадлежит области истинности предиката*** $P(x)$, оно *ложно* тогда и только тогда, когда ***все объекты*** a ***из множества*** A ***принадлежат области ложности предиката*** $P(x)$.

Примеры: 1. Если $P(x) =$ *"*x *делится нацело на 15"* – предикат на $\boldsymbol{Z}$, то высказывания $\forall x \in \boldsymbol{Z}\ P(x)$ и $\exists x \in \boldsymbol{Z}\ P(x)$ ложно и истинно соответственно.

2. Если $P(x) =$ *"*$x^2 + 6 \cdot x + 100 > 0$*"* – предикат на $\boldsymbol{R}$, то $\forall x \in \boldsymbol{R}\ P(x)$ – истинное высказывание. А каковы высказывания $\exists x \in \boldsymbol{R}\ P(x)$, $\forall x \in \boldsymbol{R}\ \overline{P}(x)$?

Аналогично предыдущему случаю предикатов от одной переменной можно связывать кванторами и любую переменную в предикате от n переменных, получая при этом предикат от $(n–1)$-й переменной: если $P(x_1, \dots, x_n)$ – предикат от n переменных на множестве A, то можно, связывая переменную x_i кванторами, образовать предикаты $\forall x_i \in A\ P(x_1, \dots, x_n)$ и $\exists x_i \in A\ P(x_1, \dots, x_n)$ от $(n–1)$-й переменных $x_1, \dots x_{i-1}, x_{i+1}, \dots, x_n$. Их области истинности состоят, по определению, ***из всех наборов*** $(a_1; \dots; a_{i-1}; a_{i+1}; \dots; a_n) \in A^{n-1}$ ***значений переменных*** $x_1, \dots x_{i-1}, x_{i+1}, \dots, x_n$, ***для которых при любом (соответственно хотя бы при одном)*** $x_i = a \in A$ ***истинно*** $P(a_1, \dots, a_{i-1}; a; a_{i+1}; \dots; a_n) = 1$.

Примеры: 1. Если $P(x, y) =$ *"*$x^2+y^2 = 1$*"* – предикат от двух переменных на множестве $\boldsymbol{R}$, то предикат $S(x) = (\forall y \in \boldsymbol{R}\ P(x, y))$ от одной переменной x принимает значение $\boldsymbol{0}$ (*ложь*) при любом $x \in \boldsymbol{R}$ (т.к., например, при $y = 2$ равенство $x^2 + y^2 = 1$ не верно, какой бы $x \in \boldsymbol{R}$ ни взять). Предикат $T(x) = (\exists y \in \boldsymbol{R}\ P(x, y))$ имеет область истинности $D_1(T) = [–1; 1]$ (при любом $x = a \in [–1; 1]$ можно найти $y = \pm\sqrt{1 - a^2}$ со свойством $x^2 + y^2 = 1$).

2. Пусть A – множество всех прямых на плоскости, $P(x, y, z) =$*"прямые* x, y, z *имеют общую точку"* – предикат от трёх переменных x, y, z на A. Тогда предикат $S(x, z) = (\forall y \in A\ P(x, y, z))$ от двух переменных x, z имеет пустую область истинности (?!), а предикат $T(x, z) = (\exists y \in A\ P(x, y, z))$ обладает тем свойством, что $(T(x, z) = 1) \Leftrightarrow (x \cap z \neq \varnothing)$.

Для удобства дальнейших рассмотрений введём следующие сокращения:

1) вместо выражения $\forall x_1 \in A\ (\forall x_2 \in A\ (\ldots (\forall x_n \in A\ P(x_1, \ldots, x_n))\ldots))$ будем писать $\forall x_1, \ldots, x_n \in A\ P(x_1, \ldots, x_n)$, а $\exists x_1, \ldots, x_n \in A\ P(x_1, \ldots, x_n)$ – вместо $\exists x_1 \in A\ (\exists x_2 \in A\ (\ldots (\exists x_n \in A\ P(x_1, \ldots, x_n))\ldots))$. Здесь важно, что кванторы при всех элементах $x_1, \ldots, x_n$ однотипны, т.е. либо все являются кванторами существования, либо же все – кванторами всеобщности, а также то, что все элементы $x_1, \ldots, x_n$ выбираются из одного и того же множества A.

2) обозначение $\exists!\, x_i \in A\ P(x_1, \ldots, x_i, \ldots, x_n)$ будет использоваться для сокращения выражения "*существует <u>единственный</u> элемент x_i во множестве A со свойством $P(x_1, \ldots, x_i, \ldots, x_n)$*". Формально это высказывание записывается так: $(\exists\, x_i \in A\ \ P(x_1, \ldots, x_i, \ldots, x_n)) \wedge (\forall y_i \in A\ \ (P(x_1, \ldots, y_i, \ldots, x_n) \to (y_i = x_i)))$.

§ 2. Равносильные и тождественно истинные предикаты

Два предиката $P(x_1, \ldots, x_n)$ и $Q(x_1, \ldots, x_n)$, определённые на множестве A (т.е. предикаты с условиями $A^n \subseteq D(P) \cap D(Q)$), называют *равносильными на множестве A* и пишут при этом $P(x_1, \ldots, x_n) \equiv_A Q(x_1, \ldots, x_n)$, если выполнено равенство $D_1(P) \cap A^n = D_1(Q) \cap A^n$, другими словами, если $\forall a_1, \ldots, a_n \in A\ (P(a_1, \ldots, a_n) = 1 \leftrightarrow Q(a_1, \ldots, a_n) = 1)$. Если $D(P) = A^n = D(Q)$, то вместо $P(x_1, \ldots, x_n) \equiv_A Q(x_1, \ldots, x_n)$ будем кратко писать $P(x_1, \ldots, x_n) \equiv Q(x_1, \ldots, x_n)$.

Если $A^n \subseteq D_1(P)$, т.е. $\forall a_1, \ldots, a_n \in A\ \ P(a_1, \ldots, a_n) = 1$, то предикат $P(x_1, \ldots, x_n)$ называется *тождественно истинным на множестве A*: $P(x_1, \ldots, x_n) \equiv_A \mathbf{1}$. Аналогично, предикат $P(x_1, \ldots, x_n)$ называют *тождественно ложным на множестве A*: $P(x_1, \ldots, x_n) \equiv_A \mathbf{0}$, если $A^n \subseteq D_0(P)$, т.е. выполнено условие $\forall a_1, \ldots, a_n \in A\ P(a_1, \ldots, a_n) = 0$.

Примеры: 1. Равносильны ли предикаты $P(x) = "\frac{1}{x} > 1"$ и $Q(x) = "x < 1"$ на множестве $\mathbf{R}_+ = \{r \in \mathbf{R} \mid r > 0\} = (0; +\infty)$?

Во-первых, оба предиката определены на $\mathbf{R}_+$: $D(P) = \mathbf{R} \setminus \{0\}$, $D(Q) = \mathbf{R}$. Найдём их области истинности. Для предиката Q ясно, что $D_1(Q) = (-\infty; 1)$. Для предиката P имеем: $\frac{1}{x} > 1 \Leftrightarrow \frac{1-x}{x} > 0 \Leftrightarrow x \cdot (1-x) > 0 \Leftrightarrow x \in (0; 1)$. Хотя получили, что $D_1(P) \neq D_1(Q)$, но

$D_1(P) \cap \mathbf{R}_+ = (0; 1) \cap (0; +\infty) = (0; 1) = (-\infty; 1) \cap (0; +\infty) = D_1(Q) \cap \mathbf{R}_+$,

так что $P(x) \equiv_{\mathbf{R}_+} Q(x)$.

2. Рассмотренные выше предикаты $P(x)$ и $Q(x)$ не равносильны на множестве $A = \mathbf{R} \setminus \{0\}$: $D_1(P) \cap A = (0; 1) \neq (-\infty; 1) \setminus \{0\} = D_1(Q) \cap A$.

3. Предикат $Q(x)$ тождественно истинен на $\mathbf{R}_- = \{r \in \mathbf{R} \mid r < 0\} = (-\infty; 0)$.

Действительно, $\mathbf{R}_- \subseteq D_1(Q) = (-\infty; 1)$.

4. Предикат $P(x)$ тождественно ложен на множестве $(1; +\infty)$.

5. Предикаты $P(x, y) =$ "$x \cdot y \in \mathbf{Z}$" и $Q(x, y) =$ "$x \in \mathbf{Z} \wedge y \in \mathbf{Z}$" равносильны на множестве $A = \mathbf{Z}$, но не равносильны на множестве $\mathbf{R}$.

В самом деле, оба предиката определены на $\mathbf{R}$, точнее $D(P) = \mathbf{R} \times \mathbf{R} = D(Q)$, и тождественно истинны на $\mathbf{Z}$: высказывания $\forall a, b \in \mathbf{Z}\ a \cdot b \in \mathbf{Z}$ и $\forall a, b \in \mathbf{Z}\ (a \in \mathbf{Z}) \wedge (b \in \mathbf{Z})$ оба истинны. Поэтому $P(x) \equiv_{\mathbf{Z}} Q(x)$. С другой стороны, $D_1(Q) = \mathbf{Z} \times \mathbf{Z} \neq D_1(P)$: например, $(0{,}5; 2) \in D_1(P) \setminus \mathbf{Z} \times \mathbf{Z}$.

Упражнения: 1. Докажите, что $P(x) \equiv_A Q(x)$, где $A = (0; 10)$, $P(x) =$ "$x > 0{,}5$", $Q(x) =$ "$x^2 > 0{,}5 \cdot x$".

2. Равносильны ли на $\mathbf{R}_+$, $\mathbf{R}$ предикаты из предыдущего упражнения ?

3. Верно ли, что $P(x_1, \ldots, x_n) \equiv_A Q(x_1, \ldots, x_n)$ тогда и только тогда, когда $(P \to Q) \equiv_A \mathbf{1}$? А если $(P \leftrightarrow Q) \equiv_A \mathbf{1}$?

4. Равносильны ли предикаты $P(x, y) =$ "$x \cdot y = 1$" и $Q(x, y) =$ "$x = 1 / y$" на множествах $\mathbf{R}$, $\mathbf{R} \setminus \{0\}$, $\mathbf{N}$?

Приведём некоторые основные равносильности предикатов с кванторами.

Теорема (об основных равносильностях с кванторами).

(0) $\forall x \in A\ P(x, \mathbf{y}) \equiv \forall z \in A\ P(z, \mathbf{y})$, $\exists x \in A\ P(x, \mathbf{y}) \equiv \exists z \in A\ P(z, \mathbf{y})$, *где* $P(x, \mathbf{y})$ *не зависит от* z,

(1) $\forall x \in A\ (\forall y \in A\ P(x, y, \mathbf{z})) \equiv \forall y \in A\ (\forall x \in A\ P(x, y, \mathbf{z}))$,

$\exists x \in A\ (\exists y \in A\ P(x, y, \mathbf{z})) \equiv \exists y \in A\ (\exists x \in A\ P(x, y, \mathbf{z}))$

(для разноимённых кванторов утверждения не верны),

(2) $\overline{\forall x \in A\ P(x, \mathbf{y})} \equiv \exists x \in A\ \overline{P}(x, \mathbf{y})$, $\exists x \in A\ P(x, \mathbf{y}) \equiv \overline{\forall x \in A\ \overline{P}(x, \mathbf{y})}$,

$\overline{\exists x \in A\ P(x, \mathbf{y})} \equiv \forall x \in A\ \overline{P}(x, \mathbf{y})$, $\forall x \in A\ P(x, y) \equiv \overline{\exists x \in A\ \overline{P}(x, \mathbf{y})}$,

(3) $(\forall x \in A\ P(x, \mathbf{y})) \wedge (\forall x \in A\ Q(x, \mathbf{y})) \equiv \forall x \in A\ (P(x, \mathbf{y}) \wedge Q(x, \mathbf{y}))$

(для связки $\vee$ ***утверждение не верно)***,

(4) $(\exists x \in A\ P(x, \mathbf{y})) \vee (\exists x \in A\ Q(x, \mathbf{y})) \equiv \exists x \in A\ (P(x, \mathbf{y}) \vee Q(x, \mathbf{y}))$

(для связки $\wedge$ ***утверждение не верно)***,

(5) $(\forall x \in A\ P(x, \mathbf{y})) \vee R(\mathbf{y}) \equiv \forall x \in A\ (P(x, \mathbf{y}) \vee R(\mathbf{y}))$,

$(\exists x \in A\ P(x, \mathbf{y})) \vee R(\mathbf{y}) \equiv \exists x \in A\ (P(x, \mathbf{y}) \vee R(\mathbf{y}))$,

(6) $(\forall\, x \in A\ \ P(x, \mathbf{y})) \wedge R(\mathbf{y}) \ \equiv\ (\forall\, x \in A\ \ (P(x, \mathbf{y}) \wedge R(\mathbf{y}))$,

$(\exists\, x \in A\ \ P(x, \mathbf{y})) \wedge R(\mathbf{y}) \ \equiv\ (\exists\, x \in A\ \ (P(x, \mathbf{y}) \wedge R(\mathbf{y}))$,

(7) $\forall\, x \in A\ (R(\mathbf{y}) \to P(x, \mathbf{y})) \ \equiv\ R(\mathbf{y}) \to (\forall x \in A\ \ P(x, \mathbf{y}))$,

$\exists\, x \in A\ (R(\mathbf{y}) \to P(x, \mathbf{y})) \ \equiv\ R(\mathbf{y}) \to (\exists x \in A\ \ P(x, \mathbf{y}))$

(8) $(\forall\, x \in A\ \ P(x, \mathbf{y})) \to R(\mathbf{y}) \ \equiv\ (\exists\, x \in A\ \ (P(x, \mathbf{y}) \to R(\mathbf{y}))$,

$(\exists\, x \in A\ \ P(x, \mathbf{y})) \to R(\mathbf{y}) \ \equiv\ (\forall\, x \in A\ \ (P(x, \mathbf{y}) \to R(\mathbf{y}))$

(всюду жирные буквы обозначают, вообще говоря, наборы переменных, которые могут и отсутствовать, в равносильностях (5)–(8) предикат $R(\mathbf{y})$ *не зависит от* x*).*

Доказательство. Все равносильности доказываются единообразно, исходя из определений истинностных значений предикатов с кванторами и равносильности предикатов.

(0) Области истинности обоих предикатов $\exists\, x \in A\ \ P(x, \mathbf{y})$ и $\exists\, z \in A\ \ P(z, \mathbf{y})$ состоят из тех наборов $\boldsymbol{a} = (a_1\, ;\, \ldots\, ;\, a_n) \in A^n$, при которых найдётся элемент $b \in A$ со свойством $P(b, \boldsymbol{a}) = 1$, а значит, эти области истинности совпадают.

(1) Область истинности предиката $\forall\, x \in A\ \ (\forall\, y \in A\ \ P(x, y, \mathbf{z}))$ состоит из всех наборов $\boldsymbol{a} = (a_1\, ;\, \ldots\, ;\, a_n) \in A^n$, при которых предикат $\forall\, y \in A\ \ P(c, y, \boldsymbol{a})$ имеет значение 1 при любом $c \in A$, т.е. из всех наборов $\boldsymbol{a} \in A^n$ со свойством $P(c, d, \boldsymbol{a}) = 1$ при любых $c, d \in A$.

Точно так же область истинности предиката $\forall\, y \in A\ \ (\forall\, x \in A\ \ P(x, y, \mathbf{z}))$ состоит из всех наборов $\boldsymbol{a} = (a_1\, ;\, \ldots\, ;\, a_n) \in A^n$, при которых предикат $\forall\, x \in A\ P(x, d, \boldsymbol{a})$ принимает значение 1 при любом $d \in A$, т.е. из тех наборов $\boldsymbol{a} \in A^n$, при которых $P(c, d, \boldsymbol{a}) = 1$ при любых $c, d \in A$.

Сравнение выводов, сделанных в предыдущих абзацах, доказывает *(1)*.

(2) Область истинности предиката $\overline{\exists\, x \in A\ P(x, \mathbf{y})}$ состоит из всех таких наборов $\boldsymbol{a} = (a_1\, ;\, \ldots\, ;\, a_n) \in A^n$, для которых предикат $\exists\, x \in A\ \ P(x, \boldsymbol{a})$ принимает значение 0, т.е. из всех таких наборов $\boldsymbol{a} \in A^n$, при которых $P(c, \boldsymbol{a}) = 0$ при любом $c \in A$. Но множество всех таких наборов образует и множество истинности предиката $\forall\, x \in A\ \ \overline{P}\,(x, \mathbf{y})$, что и доказывает равносильность рассматриваемых предикатов.

(3) Область истинности предиката $(\forall\, x \in A\ \ P(x, \mathbf{y})) \wedge (\forall\, x \in A\ \ Q(x, \mathbf{y}))$ состоит из всех наборов $\boldsymbol{a} = (a_1\, ;\, \ldots\, ;\, a_n) \in A^n$, при которых $(\forall\, x \in A\ \ P(x, \boldsymbol{a})) = 1 = (\forall\, x \in A\ \ Q(x, \boldsymbol{a}))$, т.е. из всех $\boldsymbol{a} \in A^n$, для которых $P(c, \boldsymbol{a}) = 1 = Q(c, \boldsymbol{a})$ при

любом $c \in A$. Это множество наборов совпадает с множеством истинности исследуемого предиката $\forall x \in A\ (P(x, \mathbf{y}) \wedge Q(x, \mathbf{y}))$.

(5) Область истинности предиката $(\forall x \in A\ P(x, \mathbf{y})) \vee R(\mathbf{y})$ состоит из множества всех таких $\mathbf{a} = (a_1 ; \dots ; a_n) \in A^n$, для которых либо $R(\mathbf{a}) = 1$, либо $P(c, \mathbf{a}) = 1$ при любом $c \in A$. По определению дизъюнкции, это значит, что $(P(c, \mathbf{a}) \vee R(\mathbf{a})) = 1$ при любом $c \in A$, т.е. множество рассматриваемых наборов $\mathbf{a} \in A^n$ совпадает с областью истинности предиката $\forall x \in A\ (P(x, \mathbf{y}) \vee R(\mathbf{y}))$.

(6) Область истинности предиката $(\exists x \in A\ P(x, \mathbf{y})) \wedge R(\mathbf{y})$ состоит из множества всех таких $\mathbf{a} = (a_1 ; \dots ; a_n) \in A^n$, для которых $P(c, \mathbf{a}) = 1$ при некотором $c \in A$ и $R(\mathbf{a}) = 1$. Это значит, что $(P(c, \mathbf{a}) \wedge R(\mathbf{a})) = 1$, т.е. мнжество рассматриваемых наборов $\mathbf{a} \in A^n$ совпадает с областью истинности предиката $\exists x \in A\ (P(x, \mathbf{y}) \wedge R(\mathbf{y}))$.

(7) $(\forall x \in A\ (R(\mathbf{y}) \to P(x, \mathbf{y}))) \equiv (\forall x \in A\ (\overline{R}(\mathbf{y}) \vee P(x, \mathbf{y}))) \equiv$

$\equiv (\forall x \in A\ (P(x, \mathbf{y}) \vee \overline{R}(\mathbf{y}))) \overset{(5)}{\equiv} ((\forall x \in A\ P(x, \mathbf{y})) \vee \overline{R}(\mathbf{y})) \equiv$

$\equiv (\overline{R}(\mathbf{y}) \vee (\forall x \in A\ P(x, \mathbf{y}))) \equiv (R(\mathbf{y}) \to (\forall x \in A\ P(x, \mathbf{y})))$.

(8) $((\exists x \in A\ P(x, \mathbf{y})) \to R(\mathbf{y})) \equiv ((\forall x \in A\ \overline{P}(x, \mathbf{y})) \vee R(\mathbf{y})) \overset{(5)}{\equiv}$

$\overset{(5)}{\equiv} (\forall x \in A\ (\overline{P}(x, \mathbf{y}) \vee R(\mathbf{y}))) \equiv (\forall x \in A\ (P(x, \mathbf{y}) \to R(\mathbf{y})))$.

Теорема доказана.

Замечание: Утверждения пункта *(0)* доказанной теоремы носят общематематический характер: не важно как обозначать связанную переменную. Так, результат суммирования не зависит от обозначения индекса суммирования, а интеграл – от переменной интегрирования.

Приведём примеры, показывающие существенность ограничений в доказанной теореме:

Примеры: 1. $\forall x \in \mathbf{R}\ (\exists y \in \mathbf{R}\ x > y) \not\equiv \exists y \in \mathbf{R}\ (\forall x \in \mathbf{R}\ x > y)$, т.к. левая часть истинна, а правая – ложна.

2. $(\forall x \in \mathbf{R}\ x > 0) \vee (\forall x \in \mathbf{R}\ x \le 0) \not\equiv \forall x \in \mathbf{R}\ (x > 0) \vee (x \le 0)$, т.к. левая часть ложна, а правая – истинна.

3. $(\exists x \in \mathbf{R}\ x > 0) \wedge (\exists x \in \mathbf{R}\ x \le 0) \not\equiv \exists x \in \mathbf{R}\ (x > 0) \wedge (x \le 0)$, т.к. левая часть истинна, а правая – ложна.

4. Следующие равносильности не верны:

$$\forall x \in A\ (P(x) \to R) \not\equiv (\forall x \in A\ P(x)) \to R,$$

$$\exists\, x \in A\ (P(x) \to R) \not\equiv (\exists\, x \in A\ \ P(x)) \to R,$$

$$\forall x \in A\ (P(x) \leftrightarrow R) \not\equiv (\forall x \in A\ \ P(x)) \leftrightarrow R,$$

$$\exists\, x \in A\ (P(x) \leftrightarrow R) \not\equiv (\exists\, x \in A\ \ P(x)) \leftrightarrow R.$$

Действительно, пусть $R \equiv \mathbf{0}$, $P(x)$ = "$x = 0$", $A = \mathbf{R}$. Тогда $P(x) \to R \equiv$ "$x \neq 0$", и

$\forall\, x \in A\ (P(x) \to R) \equiv \forall\ x \in \mathbf{R}\ \ (x \neq 0)$ – ложно, а $(\forall\, x \in A\ \ P(x)) \to R \equiv$ $\equiv \overline{\forall\, x \in \mathbf{R}\,(x = 0)}\ \equiv \exists\, x \in \mathbf{R}\ x \neq 0$ – истинно.

$\exists\, x \in A\ (P(x) \to R) \equiv \exists\, x \in \mathbf{R}\ (x \neq 0)$ – истинно, а $(\exists\, x \in A\ \ P(x)) \to R \equiv$ $\equiv \overline{\exists\, x \in \mathbf{R}\,(x = 0)}\ \equiv \forall x \in \mathbf{R}\ x \neq 0$ – ложно.

$\forall\, x \in A\ (P(x) \leftrightarrow R) \equiv \forall\, x \in \mathbf{R}\ (x \neq 0)$ – ложно, а $(\forall\, x \in A\ \ P(x)) \leftrightarrow R \equiv$ $\equiv \overline{\forall\, x \in \mathbf{R}\,(x = 0)} \equiv \exists x \in \mathbf{R}\ x \neq 0$ – истинно.

$\exists\, x \in A\ (P(x) \leftrightarrow R) \equiv \exists\, x \in \mathbf{R}\ (x \neq 0)$ – истинно, а $(\exists\, x \in A\ P(x)) \leftrightarrow R \equiv$ $\equiv \overline{\exists\, x \in \mathbf{R}\,(x = 0)}\ \equiv \forall x \in \mathbf{R}\ x \neq 0$ – ложно.

Таким образом, при преобразовании формул нужно осторожно обращаться с кванторами там, где стоят логические связки импликации и эквивалентности.

5. Если предикат R зависит от x, то равносильности *(5)–(8)* могут быть не верны. Например,

$$(\forall x \in \mathbf{R}\ \ (x < y)) \vee (x = y) \equiv (x = y) \not\equiv \mathbf{0} \equiv \forall\, x \in \mathbf{R}\,((x < y) \vee (x = y)),$$

$$(\exists x \in \mathbf{N}\ \ (x < 1)) \vee (x = 1) \equiv (x = 1) \not\equiv \mathbf{1} \equiv \exists\, x \in \mathbf{N}\,((x < 1) \vee (x = 1)).$$

Примеры существенности условий теоремы для равносильностей *(6)–(8)* приведите самостоятельно.

§ 3. Язык исчисления предикатов

С помощью предикатов можно формулировать содержательные утверждения в различных областях знания. Поэтому важно дать средства построения осмысленных выражений с предикатами и приписывания им истинностных значений подобно тому, как это было сделано в исчислении высказываний.

Здесь возникает одна проблема: поскольку предикаты в разных областях знания совершенно разные, то при построении исчисления предикатов нужно отвлечься от специфики конкретных предикатов, рассматривая запись $P(x_1, \ldots, x_n)$ как абстрактный *символ предиката* P *от* n *переменных* $x_1, \ldots, x_n$, вместо которого в каждой науке можно подставлять те или иные её специфические предикаты от n переменных. Например, предикатный символ $P(x, y)$ географ может наполнить своим содержанием, рассматривая конкретный предикат $P(x, y)$ = "*река* x *впадает в море* y", а математик – своим, полагая $P(x, y)$ = "$x > y$".

Алфавит языка исчисления предикатов содержит несколько групп символов:

I. *Пропозициональные переменные:* $a, b, c_{99}, d_{345}, \ldots$ *для обозначения высказываний.*

II. *Объектные переменные:* $x, y, z_{99}, t_{345}, \ldots$ *для обозначения объектов предметной области той или иной науки.*

III. *Логические связки:* $\overline{\bullet}$ *– отрицание,* $\wedge$ *– конъюнкция,* $\vee$ *– дизъюнкция,* $\rightarrow$ *– импликация и* $\leftrightarrow$ *– эквивалентность.*

IV. *Предикатные символы:* $P^{(1)}(\_)$, $Q^{(1)}(\_)$, $R^{(1)}(\_), \ldots,$ $P^{(2)}(\_,\_)$, $Q^{(2)}(\_,\_)$, $R^{(2)}(\_,\_), \ldots$ *для обозначения предикатов от любого числа переменных (количество переменных, если это необходимо, указано в скобках в верхнем индексе).*

V. *Кванторы:* $\forall$ *– квантор всеобщности и* $\exists$ *– квантор существования.*

VI. *Служебные символы:* (,) *– скобки.*

Как и в языке исчисления высказываний, осмысленными фразами в языке исчисления предикатов будут *формулы*. Понятие *формулы языка исчисления предикатов* строится от простого к сложному с помощью следующих правил, в которых одновременно даётся определение *свободных и связанных вхождений объектных переменных*. Термин *вхождение объектной переменной* обозначает любое место в последовательности символов формулы, где встречается данная переменная:

(Ф1): *любая формула исчисления высказываний (от пропозициональных переменных) является формулой исчисления предикатов, в которой нет объектных переменных и кванторов.*

(Ф2): *если* $P^{(n)}(\_,\ldots,\_)$ *– предикатный символ от* n *переменных и* $x_1, \ldots, x_n$ *– объектные переменные, то* $P^{(n)}(x_1, \ldots, x_n)$ *– формула исчисления предикатов, в которой все вхождения объектных переменных* $x_1, \ldots, x_n$ *свободны, а вхождений других объектных переменных нет.*

(Ф3): *если* A *и* B *– две формулы, то* $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$, $\overline{A}$, $\overline{B}$ *– тоже формулы, в которых свободны все вхождения объектных переменных, свободные в* A *или в* B, *и связаны все вхождения объектных переменных, связанные в* A *или в* B.

(Ф4): *если* $A(x)$ *– формула* ***хотя бы с одним свободным вхождением объектной переменной*** x, *то выражения* $(\forall x\ A(x))$ *и* $(\exists x\ A(x))$ *– формулы, в которых связаны вхождения всех объектных переменных, связанных в* A, *а также все вхождения* x, *и свободны все вхождения объектных пере-*

менных, свободные в A, кроме переменной x. При этом формула $A(x)$ называется областью действия квантора.

(Ф5): *других формул нет.*

Будем называть объектную переменную в формуле *свободной (связанной)*, если свободны (связаны) все её вхождения в этой формуле.

Примеры: 1. Если a – пропозициональная переменная, то $(\exists x\,(P(x) \leftrightarrow a))$ – формула исчисления предикатов, образованная по правилу ***(Ф4)*** из формулы $(P(x) \leftrightarrow a)$ со свободным вхождением объектной переменной x. В полученной формуле $(\exists x\,(P(x) \leftrightarrow a))$ нет свободных вхождений объектных переменных.

2. $\forall x\ P(x) \rightarrow (\exists y\ Q(y))$ – не формула, т.к. в ней не хватает скобок.

3. $(\exists y\ (P(x) \vee (\forall y\ (Q(x) \rightarrow R(y)))))$ – не формула: в ней квантор $\exists$ навешивается на переменную y, у которой нет свободных вхождений.

4. $(\forall x\ ((\forall y\ Q(y)) \leftrightarrow (\exists x\ (Q(y) \wedge R(x)))))$ – не формула (?!), но $(\forall y\ ((\forall y\ Q(y)) \leftrightarrow (\exists x\ (Q(y) \wedge R(x)))))$ – формула, в которой нет свободных вхождений объектных переменных. Такие формулы называются *замкнутыми*.

5. $((\forall x\ P(x, y)) \vee Q(x, z))$ – формула, в которой свободно вхождение объектной переменной y, вхождение переменной x в формулу $(\forall x\ P(x, y))$ связано, а вхождение переменной x в формулу $Q(x, z)$ свободно, как и вхождение z.

6. $(\forall x\ ((\forall y\ Q(y, v)) \leftrightarrow (\exists z\ (Q(z, u) \wedge R(x, t)))))$ – формула со свободными переменными v, u, t.

7. $(\exists x\,(\forall y\,(Q(y, v) \leftrightarrow (\forall z\ Q(z, x)))))$ – формула со свободной переменной v.

В формулах примеров **1** и **4** нет свободных переменных, в формуле примера **5** свободна объектная переменная z, в формуле примера **6** – переменные v, u, t, а в формуле примера **6** – переменная v.

Как и ранее, ***будем опускать внешние скобки в записи формул***, остальные скобки в сложных формулах рекомендуется сохранять.

§ 4. Интерпретации формул исчисления предикатов

Уже в исчислении высказываний возникала ситуация, когда было невозможно однозначно говорить об истинности или ложности формулы: при одних значениях пропозициональных переменных эта формула может принимать значение *истина*, а при других – *ложь*. Только значения тождественно истинных или тождественно ложных формул не зависят от выбора набора значений их перемен-

ных. Таким образом, судить об истинности формулы исчисления высказываний можно, только фиксировав те или иные значения её переменных, т.е. выбрав ту или иную интерпретацию.

Ещё сложнее обстоит дело с формулами исчисления предикатов. Если рассмотреть какую-либо формулу исчисления предикатов, например, $(\exists\ x\ P(x, y))$, то $P(x, y)$ является не более чем символом, лишённым всякого содержания. Как отмечалось выше, географ может подставить вместо него предикат $\mathcal{P}(x, y)$ = "*город* x – *крупный научный центр области* y", а математик – $\mathcal{P}(x, y)$ = "$x \cdot y = 5$". Таким образом, возникают две различные интерпретации одной и той же формулы. В первом случае предметная область состоит из географических объектов (x – это города, y – области), а во втором случае она состоит из математических объектов (x и y – это числа). В каждом случае вместо предикатного символа используются различные конкретные предикаты, заданные на указанных предметных областях, и из одной формулы получаются интерпретации, совершенно не сопоставимые друг с другом.

Поэтому так же, как и для формул исчисления высказываний, невозможно говорить об истинности той или иной формулы исчисления предикатов: одна и та же формула может быть истинной при одной интерпретации и ложной при другой, даже если эти интерпретации имеют дело с одной и той же предметной областью. Например, формула $(\exists\ x\ P(x, y))$ истинна при любом y, если вместо $P(x, y)$ взять предикат $\mathcal{P}(x, y)$ = "$x + y = 5$" на $\boldsymbol{R}$: при $y = y_0$ она превращается в истинное высказывание $(\exists\ x\ x + y_0 = 5)$, т.к. достаточно взять $x = 5 - y_0$. Но та же формула будет принимать значение *ложь*, если на $\boldsymbol{R}$ рассмотреть предикат $\mathcal{P}(x, y)$ = "$x \cdot y = 5$": при $y = 0$ невозможно найти такое число x, что $x \cdot 0 = 5$.

Итак, при выяснении вопроса об истинностных значениях формул исчисления предикатов первостепенную роль играет понятие интерпретации. Перейдём теперь к точным определениям.

Пусть Φ – некоторое (конечное) множество формул исчисления предикатов, в записи которых участвуют пропозициональные переменные $a_1, \dots, a_m$, объектные переменные $x_1, \dots, x_n$, имеющие хотя бы одно свободное вхождение, предикатные символы $P_1^{(k_1)}(\_, \dots, \_), \dots, P_s^{(k_s)}(\_, \dots, \_)$ от $k_1, \dots, k_s$ аргументов. *Интерпретацией множества формул* Φ называется упорядоченный набор

$$\mathcal{J} = (M,\ a_1 = \alpha_1, \dots, a_m = \alpha_m,\ x_1 = o_1, \dots,\ x_n = o_n,\ \mathcal{P}_1^{(k_1)}(\_, \dots, \_), \dots, \mathcal{P}_s^{(k_s)}(\_, \dots, \_)),$$

где M – некоторое фиксированное множество – *предметная область интерпретации*, $\alpha_1, \ldots, \alpha_m$ – высказывания об элементах множества M (об объектах предметной области), $o_1, \ldots, o_n$ – фиксированные элементы множества M (объекты этой предметной области), а $\mathcal{P}_1^{(k_1)}(\_,\ldots,\_), \ldots, \mathcal{P}_s^{(k_s)}(\_,\ldots,\_)$ – фиксированные предикаты от $k_1, \ldots, k_s$ аргументов, заданные на предметной области M. Следует отметить, что одна предметная переменная может иметь, вообще говоря, несколько свободных вхождений в одной формуле, для каждого из которых в интерпретации должно быть зарезервировано своё значение.

При заданной интерпретации каждая из формул $A \in \Phi$ превращается в высказывание A_J после замены всех входящих в неё пропозициональных переменных a_i на высказывания α_i $(1 \le i \le m)$, свободных вхождений объектных переменных x_j – на объекты o_j $(1 \le j \le n)$, переменных, связанных кванторами, – на переменные, пробегающие множество M, связанные теми же кванторами, а всех предикатных символов $P_l^{(k_l)}(\_,\ldots,\_)$ – на предикаты $\mathcal{P}_l^{(k_l)}(\_,\ldots,\_)$ $(1 \le l \le s)$. При этом все кванторные приставки вида $\exists x$ или $\forall x$ заменяются на выражения $\exists x \in M$ и $\forall x \in M$ соответственно. Полученное высказывание имеет истинностное значение 0 или 1, которое называется *значением истинности данной формулы* <u>*при данной интерпретации*</u>.

Примеры: 1. Для одной формулы $A = (\forall x\ P(x)) \vee Q(x)$ можно рассмотреть следующую интерпретацию: $J = (M = \mathbf{N},\ x = 1,\ P = \mathcal{P}(\_),\ Q = Q(\_))$, где предикаты $\mathcal{P}(\_)$, $Q(\_)$ от одного переменного заданы на множестве $\mathbf{N}$ так: $\mathcal{P}(n)$ = "$n = 2$", $Q(n)$ = "n – *нечётно*". В данном случае не нужно задавать высказывания, т.к. в формуле нет пропозициональных переменных. Для свободного вхождения объектной переменной x в этой интерпретации зарезервирован объект $1 \in \mathbf{N}$. Получаем значение формулы в данной интерпретации

$$A_J = (\forall x \in \mathbf{N}\ (x = 2)) \vee (1 - \textit{нечётно}) = 1.$$

2. Для формулы A примера **1** можно рассмотреть и другую интерпретацию, переставив предикаты $\mathcal{P}(\_)$ и $Q(\_)$: $I = (M = \mathbf{N},\ x = 1,\ P = Q(\_),\ Q = \mathcal{P}(\_))$. В этой интерпретации I формула имеет значение *ложь*:

$$A_I = (\forall x \in \mathbf{N}\ (x - \textit{нечётно})) \vee (1 = 2)) = 0.$$

3. Рассмотрим формулу $\Phi = a \wedge (\exists x\ (P(x, y) \leftrightarrow Q(x, y)))$ и интерпретацию:

$$J = (M = \{0, 1\},\ a = \text{"}0 \le 1\text{"},\ y = 1,\ P = \mathcal{P}(\_\ ,\_\ ),\ Q = Q(\_\ ,\ \_\ )),$$

где "$0 \le 1$" – высказывание об элементах множества M, 1 – фиксированный объект множества M, а предикаты $\mathcal{P}(\_\ ,\_\ )$, $Q(\_\ ,\ \_\ )$ от двух аргументов за-

даны на M следующим образом: $P(u, v)$ = “$u \cdot v = 1$”, $Q(u, v)$ = “$u = v$”. В этой интерпретации значение формулы таково:

$$\Phi_J = \text{“}0 \le 1\text{”} \wedge (\exists\, x \in \{0, 1\}\ ((x \cdot 1 = 1) \leftrightarrow (x = 1))) = 1.$$

4. Ещё одна интерпретация для формулы предыдущего примера:

$$I = (M = \{0, 1\},\ a = \text{“}0 \cdot 0 = 1 \cdot 1\text{”},\ y = 0,\ P = P(\_\ ,\_\ ),\ Q = Q(\_\ ,\ \_\ ))$$

с теми же предикатами. В этой интерпретации формула превращается в высказывание Φ_I = “$0 \cdot 0 = 1 \cdot 1$” $\wedge$ $(\exists\ x \in M\ ((x \cdot 0 = 1) \leftrightarrow (x = 0)))$, которое ложно, поскольку ложно высказывание “$0 \cdot 0 = 1 \cdot 1$”. Следует отметить, что высказывание $\exists\, x \in M\ ((x \cdot 0 = 1) \leftrightarrow (x = 0))$ истинно, т.к. при $x = 1$ верно $(1 \cdot 0 = 1) \leftrightarrow (1 = 0)$ – оба аргумента эквивалентности ложны.

5. Если рассмотреть интерпретацию

$$K = (M = \{0, 1\},\ a = \text{“}0 \cdot 0 = 1 \cdot 0\text{”},\ y = 0,\ P = P(\_\ ,\_\ ),\ Q = Q(\_\ ,\ \_\ )),$$

то формула примера **3** имеет значение

$$\Phi_K = \text{“}0 \cdot 0 = 1 \cdot 0\text{”} \wedge (\exists\, x \in M\ ((x \cdot 0 = 1) \leftrightarrow (x = 0))) = 1,$$

т.к. оба высказывания “$0 \cdot 0 = 1 \cdot 0$” и $(\exists\, x \in M\ ((x \cdot 0 = 1) \leftrightarrow (x = 0)))$ истинны.

6. Интерпретация формулы $\Phi(a_1, \ldots, a_n)$ исчисления высказываний имеет вид $J = (M,\ a_1 = \alpha_1, \ldots, a_n = \alpha_n)$, где M – некоторое множество, а $\alpha_1, \ldots, \alpha_n$ – высказывания об элементах этого множества, подставляемые вместо пропозициональных переменных $a_1, \ldots, a_n$. По существу она совпадает с прежней интерпретацией $\varepsilon = (\varepsilon_1; \ldots; \varepsilon_n)$, где ε_i – значение истинности для высказывания α_i $(1 \le i \le n)$. Таким образом, введённое более общее понятие интерпретации формул исчисления предикатов согласуется с использованным ранее понятием интерпретации формул исчисления высказываний.

Ясно, что при любой интерпретации значением $\Phi(\alpha_1, \ldots, \alpha_n)$ тождественно истинной формулы исчисления высказываний будет 1, а значение тождественно ложной формулы будет равно 0. В то же время выполнимые формулы исчисления высказываний могут при разных интерпретациях принимать различные значения. Например, выполнимая формула $(a \wedge b)$ принимает значение 1 при интерпретации $J = (M = \{0, 1\},\ a = \text{“}0 = 0\text{”},\ b = \text{“}1 = 1\text{”})$, и имеет значение 0 при интерпретации $I = (M = \{0, 1\},\ a = \text{“}0 \ne 0\text{”},\ b = \text{“}1 = 1\text{”})$.

Теперь можно ввести классификацию формул, аналогичную той, которая была использована для формул исчисления высказываний.

Формула исчисления предикатов называется *тождественно истинной (или общезначимой)*, если она принимает значение 1 в любой интерпретации. Фор-

мула называется *тождественно ложной (или противоречием)*, если она принимает значение *0* при любой интерпретации. Если формула не тождественно истинна и не тождественно ложна, то она называется *выполнимой*.

Две формулы исчисления предикатов называются *равносильными*, если они принимают одинаковые значения при любой интерпретации этой пары формул.

Примеры: 1. Любой закон логики исчисления высказываний является общезначимой формулой, а любая тождественно ложная формула исчисления высказываний – противоречием.

2. Формула $\forall x\ (P(x) \to Q(x))$, рассмотренная выше, выполнима, т.к. в одних интерпретациях принимает значение *1*, а в других – значение *0*.

3. Формула $\overline{(\forall x\, P(x))} \leftrightarrow (\exists x\ \overline{P}(x))$ общезначима. Это следует из того, что при любой интерпретации $\mathcal{J} = (M,\ P = \mathcal{P}(\_))$ значением этой формулы будет высказывание $\overline{(\forall x \in M\ \mathcal{P}(x))} \leftrightarrow (\exists x \in M\ \overline{\mathcal{P}}(x))$, которое истинно ввиду доказанных ранее равносильностей с предикатами и кванторами.

4. Из **3** следует (?!), что $\overline{(\forall x\, P(x))} \equiv (\exists x\ \overline{P}(x))$.

5. Основные равносильности с кванторами дают примеры равносильных формул, если исключить из них отношения принадлежности переменных множествам и вместо предикатов рассматривать предикатные символы. Например, равносильность $\forall x \in A\ (P(x, \mathbf{y}) \wedge Q(x, \mathbf{y})) \equiv (\forall x \in A\ P(x, \mathbf{y})) \wedge (\forall x \in A\ Q(x, \mathbf{y}))$ даёт равносильные формулы $\forall x\ (P(x, \mathbf{y}) \wedge Q(x, \mathbf{y})) \equiv (\forall x\ P(x, \mathbf{y})) \wedge (\forall x\ Q(x, \mathbf{y}))$.

Действительно, если рассмотреть любую интерпретацию

$$\mathcal{J} = (M, y_1 = o_1, \dots, y_n = o_n,\ P = \mathcal{P}^{(n+1)}(\_, \dots, \_),\ Q = Q^{(n+1)}(\_, \dots, \_)),$$

то $\forall x \in M\ (\mathcal{P}(x, \mathbf{y}) \wedge Q(x, \mathbf{y})) \equiv (\forall x \in M\ \mathcal{P}(x, \mathbf{y})) \wedge (\forall x \in M\ Q(x, \mathbf{y}))$ по теореме об основных равносильностях с кванторами, а значит

$$(\forall x\ (P(x, \mathbf{y}) \wedge Q(x, \mathbf{y})))_{\mathcal{J}} = ((\forall x\ P(x, \mathbf{y})) \wedge (\forall x\ Q(x, \mathbf{y})))_{\mathcal{J}}.$$

6. Для любой формулы исчисления предикатов существует равносильная ей формула, в которой каждая объектная переменная либо свободна, либо связана, т.е. любая переменная не может иметь двух вхождений, в одном из которых она свободна, а в другом – связана.

Для доказательства достаточно, пользуясь утверждением *(0)* из теоремы об основных равносильностях с кванторами заменить все вхождения связанных переменных в области действия связывающего их квантора на вхождения уникальных переменных (не встречающихся в других местах формулы), связанных теми же кванторами с теми же областями действия. Например,

$$P(x, y, z) \to ((\exists x\ Q(x, z)) \vee (\forall z\ P(x, y, z))) \equiv$$

$$\equiv P(x, y, z) \to ((\exists\, u\, Q(u, z)) \vee (\forall v\, P(x, y, v))).$$

В последней формуле переменные x, y, z свободны, а u и v – связаны.

7. Формула Φ общезначима тогда и только тогда, когда $\overline{\Phi}$ тождественно ложна.

8. Формула $\forall x\, (\exists y\ P(x, y))$ выполнима. В самом деле, её значение 1 при интерпретации $(\boldsymbol{N},\ P = \mathcal{P}(\_\ ,\ \_\ ))$, где $\mathcal{P}(x\ , y) =$ "$x < y$", и значение 0 – при интерпретации $(\boldsymbol{N},\ P = Q(\_\ ,\ \_\ ))$, где $Q(x\ , y) =$ "$x > y$". Действительно, значением при первой интерпретации будет $(\forall x \in \boldsymbol{N}\, (\exists y \in \boldsymbol{N}\ \ (x < y))) = 1$ – высказывание, выражающее факт неограниченности натурального ряда. А её значение при второй интерпретации $(\forall x \in \boldsymbol{N}\, (\exists y \in \boldsymbol{N}\ \ (x > y))) = 0$, поскольку при $x = 1$ найти меньший элемент $y \in \boldsymbol{N}$ невозможно.

Можно ввести и понятие логического следования для формул исчисления предикатов: говорят, что *формула* A *является логическим следствием формул* $A_1\ , \ldots\ , A_n$ (пишут $A_1\ , \ldots\ , A_n \models A$), если для любой интерпретации множества формул $\Phi = \{A_1\ , \ldots\ , A_n\ , A\}$, в которой все формулы-*посылки* $A_1\ , \ldots\ , A_n$ принимают значение *истина*, формула-*заключение* A также принимает значение *истина*. Если нет ни одной интерпретации, в которой все формулы $A_1\ , \ldots\ , A_n$ принимают значение *истина*, то A считается логическим следствием формул $A_1\ , \ldots\ , A_n$ по определению. Как и для формул исчисления высказываний, используется и запись вида $\Gamma \models A$, где $\Gamma = \{A_1\ , \ldots\ , A_n\ \}$. В случае $\Gamma = \varnothing$ запись $\models A$ означает, что формула A общезначима. Легко понять, что введённые понятия согласуются с соответствующими понятиями для формул исчисления высказываний.

Теорема (критерий логического следования). $A_1\ , \ldots\ , A_n \models A$ *тогда и только тогда, когда формула* $(A_1 \wedge \ldots \wedge A_n \to A)$ *тождественно истинна.*

Доказательство. Если $A_1\ , \ldots\ , A_n \models A$, то при любой интерпретации множества формул $\Phi = \{A_1\ , \ldots\ , A_n\ , A\}$, в которой все формулы-посылки $A_1\ , \ldots\ , A_n$ принимают значение *истина*, формула-заключение A также принимает значение *истина*. Поэтому формула $(A_1 \wedge \ldots \wedge A_n \to A)$ принимает значение *истина* для любой интерпретации, при которой значение *истина* принимает формула $(A_1 \wedge \ldots \wedge A_n)$. Если же интерпретация такова, что формула $A_1 \wedge \ldots \wedge A_n$ принимает значение *ложь*, то импликация $(A_1 \wedge \ldots \wedge A_n \to A)$ в этой интерпретации всё равно принимает значение *истина*. Таким образом, эта формула-импликация

принимает значение *истина* при любой интерпретации, т.е. она тождественно истинна.

Обратно, если формула $(A_1 \wedge \ldots \wedge A_n \to A)$ имеет значение *истина* при любой интерпретации, то при интерпретации множества $\Phi = \{A_1, \ldots, A_n, A\}$, в которой все формулы-посылки $A_1, \ldots, A_n$ принимают значение *истина*, будет истинна и конъюнкция $A_1 \wedge \ldots \wedge A_n$. Поэтому из истинности в этой интерпретации импликации $(A_1 \wedge \ldots \wedge A_n \to A)$ получим истинность в рассматриваемой интерпретации и формулы A, т.е. логическое следование $A_1, \ldots, A_n \models A$ имеет место.

Теорема доказана.

Теорема (о дедукции). *Для любого множества формул Γ и формул A, B условие $\Gamma, A \models B$ выполнено тогда и только тогда, когда $\Gamma \models A \to B$.*

Доказательство. Если $\Gamma = \varnothing$, то $A \models B \Leftrightarrow (A \to B$ *тождественно истинна)* $\Leftrightarrow \models A \to B$.

Если $\Gamma = \{A_1, \ldots, A_n\} \neq \varnothing$, то $\Gamma, A \models B \Leftrightarrow (A_1 \wedge \ldots \wedge A_n \wedge A \to B$ *тождественно истинна)* $\Leftrightarrow$ $(A_1 \wedge \ldots \wedge A_n \to (A \to B)$ *тождественно истинна)* $\Leftrightarrow$ $\Leftrightarrow \Gamma \models A \to B$. Здесь использованы равносильности

$$(A_1 \wedge \ldots \wedge A_n \wedge A \to B) \equiv \overline{A_1 \wedge \ldots \wedge A_n \wedge A} \vee B \equiv \overline{A_1 \wedge \ldots \wedge A_n} \vee \overline{A} \vee B \equiv$$

$$\equiv \overline{A_1 \wedge \ldots \wedge A_n} \vee (A \to B) \equiv A_1 \wedge \ldots \wedge A_n \to (A \to B).$$

Теорема доказана.

Примеры: 1. $(\forall x\ A(x)) \models A(y)$, где переменная y не совпадает с x.

Рассмотрим произвольную интерпретацию формулы $((\forall x\ A(x)) \to A(y))$:

$$\mathcal{J} = (M,\ a_1 = \alpha_1, \ldots, a_m = \alpha_m,\ x_1 = o_1, \ldots,\ x_n = o_n,\ \mathcal{P}_1^{(k_1)}(\_, \ldots, \_), \ldots, \mathcal{P}_s^{(k_s)}(\_, \ldots, \_)),$$

Если значение формулы $(\forall x\ A(x))$ в этой интерпретации ложно: $(\forall x\ A(x))_{\mathcal{J}} = 0$, то значение формулы-импликации истинно. Если же $(\forall x\ A(x))_{\mathcal{J}} = 1$, то для любого объекта $u \in M$ верно $A(u)_{\mathcal{J}} = 1$, в частности, это верно и для $u = o$, т.е. $A(y)_{\mathcal{J}} = A(o)_{\mathcal{J}} = 1$. Поэтому рассматриваемая формула-импликация принимает в интерпретации $\mathcal{J}$ значение *истина*, т.е. является тождественно истинной. Значит, логическое следование $(\forall x\ A(x)) \models A(y)$ имеет место.

2. Докажите, что $A(y) \models (\exists x\ A(x))$, где переменная y не совпадает с x.

3. $(A(x) \to B) \models ((\exists x\ A(x)) \to B)$, где формула B не зависит от x.

Рассмотрим любую интерпретацию

$\mathcal{J} = (M,\ a_1 = \alpha_1, \ldots, a_m = \alpha_m,\ x_1 = o_1, \ldots,\ x_n = o_n,\ \mathcal{P}_1^{(k_1)}(\_,\ldots,\_), \ldots, \mathcal{P}_s^{(k_s)}(\_,\ldots,\_))$,

формулы $(A(x) \to B) \to ((\exists x\ A(x)) \to B)$. Если значение формулы $A(x) \to B$ в этой интерпретации ложно, то значение рассматриваемой формулы-импликации истинно. Если же $(A(x) \to B)_{\mathcal{J}} = 1$, то истинно и значение импликации $((\exists x\ A(x)) \to B)$, т.к. можно взять $x = o$, а значит, истинно и значение всей рассматриваемой формулы-импликации $(A(x) \to B) \to ((\exists x\ A(x)) \to B)$. Поэтому логическое следование $(A(x) \to B) \models ((\exists x\ A(x)) \to B)$ имеет место.

4. Условие на формулу B в примере **3** существенно. Например, если $B = A(x)$, то формула $A(x) \to B$ тождественно истинна, но импликация $(\exists x\ A(x)) \to A(x)$ принимает значение *истина* не всегда: например, если $\mathcal{J} = (M = \mathbf{Z},\ x = -1,\ A = (x > 0))$, то эта формула превращается в ложное высказывание $(\exists x \in \mathbf{Z}\ (x > 0)) \to (-1 > 0)$.

5. Докажите, что $(B \to A(x)) \models (B \to (\forall x\ A(x)))$, где B не зависит от x.

Точно так же, как для исчисления высказываний, можно рассматривать *правила логического вывода для исчисления предикатов*.

Например, предыдущие примеры доказывают следующие правила логического вывода с предикатами:

$\dfrac{C \to A(x)}{C \to (\forall x\ A(x))}$ *(введение квантора* $\forall$*)*, $\dfrac{A(x) \to C}{(\exists x\ A(x)) \to C}$ *(введение квантора* $\exists$*)*,

где C *не содержит вхождений переменной* x.

Упражнение: Придумайте несколько других правил логического вывода с кванторами в исчислении предикатов.

§ 5. Приведённая и предварённая нормальные формы

По аналогии с исчислением высказываний, найдём некоторую нормальную форму, к которой можно равносильными преобразованиями привести любую формулу исчисления предикатов.

С помощью известных основных равносильностей $(A \to B) \equiv (\overline{A} \vee B)$ и $(A \leftrightarrow B) \equiv ((A \wedge B) \vee (\overline{A} \wedge \overline{B}))$ в произвольной формуле исчисления предикатов можно избавиться от всех логических связок $\to$ и $\leftrightarrow$. Затем, по законам де Моргана $\overline{(A \wedge B)} \equiv \overline{A} \vee \overline{B}$, $\overline{(A \vee B)} \equiv \overline{A} \wedge \overline{B}$, правилу двойного отрица-

ния $\overline{\overline{A}} \equiv A$ и равносильностям с кванторами $\overline{(\forall x\ P(x, \mathbf{y}))} \equiv (\exists x\ \overline{P}(x, \mathbf{y}))$, $\overline{(\exists x\ P(x, \mathbf{y}))} \equiv (\forall x\ \overline{P}(x, \mathbf{y}))$ можно переработать все "длинные" отрицания (т.е. отрицания, стоящие над формулами, не являющимися пропозициональными переменными и предикатными символами) в "короткие", добившись, чтобы отрицания стояли только над пропозициональными переменными или над предикатными символами.

Полученный вид формулы называется *приведённым* или *приведённой формой (ПФ)*. Таким образом, доказана следующая

Теорема (о ПФ). *Любая формула исчисления предикатов равносильна некоторой приведённой форме.*

Примеры: 1. $(\forall x\ (\exists y\ (P(y) \to Q(x)))) \equiv (\forall x\ (\exists y\ (\overline{P}(y) \vee Q(x)))) - ПФ.$

2. $(\forall y\ \overline{((\exists x\ P(x)) \to Q(x, y))}) \equiv (\forall y\ \overline{(\overline{(\exists x\ P(x))} \vee Q(x, y))}) \equiv$

$$\equiv (\forall y\ ((\exists x\ P(x)) \wedge \overline{Q}(x, y))) - ПФ.$$

3. $(P(x, y) \to \overline{((\exists z\ Q(z)) \leftrightarrow R(x))}) \equiv$

$$\equiv (\overline{P}(x, y) \vee (\overline{((\exists z\ Q(z)) \wedge R(x)) \vee (\overline{(\exists z\ Q(z))} \wedge \overline{R(x)})})) \equiv$$

$$\equiv (\overline{P}(x, y) \vee (((\forall z\ \overline{Q}(z)) \vee \overline{R}(x)) \wedge ((\exists z\ Q(z)) \vee R(x)))) - ПФ.$$

Говорят, что формула исчисления предикатов находится в *предварённой нормальной форме (ПНФ)*, если она либо не содержит кванторов, либо имеет следующий вид: $Q_1 x_1\ (Q_2 x_2\ (\ldots\ (Q_n x_n\ \Phi(x_1, \ldots, x_n)))\ldots)$, где Q_i – один из кванторов $\forall$ или $\exists$ $(1 \le i \le n)$, формула Φ бескванторная и может зависеть от других переменных, кроме $x_1, \ldots, x_n$. Иными словами, кванторы в *ПНФ* предшествуют её бескванторной подформуле Φ и область действия каждого квантора распространяется до конца формулы (не учитывая закрывающие скобки).

Если формула является *ПНФ* и приведена, то говорят, что она находится в *предварённой приведённой нормальной форме (ППНФ)*.

Примеры: 1. $(P(x) \wedge Q(y))$ – бескванторная формула в *ПНФ* и *ППНФ*.

2. $(\forall x\ (\exists y\ (P(y) \to Q(x)))) -$ *ПНФ*, но не *ППНФ*.

3. $(\forall x\ ((\exists y\ P(y)) \to Q(x))) -$ не *ПНФ*, т.к. область действия квантора $\exists$ распространяется только на $P(x)$, а не до конца формулы.

4. $(P(z, y) \vee (\forall x\ Q(x)))$ – не *ПНФ*, т.к. квантор $\forall$ не предшествует подформуле $P(z, y)$.

Теорема (о ППНФ). *Любая формула исчисления предикатов равносильна некоторой предварённой приведённой нормальной форме.*

Доказательство. Будем исследовать формулы в процессе их создания по правилам образования формул ***(Ф1)-(Ф5)*** и приводить их к *ППНФ*.

Во-первых, любая бесквантворная формула сама находится в *ПНФ* и равносильна некоторой приведённой форме ввиду предыдущей теоремы. Таким образом, любая формула, возникшая по правилам ***(Ф1)***, ***(Ф2)***, обладает *ППНФ*.

Во-вторых, если для формул A и B уже найдены равносильные им *ППНФ*:

$$A \equiv Q_1\ x_1\ (Q_2\ x_2\ (\dots\ (Q_n\ x_n\ C(x_1, \dots, x_n))\dots)),$$

$$B \equiv \mathcal{R}_1\ y_1\ (\mathcal{R}_2\ y_2\ (\dots\ (\mathcal{R}_m\ y_m\ D(y_1, \dots, y_m))\dots)) = \Psi,$$

где Q_i, $\mathcal{R}_j$ – один из кванторов $\forall$ или $\exists$ $(1 \le i \le n,\ 1 \le j \le m)$, то (как уже отмечалось выше) связанные переменные в этих формулах можно переобозначить уникальными буквами так, чтобы в формуле для A не было одинаковых связанных переменных с формулой для B и чтобы все связанные переменные отличались от свободных. Найдём *ППНФ*, равносильную формулам $\overline{A}$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$.

Для $\overline{A}$ воспользуемся равносильностями *(2)*, теоремы об основных равносильностях с кванторами:

$$\overline{A} \equiv \overline{(Q_1\ x_1\ (Q_2\ x_2\ (\dots(Q_n\ x_n\ C(x_1,\dots,x_n))\dots)))} \equiv$$
$$\equiv \overline{(Q_1}\ x_1\ \overline{(Q_2}\ x_2\ \overline{(\dots(Q_n}\ x_n\ C(x_1,\dots,x_n))\dots)) \equiv$$
$$\equiv (Q_1\ x_1\ (Q_2\ x_2\ (\dots(Q_n\ x_n\ C(x_1,\dots,x_n))\dots))) \equiv \dots$$
$$\dots \equiv (Q_1\ x_1\ (Q_2\ x_2\ (\dots(Q_n\ x_n\ \overline{C(x_1,\dots,x_n)})\dots))),$$

где $\overline{Q_i}$ – кванторы, противоположные кванторам Q_i $(1 \le i \le n)$. Последняя формула в этой цепочке – *ПНФ* – является искомой. Остаётся привести её к приведённому виду, избавившись от "длинных" отрицаний в бесквантворной формуле. Таким образом, $\overline{A}$ обладает равносильной *ППНФ*.

Для остальных формул вида $(A\ \omega B)$, где $\omega \in \{\wedge, \vee\}$ рассуждения однотипны и используют равносильности *(5)*, *(6)* теоремы об основных равносильностях с кванторами (следует учесть, что все связанные переменные уникальны, так что условия для применения равносильностей *(5)*, *(6)* выполнены): $(A\ \omega B) \equiv$

$$\equiv ((Q_1\ x_1\ (\dots(Q_n\ x_n\ C(x_1, \dots, x_n))\dots))\ \omega\ (\mathcal{R}_1\ y_1\ (\dots(\mathcal{R}_m\ y_m\ D(y_1, \dots, y_m))\dots))) =$$
$$= ((Q_1\ x_1\ (Q_2\ x_2\ (\dots\ (Q_n\ x_n\ C)\dots)))\ \omega\ \Psi) \equiv (Q_1\ x_1\ ((Q_2\ x_2\ (\dots\ (Q_n\ x_n\ C))\dots))\ \omega\ \Psi)) \equiv$$
$$\equiv (Q_1\ x_1\ (Q_2\ x_2\ ((\dots\ (Q_n\ x_n\ C)\dots))\ \omega\ \Psi))) \equiv \dots$$
$$\dots \equiv (Q_1\ x_1\ (Q_2\ x_2\ (\dots(Q_n\ x_n\ (C\ \omega\ \Psi))\dots))) \equiv (Q_1\ x_1\ (Q_2\ x_2\ (\dots(Q_n\ x_n\ (\Psi\ \omega\ C))\dots))) \equiv$$

$$\equiv (Q_1 x_1 (Q_2 x_2 (\dots (Q_n x_n \ ((\mathcal{R}_1 y_1 (\mathcal{R}_2 y_2 (\dots (\mathcal{R}_m y_m \ D)\dots))) \ \omega \ C))\dots))) \ \equiv$$

$$\equiv (Q_1 x_1 (Q_2 x_2 (\dots (Q_n x_n \ (\mathcal{R}_1 y_1 ((\mathcal{R}_2 y_2 (\dots (\mathcal{R}_m y_m \ D)\dots)) \ \omega \ C)))\dots))) \ \equiv$$

$$\equiv (Q_1 x_1 (Q_2 x_2 (\dots (Q_n x_n \ (\mathcal{R}_1 y_1 (\mathcal{R}_2 y_2 ((\dots (\mathcal{R}_m y_m \ D)\dots) \ \omega \ C))))\dots))) \equiv \dots$$

$$\dots \equiv (Q_1 x_1 (Q_2 x_2 (\dots (Q_n x_n \ (\mathcal{R}_1 y_1 (\mathcal{R}_2 y_2 (\dots (\mathcal{R}_m y_m \ (D \ \omega \ C))\dots))))\dots))),$$

и последняя формула является *ППНФ*.

Связки $\rightarrow$ и $\leftrightarrow$ выражаются через $\wedge$, $\vee$, $\overline{\bullet}$, так что для формул вида $(A \rightarrow B)$ и $(A \leftrightarrow B)$ существование *ППНФ* следует из предыдущего.

Таким образом, все формулы, полученные по правилу ***(Ф3)*** образования формул, обладают *ППНФ*.

Наконец, если $A(x)$ – формула со свободной переменной x, которая уже равносильна некоторой *ППНФ*:

$$A(x) \equiv (Q_1 \ x_1 (Q_2 \ x_2 (\dots (Q_n \ x_n \ C(x, \ x_1 , \dots , x_n))\dots))),$$

где $Q_i \ (1 \le i \le n)$ – один из кванторов $\forall$ или $\exists$, то формула $(Q \ x \ A(x))$, очевидно, равносильна формуле $(Q \, x \, (Q_1 \ x_1 (Q_2 \ x_2 (\dots (Q_n \ x_n \ C(x, \ x_1 , \dots , x_n))\dots))))$ – *ППНФ*. Таким образом, любая формула обладает равносильной *ППНФ*.

Теорема доказана.

Примеры: 1. $(\forall x ((\exists y \, P(y)) \rightarrow Q(y, x))) \equiv (\forall x (\overline{(\exists \, y \, P(y))} \vee Q(y, x))) \equiv$

$$\equiv (\forall x ((\forall y \ \overline{P} \ (y)) \vee \ Q(y, x))) \equiv (\forall x ((\forall z \ \overline{P} \ (z)) \vee \ Q(y, x))) \equiv$$

$$\equiv (\forall x (\forall z (\overline{P} \ (z) \vee \ Q(y, x)))) \ - \ ППНФ.$$

2. $(P(u, y) \wedge (\forall \ y \ \ Q(y))) \equiv (P(u, y) \wedge (\forall \ z \ \ Q(z))) \equiv$

$$\equiv ((\forall \ z \ \ Q(z)) \wedge P(u, y)) \equiv (\forall \ z \, (Q(z) \wedge P(u, y))) - \ ППНФ.$$

3. $((\exists x \, R(x, y, z)) \rightarrow \overline{(\forall \ x \, Q(x, \ y))}) \equiv ((\exists x \, R(x, y, z)) \rightarrow (\exists x \ \overline{Q} \ (x, y))) \equiv$

$$\equiv (\overline{(\exists \ x \, R(x, y, z))} \vee (\exists t \ \overline{Q} \ (t, y))) \equiv ((\forall x \ \overline{R} \ (x, y, z)) \vee (\exists t \ \overline{Q} \ (t, y))) \ \equiv$$

$$\equiv (\forall x \ (\overline{R} \ (x, y, z) \vee (\exists t \ \overline{Q} \ (t, y)))) \equiv (\forall x (\exists t (\overline{R} \ (x, y, z) \vee \overline{Q} \ (t, y)))) - ППНФ.$$

4. $((\forall x \ P(x, y)) \vee ((\exists x \ P(x, x)) \rightarrow (\forall z \ \overline{(Q(y, z) \rightarrow (\exists \ x \, P(x, z)))})) \equiv$

$$\equiv ((\forall x \ P(x, y)) \vee ((\exists x \ P(x, x)) \rightarrow (\forall z \ \overline{(\overline{Q(y, z)} \vee (\exists \ x \, P(x, z)))})) \ \equiv$$

$$\equiv ((\forall x \ P(x, y)) \vee ((\exists x \ P(x, x)) \rightarrow (\forall z \ (Q(y, z) \wedge \ \overline{(\exists \ x \, P(x, z))}))) \ \equiv$$

$$\equiv ((\forall x \ P(x, y)) \vee ((\exists x \ P(x, x)) \rightarrow (\forall z \ (Q(y, z) \wedge (\forall x \ \overline{P} \ (x, z)))))) \ \equiv$$

$$\equiv ((\forall x \ P(x, y)) \vee ((\exists u \ P(u, u)) \rightarrow (\forall z \ (Q(y, z) \wedge (\forall v \ \overline{P} \ (v, z)))))) \ \equiv$$

$$\equiv ((\forall x \ P(x, y)) \vee ((\exists u \, P(u, u)) \rightarrow (\forall z \ (\forall v \, (Q(y, z) \wedge \overline{P} \ (v, z)))))) \ \equiv$$

$$\equiv ((\forall x\ P(x,y)) \vee ((\forall u\ \overline{P}(u,u)) \vee (\forall z\ (\forall v\,(Q(y,z) \wedge \overline{P}(v,z)))))) \equiv$$

$$\equiv ((\forall x\ P(x,y)) \vee (\forall z\,((\forall u\ \overline{P}(u,u)) \vee (\forall v\,(Q(y,z) \wedge \overline{P}(v,z)))))) \equiv$$

$$\equiv ((\forall x\ P(x,y)) \vee (\forall z\,(\forall v\,((\forall u\ \overline{P}(u,u)) \vee (Q(y,z) \wedge \overline{P}(v,z)))))) \equiv$$

$$\equiv ((\forall x\ P(x,y)) \vee (\forall z\,(\forall v\,(\forall u\,(\overline{P}(u,u) \vee (Q(y,z) \wedge \overline{P}(v,z))))))) \equiv$$

$$\equiv (\forall z\,((\forall x\ P(x,y)) \vee (\forall v\,(\forall u\,(\overline{P}(u,u) \vee (Q(y,z) \wedge \overline{P}(v,z))))))) \equiv$$

$$\equiv (\forall z\,(\forall v\,((\forall x\ P(x,y)) \vee (\forall u\,(\overline{P}(u,u) \vee (Q(y,z) \wedge \overline{P}(v,z))))))) \equiv$$

$$\equiv (\forall z\,(\forall v\,(\forall u\,((\forall x\ P(x,y)) \vee (\overline{P}(u,u) \vee (Q(y,z) \wedge \overline{P}(v,z))))))) \equiv$$

$$\equiv (\forall z\,(\forall v\,(\forall u\,(\forall x\ (P(x,y) \vee (\overline{P}(u,u) \vee (Q(y,z) \wedge \overline{P}(v,z)))))))) - \text{ППНФ}.$$

§ 6. О структуре современных математических теорий

Очень кратко, не претендуя на полноту, опишем лишь основные черты, присущие всем математическим теориям на современном этапе развития.

Фундаментом любой математической теории служат три нераздельные и единосущные дисциплины: логика, теория множеств и арифметика. Невозможно отделить корни ни одной из этих наук от корней двух других, хотя, конечно, в процессе развития их ветви разрослись вширь, а кроны раскинулись далеко и независимо друг от друга.

В самом деле, законы логики используются во всех математических дисциплинах, в доказательствах любых утверждений и формулировках любых математических теорий. Без логики, таким образом, не обойдутся ни теория множеств, ни арифметика. С другой стороны, конструируя язык исчисления высказываний, мы неявно пользовались языком множеств, например, рассматривая бесконечное множество пропозициональных переменных. На самом деле, существование бесконечного множества далеко не очевидно и гарантируется так называемой аксиомой бесконечности теории множеств. Так что логика неявно использует аппарат теории множеств. Точно так же, основа арифметики – аксиоматика Пеано, – как будет показано ниже, явно обращается в аксиоме индукции к понятию множества. Поэтому нет арифметики без теории множеств. Наконец, без арифметики невозможно определить понятие формулы в любой содержательной аксиоматической теории. Например, понятие формулы исчисления высказываний вводилось нами фактически с помощью индукции по длине формулы: вначале были определены некоторые формулы длины *1* – пропозициональные переменные, а затем по заданным формулам A и B строились более сложные формулы большей длины

$(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$ и формула той же длины $\overline{A}$. Другой пример использования арифметики – это нумерация объектов математической теории. Так, используя пропозициональные переменные с индексами, неявно допускалось наличие натурального ряда. Таким образом, арифметика пронизывает собой всё здание математики и без неё нельзя построить ни одну математическую теорию.

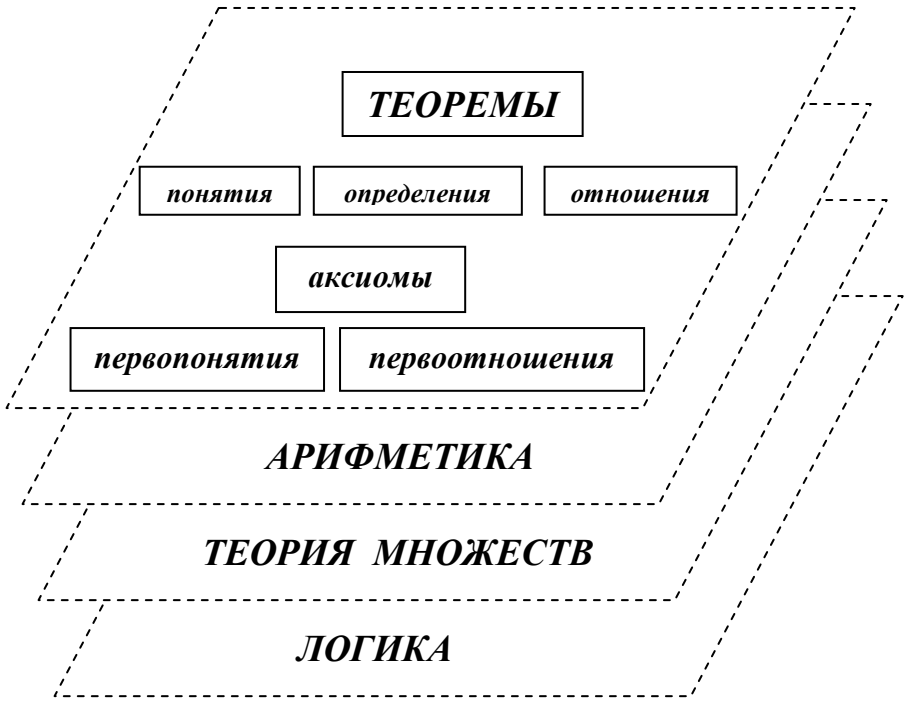
Каждая математическая дисциплина изучает свои специфические объекты, которые вводятся с помощью *определений*. Чтобы процесс определения объектов был конечен, необходимо допустить некоторые *первичные неопределяемые понятия*, которые связаны некими неопределяемыми *первичными отношениями*. Например, геометрия имеет дело с такими неопределяемыми первопонятиями как "точка", "прямая", "плоскость", связанными первичными отношениями "равенства", "принадлежности", "расположения между" и др.; теория множеств не определяет понятия "множества", "элемента", отношения "равенства элементов" и "принадлежности элемента множеству"; арифметика оперирует неопределяемым понятием "натурального числа" и отношением "непосредственного следования" чисел. Эти неопределяемые понятия и отношения каждой теории подчиняются специфическим для этой теории *аксиомам* – утверждениям, принимаемым на веру. При этом разные математические дисциплины, могут иметь дело с одними и теми же объектами, но интересоваться различными свойствами этих объектов, акцентируя внимание на одних аксиомах и не обращая внимания на другие (если они не используются в рассуждениях). Например, при изучении действительных чисел алгебраиста заинтересуют, прежде всего, алгебраические операции и их свойства, а специалиста по анализу – непрерывные структуры на множестве этих чисел. Поэтому для анализа первостепенную роль играет аксиома непрерывности, на которую алгебраисты почти не обращают внимания.

Особо следует подчеркнуть, что аксиомы далеко не очевидны. Часто можно услышать, что "аксиомы – это очевидные утверждения, принимаемые без доказательства". Ошибкой будет считать аксиомы и "утверждениями, не требующими доказательств". Это не так ! Например, неевклидовы геометрии, широко используемых ныне в физике и других практических дисциплинах, появились именно благодаря попыткам доказать аксиому параллельности Евклида, которые и привели в конечном итоге к созданию новых геометрий в работах Н. Лобачевского, Я. Бойяи и Б. Римана. Неевклидовы геометрии имеют такое же право на существование, как и знакомая со школьной скамьи геометрия Евклида. Выбор той или иной аксиоматики – сложная проблема, в решении которой первостепенная роль принадлежит внутренней интуитивной уверенности в непротиворечиво-

сти принимаемой системы аксиом, т.е. вера в существование математического объекта с постулируемыми свойствами.

Итак, всякая математическая теория изучает свой особый мир со специфическими первообъектами и первоотношениями, подчиняющийся законам, сформулированным в виде аксиом. Следует отметить, что само по себе задание списка первообъектов и аксиом не является гарантией содержательности теории. Так, например, в реферативном журнале "Математика", в котором аннотировались большинство математических статей, публикующихся в отечественных и зарубежных журналах, часто встречались замечания рецензентов о том, что изучаемый автором статьи класс объектов тривиален и потому не представляет интереса для изучения. Так что за кажущейся многозначительностью и псевдонаучностью часто скрывается пустота.

Как уже отмечалось, из первопонятий можно конструировать более сложные понятия, которые вводятся либо с помощью определений, выделяющих среди уже известных объектов те, которые удовлетворяют некоторым особо интересным свойствам, либо используя универсальные средства, предоставляемые теорией множеств, либо с помощью специфических средств самой теории. Например, имея понятие треугольника в геометрии, можно определить равносторонние тре-



угольники, выделяя их свойством равенства всех сторон, а работая с множествами, можно образовывать новые множества, выделяя подмножества элементов данного множества, используя известные операции над множествами, рассматривая множество подмножеств данного множества, декартово произведение множеств, специфические функции, определённые на множестве, функциональные

образы и прообразы множеств и.т.д. Таким образом, математик в процессе работы знакомится со всё новыми и новыми обитателями изучаемого мира, которые становятся доступными благодаря средствам, заложенным в основания теории, а значит, потенциально скрытых в аксиомах. Конечно, как отмечалось выше, можно вводить противоречивые определения и всю жизнь изучать свойства несуществующих объектов. Но эта ситуация не уникальна для математики: с тем же успехом криптозоологи могут тратить жизнь на поиски кентавров, а палеонтологи – на доказательство происхождения человека от обезьяны.

Наконец, цель всякой математической дисциплины состоит в изучении свойств введённых объектов и отношений между ними, которые формулируются в виде *теорем* на специфическом формальном языке данной дисциплины и доказываются, исходя из аксиом, с использованием логических правил вывода. Может показаться, что цель математики – доказательство как можно большего числа теорем. Однако, как и в каждой науке, важно не количество результатов, но их смысл, определяемый целью исследования. Таким образом, задача исследователя состоит не только и не столько в умении доказывать теоремы, сколько в правильном выборе цели. Не случайно сказано: “Гениальные математики формулируют теоремы, а талантливые их доказывают”. На первое место в исследованиях выступает как раз интуиция, умение отрешиться от сиюминутных “перспективных” и “актуальных” задач и сконцентрироваться на том, к чему зовёт душа, суметь не разменять жажду математических странствий на доходное место обеспеченного чиновника при математическом департаменте.

История науки показывает, что часто наиболее важные открытия, составляющие гордость и славу той или иной науки делались не на проторенных магистральных направлениях, но в стороне от них, вопреки мнению большинства, считавшего эти исследования бесперспективными. Таким образом, целью подлинно научного творчества должно быть стремление к Истине, познание той гармонии, которая правит миром в целом, которая движет его солнце и светила и отражается тысячью граней в каждой мельчайшей капельке, падающей с небес на ладони неравнодушного исследователя, чистого сердцем и одухотворённого стремлением к Совершенству.

§ 7. Виды математических утверждений

Будем рассматривать высказывания о математических объектах, т.е. произвольные математические утверждения, которым можно приписать значение *ис-*

тина или *ложь*. Например, *"2×2=5"*, *"2×2=4"* и *"сумма углов треугольника равна* 180^0*"* – математические высказывания.

Несколько упрощая и огрубляя действительность, можно сказать, что любое математическое утверждение можно записать в одном из следующих видов: $\forall\ x\ P(x)$ или $\exists\ x\ P(x)$, где x – некоторая переменная, а $P(x)$ – предикат (на самом деле переменных может быть несколько). В общем виде будем писать $Q\ x\ P(x)$, подразумевая под Q один из кванторов ($Q \in \{\forall, \exists\}$). Конечно, сам предикат $P(x)$ при этом может иметь сколь угодно сложную структуру.

Например, знакомое из анализа утверждение $(\forall \varepsilon > 0\ (\exists n \in \mathbf{N}\ (\forall\ k, m \in \mathbf{N}\ (k, m \geq n) \rightarrow |a_m - a_n| < \varepsilon)))$ представляет собой критерий Коши сходимости последовательности $\{a_n\}$. Здесь в качестве переменной использован символ ε, а предикат $P(\varepsilon)$ – это достаточно сложное высказывание с переменной $(\exists n \in \mathbf{N}\ (\forall\ k, m \in \mathbf{N}\ (k, m \geq n) \rightarrow\ |a_m - a_n| < \varepsilon))$. На самом деле это высказывание правильно записать так: $(\exists n \in \mathbf{N}\ (\forall\ k, m \in \mathbf{N}\ (k \geq n) \wedge (m \geq n) \rightarrow |a_m - a_n| < \varepsilon))$. Таким образом, исходное утверждение состоит из *кванторной приставки* $\forall \varepsilon > 0\ \exists n \in \mathbf{N}\ \forall\ k, m \in \mathbf{N}$ и *условия* $(k \geq n) \wedge (m \geq n) \rightarrow\ |a_m - a_n| < \varepsilon$, имеющего вид импликации двух предикатов: одного – $(k \geq n) \wedge (m \geq n)$ и второго – $|a_m - a_n| < \varepsilon$. Эти предикаты сами используют другие предикаты $\geq$, $<$ и знаки функций – ведь последовательность – это функция, сопоставляющая каждому натуральному числу n значение a_n. Ещё более формально критерий Коши следует писать так:

$$\forall \varepsilon\ (\exists n\ (\forall\ k\ (\forall m\ ((\varepsilon \in \mathbf{R} \wedge \varepsilon > 0) \wedge (n \in \mathbf{N}) \wedge (k \in \mathbf{N} \wedge k \geq n) \wedge (m \in \mathbf{N} \wedge m \geq n) \rightarrow |a_m - a_n| < \varepsilon)))).$$

Здесь $\forall \varepsilon\ \exists n\ \forall\ k\ \forall m$ – кванторная приставка, а всё остальное – высказывание с переменными, т.е. предикат, образованный с помощью логических связок из более простых предикатов $\varepsilon \in \mathbf{R}$, $\varepsilon > 0$, $n \in \mathbf{N}$, $k \in \mathbf{N}$, $m \in \mathbf{N}$, $k \geq n$, $m \geq n$, $|a_m - a_n| < \varepsilon$.

Как правило, встречающиеся математические утверждения можно записать в аналогичном виде: *(кванторная_приставка) (предикат_1* $\rightarrow$ *предикат_2)*. Такая запись называется *импликативной формой записи математического утверждения* (т.к. в ней используется импликация).

Сразу напрашивается возражение: теорема Пифагора формулируется совсем иначе – квадрат гипотенузы равен сумме квадратов катетов – где же тут импликация ? Просто приведённая формулировка не является строгой: например, в ней совсем не упоминается прямоугольный треугольник, не ясно также, что такое его гипотенуза и катеты. Импликативная форма записи выглядит, например, так: $\forall\ \Delta ABC\ ((\angle ACB = 90^0) \rightarrow\ AB^2 = AC^2 + BC^2)$. Здесь $\forall\ \Delta ABC$ – кванторная

приставка, $\angle ACB = 90^0$ – *предикат_1*, $AB^2 = AC^2 + BC^2$ – *предикат_2*. Если опуститься (а может быть, подняться ?!) на ещё более высокую ступень формализма, то следует ввести множество Δ всех треугольников и функции $\angle C(x)$, $AB(x)$, $BC(x)$, $AC(x)$, сопоставляющие каждому треугольнику $x = \Delta ABC$ соответственно величину угла C и длины сторон AB, BC, AC. Тогда теорема Пифагора станет ещё более загадочной: $\forall x \in \Delta\ ((\angle C(x)=90^0) \to AB(x)^2 = AC(x)^2 + BC(x)^2)$. Хотя это и не предел формализации, но, как правило, мы не будем забредать слишком далеко в подобные формалистические дебри.

Другой пример преобразования неимпликативного утверждения в импликативную форму: утверждение "*1 является минимальным натуральным числом*" может быть записано в импликативной форме так: $\forall\ n\ (n \in \mathbf{N} \to n \geq 1)$.

Упражнение: Преобразовать в импликативную форму и записать в виде формул с кванторами и предикатами следующие утверждения:

1) Сумма углов n-угольника равна $(n-2)\cdot\pi$,
2) Квадрат действительного числа неотрицателен,
3) Натуральное число m делится на 12 тогда и только тогда, когда оно делится на 3 и на 4,
4) Если последовательность сходится, то сходится и её подпоследовательность с чётными номерами,
5) Диагонали параллелограмма делятся в точке пересечения пополам.

В дальнейшем ограничимся рассмотрением только простейших утверждений вида $Q\ x\ (P(x) \to R(x))$. По ним можно образовать следующие утверждения:

$$Q x\ (R(x) \to P(x)),\quad Q\ x\ (\overline{P(x)} \to \overline{R(x)}),\quad Q\ x\ (\overline{R(x)} \to \overline{P(x)}),$$

которые называются соответственно *обратным, противоположным и контрапозиционным* утверждениями к исходному. При этом само исходное утверждение $Q\ x\ (P(x) \to R(x))$ называют *прямым*. Легко видеть, что контрапозиционное утверждение является противоположным к обратному, а утверждение обратное к обратному будет прямым, так же как и противоположное к противоположному.

Примеры: 1. Рассмотрим утверждение "*если натуральное число n делится на 6, то оно делится на 2 и на 3*". Его <u>импликативная форма</u>:

$$\forall n \in \mathbf{N}\ ((n \vdots 6) \to (n \vdots 2) \wedge (n \vdots 3))$$

– это <u>прямое</u> утверждение. Сформулируем другие виды утверждений:

<u>обратное:</u> $\forall n \in \mathbf{N}\ ((n \vdots 2) \wedge (n \vdots 3) \to (n \vdots 6))$ – "*если натуральное число n делится на 2 и на 3, то оно делится на 6*";

противоположное: $\forall n \in \mathbf{N}\ ((n \vdots 6) \to (n \vdots 2) \vee (n \vdots 3))$ – *"если натуральное число n не делится на 6, то оно не делится на 2 или на 3";*

контрапозиционное: $\forall n \in \mathbf{N}\ ((n \vdots 2) \vee (n \vdots 3) \to (n \vdots 6))$ – *"если натуральное число n не делится на 2 или на 3, то оно не делится на 6".*

2. Для прямого утверждения *"если последовательности $\{a_n\}$ и $\{b_n\}$ сходятся, то сходится последовательность $\{a_n + b_n\}$"* обратное звучит так: *"если сходится последовательность $\{a_n + b_n\}$, то последовательности $\{a_n\}$ и $\{b_n\}$ сходятся"*, *противоположное – "если одна из последовательностей $\{a_n\}$ или $\{b_n\}$ не сходится, то не сходится последовательность $\{a_n + b_n\}$"* и *контрапозиционное – "если не сходится последовательность $\{a_n + b_n\}$, то одна из последовательностей $\{a_n\}$ или $\{b_n\}$ не сходится".*

Упражнение. Сформулировать все виды утверждений для прямых утверждений из предыдущего упражнения.

Каждое математическое утверждение, будучи высказыванием, является истинным или ложным. Поэтому для проверки истинности утверждения необходимо сопоставить его смысл с "окружающей математической действительностью" в самом широком смысле. Для доказательства истинности утверждения вида $\exists x\ P(x)$ (не обязательно в импликативной форме) нужно *найти хотя бы один объект $a \in D(P)$ со свойством $P(a)$, т.е. хотя бы один элемент из области истинности предиката $P(x)$: $a \in D_1(P)$.* Для доказательства истинности утверждения вида $\forall x\ P(x)$ нужно *проверить, что для любого объекта $a \in D(P)$ выполнено свойство $P(a)$, т.е. доказать равенство $D(P) = D_1(P)$.*

Ложность утверждения вида $Q x\ P(x)$ равносильна истинности утверждения $\overline{Q\ x\ P(x)} \equiv \overline{Q}\ x\ \overline{P}(x)$, где $\overline{Q} = \begin{cases} \forall, \text{ если } Q = \exists \\ \exists, \text{ если } Q = \forall \end{cases}$ (см. основные равносильности с кванторами). Поэтому проверка ложности математического утверждения сводится к проверке истинности некоторого другого утверждения аналогичной структуры.

Примеры: 1. Истинно ли утверждение $\exists\, x \in \mathbf{Z}\ (\forall\, y \in \mathbf{R}\ \ x \cdot y = 3)$?

Пусть $x = x_0 \in \mathbf{Z}$ фиксировано. Рассмотрим высказывание $\forall\, y \in \mathbf{R}\ \ x_0 \cdot y = 3$. Очевидно, что оно ложно, т.к. при $y = 0$ условие $x_0 \cdot y = 3$ не выполнено ни при каком $x_0 \in \mathbf{Z}$. Поэтому исходное утверждение ложно.

2. Истинно ли утверждение $\forall x \in \mathbf{N}\ (\exists y \in \mathbf{R}\ \ x \cdot y = 3)$?

Пусть $x = x_0 \in \mathbf{N}$ фиксировано. Рассмотрим высказывание $\exists\, y \in \mathbf{R}\ \ x_0 \cdot y = 3$. Поскольку $x_0 \in \mathbf{N}$, а значит, $x_0 \neq 0$, то это высказывание равносильно утвержде-

нию $\exists\ y \in \boldsymbol{R}\ \ y = \dfrac{3}{x_0}$, которое, очевидно, истинно (y явно вычислено по x_0). Поэтому исходное утверждение истинно.

3. Истинно ли утверждение $\forall x \in \boldsymbol{N}\ (\forall y \in \boldsymbol{N}\ \ x \cdot y + 1 > x + y)$?

Для $x = x_0 \in \boldsymbol{N}$ рассмотрим высказывание $\forall y \in \boldsymbol{N}\ \ (x_0 \cdot y + 1 > x_0 + y)$, которое при $x_0 = 1$ принимает вид $\forall\ y \in \boldsymbol{N}\ \ y + 1 > 1 + y$ и является ложным. Значит оно истинно не для любого $x_0 \in \boldsymbol{N}$, т.е. исходное утверждение ложно.

Упражнение. Найдите истинные и ложные утверждения из предыдущего упражнения.

Совершенно не обязательно, что истинность прямого утверждения влечёт истинность и других – обратного, противоположного и контрапозиционного. Например, утверждение $\forall m, n \in \boldsymbol{N}\ \ (m \mid n\ \rightarrow\ m \le n)$ истинно, но обратное к нему: $\forall\ m,\ n \in \boldsymbol{N}\ \ (m \le\ n \rightarrow m \mid n)$ ложно, как и противоположное $\forall\ m,\ n \in \boldsymbol{N}\ \ (m \nmid n\ \rightarrow\ m > n)$; контрапозиционное утверждение $\forall m, n \in \boldsymbol{N}\ \ (m > n \rightarrow m \nmid n)$ снова истинно.

На самом деле контрапозиционное утверждение $Q x\ (\overline{R(x)} \rightarrow \overline{P(x)})$ и прямое $Q\ x\ (P(x) \rightarrow R(x))$ всегда равносильны, т.е. истинны или ложны одновременно. Это следует из известного закона контрапозиции $(a \rightarrow b) \leftrightarrow (\overline{b} \rightarrow \overline{a})$. Эту равносильность иногда удобно использовать при доказательствах теорем: вместо прямого утверждения иногда удобнее доказывать контрапозиционное к нему.

Если прямое утверждение $Q x\ \ (P(x) \rightarrow R(x))$ истинно, то истинна импликация $P(x) \rightarrow R(x)$ для некоторой совокупности объектов x (по крайней мере, для одного, если $Q = \exists$, и для всех, – если $Q = \forall$). Особое внимание уделим случаю $Q = \forall$. Тогда предикат $P(x) \rightarrow R(x)$ тождественно истинен, и вместо записи $\forall x\ (P(x) \rightarrow R(x))$ иногда кратко пишут $P(x) \Rightarrow R(x)$. При этом предикат $P(x)$ называется *достаточным условием для* $R(x)$, а предикат $R(x)$ – *необходимым условием для* $P(x)$ или *логическим следствием предиката* $P(x)$. Смысл названий состоит в том, что для любого объекта a для проверки истинности условия $R(a)$ *достаточно* проверить истинность условия $P(a)$, а для того, чтобы $P(a)$ было истинным, *необходимо* (т.е. обязательно требуется), чтобы истинным было высказывание $R(a)$, истинность которого *следует* из истинности $P(a)$.

Если предикаты $P(x)$ и $R(x)$ равносильны, т.е. $\forall x\ (P(x) \leftrightarrow R(x))$, то иногда кратко пишут $P(x) \Leftrightarrow R(x)$. Ввиду равносильности $\forall\ x\ (P(x) \leftrightarrow R(x)) \equiv$ $\equiv\ \forall x\ ((P(x) \rightarrow R(x)) \wedge (R(x) \rightarrow P(x)))$, условие $R(x)$ не только необходимо, но и

достаточно для $P(x)$, а $P(x)$, в свою очередь, необходимо для $R(x)$ и является логическим следствием предиката $R(x)$. Вот почему вместо $P(x) \Leftrightarrow R(x)$ часто говорят "условие $P(x)$ необходимо и достаточно для выполнения $R(x)$". Ясно, что $P(x) \Leftrightarrow R(x) \equiv (P(x) \Rightarrow R(x)) \wedge (R(x) \Rightarrow P(x))$ поэтому вместе с прямым утверждением в этом случае справедливо и обратное.

Примеры: 1. Условие $R(x) \equiv$ "*натуральное число x делится на 2*" является необходимым условием для $P(x) \equiv$ "*натуральное число x делится на 6*", т.к. высказывание $P(x) \Rightarrow R(x)$ $(\equiv \forall x\,(P(x) \to R(x)))$ истинно. Обратное утверждение $R(x) \Rightarrow P(x)$ в данном случае не верно, т.к. например, $2 \vdots 2$, но $2 \nmid 6$. Таким образом, условие $R(x)$ необходимо, но не достаточно для $P(x)$.

2. Очевидно, что необходимым и достаточным условием для $P(x) \equiv$ "*натуральное число x делится на 6*" является условие $S(x) \equiv$ "*натуральное число x делится на 2 и на 3*". Таким образом, в этом случае справедливо $P(x) \Leftrightarrow S(x)$.

Упражнение: Среди нижеследующих условий выделить необходимые, достаточные и необходимые и достаточные:

1) $P(x) =$ "*два угла треугольника x и две его стороны равны между собой*",
   $R(x) =$ "*треугольник x равносторонний*",
2) $P(x) =$ "*два угла треугольника x равны между собой*",
   $R(x) =$ "*треугольник x равнобедренный*",
3) $P(x) =$ "*три медианы треугольника x равны между собой*",
   $R(x) =$ "*треугольник x равносторонний*",
4) $P(x) =$ "$x \in \mathbf{N}$ *и* $x \geq 5$", $R(x) \equiv$ "$x \in \mathbf{N}$ *и* $2^x > 5$",
5) $P(x) \equiv$ "$x \in \mathbf{N}$ *и* $x \geq 5$", $R(x) \equiv$ "$x \in \mathbf{N}$ *и* $2^x > 5 \cdot x + 6$",
6) $P(x) \equiv$ "*последовательность* $\{x_n\}$ *сходится*",
   $R(x) \equiv$ "*последовательность* $\{x_{2 \cdot n}\}$ *сходится*",
7) $P(x) \equiv$ "*последовательность* $\{x_n\}$ *сходится*",
   $R(x) \equiv$ "*последовательность* $\{2 \cdot x_n\}$ *сходится*".

§ 8. Некоторые методы доказательства теорем

Под теоремой обычно понимается математическое утверждение, которое можно *доказать*. *Доказательством теоремы* T называется конечная последовательность теорем T_1, T_2, … , $T_n = T$, где каждое T_i является аксиомой или получается из предыдущих утверждений T_1, T_2, … , T_{i-1} с помощью заранее ого-

воренных правил логического вывода. Теорема T_1 , у которой нет предыдущих, очевидно, должна быть аксиомой.

Таким образом, доказательство любой теоремы разбивается на части, каждая из которых представляет собой мини-теорему. Из этих частей затем выводится утверждение исходной теоремы T. Конечно, можно требовать, чтобы в любом доказательстве использовались только аксиомы, но тогда вывод самой простой теоремы занял бы многие страницы, и кроме того, в доказательствах встречались бы длинные куски одинаковых рассуждений, затемняющие основную идею. Поэтому, для большей ясности, часто используемые однотипные рассуждения оформляют в виде лемм, предложений и прочих вспомогательных утверждений (каждое из которых является теоремой), на которые затем ссылаются, не повторяя заново их доказательства.

Аксиомы специфичны для каждой отрасли математического знания. Уже в школе знакомятся с аксиомами евклидовой геометрии, в институтском курсе алгебры и логики – с аксиомами исчисления высказываний (таблицами истинности для логических связок) и аксиомами Пеано для натуральных чисел. Существуют свои списки аксиом теории множеств, теории действительных чисел, неевклидовых геометрий и многие другие, с которыми вы уже встречались. Поэтому в доказательстве той или иной теоремы могут участвовать аксиомы разной природы – всё зависит от специфики тех объектов, свойства которых устанавливает доказываемая теорема.

Точный и полный список правил логического вывода для некоторых математических теорий будет приведён в следующей главе. Отметим только, что эти правила вывода основаны на доказанных нами законах логики и правилах действий с кванторами. Сейчас же будем пользоваться приведённым не вполне строгим, но интуитивно ясным понятием математического доказательства.

Упражнение. Проанализируйте доказательства каких-либо встречавшихся в курсах алгебры, геометрии, математического анализа теорем и выделите (по крайней мере, некоторые) аксиомы, которые были использованы при этом, а также правила вывода, применявшиеся в рассуждениях.

Гарантирует ли наличие доказательства истинность теоремы ? Другими словами, существуют ли в “математической реальности” те объекты и отношения, о которых говорит доказанная теорема ? Вообще говоря, не всегда: если, например, включить в список аксиом ложное утверждение, то из этой аксиомы можно логически вывести любую, в том числе и ложную, теорему. Однако, если хотя бы одно утверждение не выводится из аксиом (аксиомы *непротиворечивы*), то любая

доказанная теорема истинна. Этот нетривиальный факт составляет суть так называемой теоремы о существовании модели (более подробно об этом речь пойдёт в следующей главе).

Таким образом, ***доказательство теоремы в непротиворечивой аксиоматике гарантирует её истинность. Обратное не верно ! Существуют примеры истинных, но не доказуемых (в данной непротиворечивой системе аксиом) теорем.*** В самом деле, рассмотрим множество всех натуральных чисел $\boldsymbol{N} = \{1, 2, 3, \ldots\}$ с операцией "прибавления единицы", которая сопоставляет каждому натуральному числу n следующее натуральное число $n + 1$ и подчиняется следующим трём аксиомам: $1 + 1 = 2,\ 2 + 1 = 3,\ 3 + 1 = 4$. Обычная операция сложения натуральных чисел, конечно, удовлетворяет этим аксиомам, но выполненное для неё свойство $2 + 2 = 4$ невозможно доказать, используя только перечисленные аксиомы, т.к. нет возможности с их помощью преобразовать $2 + 2$ в 4: $2 + 2 = (1 + 1) + 2 = (1 + 1) + (1 + 1) = 2 + (1 + 1)$ и $4 = 3 + 1 = (2 + 1) + 1 = ((1 + 1) + 1) + 1$ – вот все возможные способы записи выражения $2 + 2$ и числа 4 с использованием только трёх указанных аксиом. При этом ни одна из записей выражения $2 + 2$ не совпадает ни с одной записью числа 4, и отсутствуют иные средства преобразовать эти записи одна в другую, т.к. всё, что можно использовать – это три правила, зафиксированные в рассматриваемых аксиомах. Таким образом, теорема арифметики $2 + 2 = 4$ не доказуема, исходя только из трёх приведённых аксиом, но она истинна и доказуема с использованием полной аксиоматики Пеано натуральных чисел.

Упражнения. 1. Доказуемы ли, исходя из рассмотренных трёх аксиом, теоремы $1 + 2 = 2 + 1,\ 1 + 3 = 4$?

2. Докажите теоремы $2 + 2 = 4$ и $2 \times 2 = 4$ на основе аксиом Пеано.

Доказательство любой теоремы – это творческая работа. Здесь нет, и не может быть универсальных рецептов. Приведём лишь некоторые наиболее употребительные приёмы, часто используемые в математических доказательствах.

I. Метод полного перебора возможных случаев. *Пусть нужно доказать утверждение $A(x)$ о некотором математическом объекте x. Предположим, что для x доказана теорема $A_1(x) \vee \ldots \vee A_n(x)$, где $A_1(x), \ldots, A_n(x)$ – некоторые утверждения, и для каждого i $(1 \le i \le n)$ доказана импликация $A_i(x) \to A(x)$. Тогда $A(x)$ следует из теорем $A_1(x) \vee \ldots \vee A_n(x)$ и $A_i(x) \to A(x)$ $(1 \le i \le n)$ на основании правила логического вывода о переборе возможных случаев:*

$$\frac{\models \mathcal{A}_1 \vee \ldots \vee \mathcal{A}_n ; \models \mathcal{A}_1 \to C ; \ldots ; \models \mathcal{A}_n \to C}{\models C} .$$

Доказательство. Если $T_1, \ldots, T_k, A_1(x) \vee \ldots \vee A_n(x)$ – доказательство теоремы $A_1(x) \vee \ldots \vee A_n(x)$, а $T_{i_1}, \ldots, T_{i_{k_i}}$, $A_i(x) \to A(x)$ – доказательства теорем $A_i(x) \to A(x)$ $(1 \le i \le n)$, то цепочка $T_1, \ldots, T_k, A_1(x) \vee \ldots \vee A_n(x), T_{i_1}, \ldots, T_{i_{k_i}}, A_1(x) \to A(x), \ldots, T_{n_1}, \ldots, T_{n_{k_n}}, A_n(x) \to A(x), A(x)$ будет доказательством теоремы $A(x)$ с применением (на последнем шаге) упомянутого правила вывода.

Докажем это правило от противного: если $C(\varepsilon) = 0$, то из $(\mathcal{A}_i(\varepsilon) \to C(\varepsilon)) = 1$ получаем $\mathcal{A}_i(\varepsilon) = 0$, т.е. $\mathcal{A}_1(\varepsilon) \vee \ldots \vee \mathcal{A}_n(\varepsilon) = 0$ – противоречие.

Теорема доказана.

Пример. Доказать, что $\forall n \in \mathbf{N}\ n \cdot (n+1) \vdots 2$.

Доказательство можно записать в две строчки: “любое натуральное число n либо чётно, и тогда $n \cdot (n+1) \vdots 2$, либо нечётно – тогда $n+1$ чётно, и снова $n \cdot (n+1) \vdots 2$”. Более формально, на основе аксиоматики Пеано нужно рассуждать следующим образом.

Здесь $A(n) =$ “$n \cdot (n+1) \vdots 2$”. Рассмотрим два утверждения $A_1(n) =$ “n *нечётно*”, $A_2(n) =$ “n *чётно*” и докажем теорему $A_1(x) \vee A_2(x)$, представляющую собой очевидное высказывание о том, что каждое натуральное число n либо чётно, либо нечётно. Если опираться только на аксиомы Пеано, то это утверждение неочевидно, и его доказательство требует привлечения аксиомы индукции. Для этого образуем множества: $\{n \in \mathbf{N} \mid \exists k \in \mathbf{N}\ n = 2 \cdot k\}$ – всех чётных чисел, $\{n \in \mathbf{N} \mid \exists k \in \mathbf{N}\ n = 2 \cdot k - 1\}$ – всех нечётных чисел и убедимся, что их объединение M равно $\mathbf{N}$. Применим аксиому индукции: ясно, что $1 \in M$ и $\forall m \in M$ $m + 1 \in M$ (?!). На основании аксиомы индукции заключаем, что $M = \mathbf{N}$.

Кроме того, доказуемы импликации $A_1(x) \to A(x)$ и $A_2(x) \to A(x)$: если n нечётно, то $n = 2 \cdot k - 1$ и $n \cdot (n+1) = (2k-1) \cdot 2 \cdot k = 2 \cdot k \cdot (2 \cdot k - 1)$ чётно, а если n чётно, то $n = 2 \cdot k$ и снова $n \cdot (n+1) = 2 \cdot k \cdot (2 \cdot k + 1)$ чётно. Таким образом, на основании метода перебора возможных случаев утверждение $A(n)$ доказано.

Кстати, в этом доказательстве использована коммутативность умножения натуральных чисел. Вывести этот закон из аксиом Пеано не так-то просто.

II. Метод рассуждения от противного. *Пусть о некотором математическом объекте x нужно доказать утверждение $A(x)$. Предположим, что доказаны теоремы $B(x)$ и $\overline{A(x)} \to \overline{B(x)}$ (т.е. из предположения о ложности дока-*

зываемой теоремы следует отрицание доказанного ранее утверждения). Тогда $A(x)$ *следует из упомянутых теорем на основании правила опровержения:* $\dfrac{\models \mathcal{B};\ \models \overline{\mathcal{A}} \to \overline{\mathcal{B}}}{\models \mathcal{A}}$.

Доказательство. Если $T_1, \dots, T_k, B(x)$ – доказательство теоремы $B(x)$, а $S_1, \dots, S_m, \overline{A(x)} \to \overline{B(x)}$ – доказательство теоремы $\overline{A(x)} \to \overline{B(x)}$, то $T_1, \dots, T_k, B(x), S_1, \dots, S_m, \overline{A(x)} \to \overline{B(x)}, A(x)$ – доказательство теоремы $A(x)$ с использованием упомянутого правила, которое доказывается стандартно: если $\mathcal{B}(\varepsilon) \equiv 1$ и $(\overline{\mathcal{A}} \to \overline{\mathcal{B}})(\varepsilon) \equiv 1$, то $\overline{\mathcal{A}}(\varepsilon) \equiv 0$, $\mathcal{A}(\varepsilon) \equiv 1$.

Теорема доказана.

Пример. Доказать, что в любом прямоугольном треугольнике квадрат гипотенузы не меньше удвоенного произведения катетов.

Предположим, что высказанное утверждение $A(x)$ неверно, т.е. для некоторого прямоугольного треугольника x с гипотенузой c и катетами a, b выполнено неравенство $c^2 < 2 \cdot a \cdot b$. Используя известное неравенство о среднем арифметическом и среднем геометрическом $(\forall x, y \in \mathbf{R}_+ \ \sqrt{x \cdot y} \le \dfrac{x+y}{2})$, получим $c^2 < 2 \cdot a \cdot b = 2 \cdot \sqrt{a^2 \cdot b^2} \le 2 \cdot \dfrac{a^2 + b^2}{2} = a^2 + b^2$, что противоречит доказанной в школе теореме Пифагора $B(x)$ о справедливости равенства $c^2 = a^2 + b^2$. Таким образом, доказана импликация $\overline{A(x)} \to \overline{B(x)}$. Значит, доказана и теорема $A(x)$.

III. Доказательство эквивалентности нескольких условий. *Пусть для математического объекта* x *сформулированы условия* $A_1(x), \dots, A_n(x)$. *Нарисуем граф с вершинами* $1, \dots, n$, *в котором из вершины* i *выходит стрелка в вершину* j *тогда и только тогда, когда доказана импликация* $A_i(x) \to A_j(x)$. *Если из любой вершины такого графа можно пройти по стрелкам в любую другую вершину, то можно доказать эквивалентность всех условий* $A_1(x), \dots, A_n(x)$.

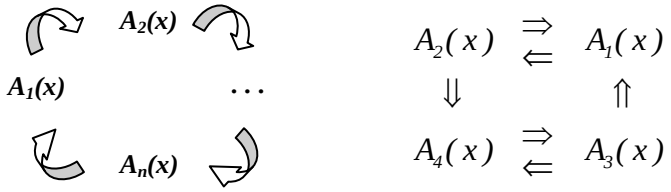
Доказательство. Докажем что для любых i и j $(1 \le i, j \le n)$ доказуема эквивалентность $A_i(x) \leftrightarrow A_j(x)$. В самом деле, рассмотрим в графе путь из вершины i в вершину j: $i = i_1 \to \dots \to i_k = j$. По условию, ему соответствует цепочка доказуемых импликаций $A_i(x) = A_{i_1} \to A_{i_2}, A_{i_2} \to A_{i_3}, \dots, A_{i_{k-1}} \to A_{i_k} = A_j(x)$. Применяя несколько раз правило силлогизма $\dfrac{\mathcal{A} \models \mathcal{B};\ \mathcal{B} \models C}{\mathcal{A} \models C}$ в виде $\dfrac{\models \mathcal{A} \to \mathcal{B};\ \models \mathcal{B} \to C}{\models \mathcal{A} \to C}$, получим доказательство импликации $A_i(x) \to A_j(x)$.

Поменяв в этих рассуждениях i и j местами, докажем $A_j(x) \to A_i(x)$. Поскольку $(x \leftrightarrow y) \equiv (x \to y) \wedge (y \to x)$, то доказуема и эквивалентность $A_i(x) \leftrightarrow A_j(x)$.

Теорема доказана.

Примеры: 1. Для доказательства эквивалентности n условий $A_1(x), \ldots, A_n(x)$ достаточно доказать импликации $A_i(x) \to A_{i+1}(x)$ $(1 \le i \le n-1)$, $A_n(x) \to A_1(x)$.

2. Для доказательства эквивалентности четырёх условий достаточно доказать, например, что $A_1(x) \leftrightarrow A_2(x)$, $A_3(x) \leftrightarrow A_4(x)$, $A_2(x) \to A_4(x)$, $A_3(x) \to A_1(x)$. Какие стрелки можно убрать ?



Упражнения: 1. Приведите другие примеры доказательств с использованием перечисленных методов. Какие ещё методы математических доказательств Вы знаете ?

2. Какое минимальное число импликаций нужно доказать, чтобы обосновать эквивалентность n условий ?

ГЛАВА III. ФОРМАЛЬНЫЕ АКСИОМАТИЧЕСКИЕ ТЕОРИИ

§ 1. Формальные и неформальные аксиоматические теории

Нами изучены две математические теории, относящиеся к логике: алгебра высказываний и алгебра предикатов. В обоих случаях делалось следующее:

- были объявлены первоначальные (неопределяемые) понятия: *высказывание*, *истина*, *ложь*, *предикат*.
- все остальные понятия определялись, опираясь на неопределяемые понятия, а также на общематематические неопределяемые понятия: множество, принадлежность элемента множеству, натуральное число, и др.
- были сформулированы некоторые аксиомы – утверждения, постулирующие свойства неопределяемых понятий: например, это были таблицы истинности логических связок в исчислении высказываний. Другие аксиомы использовались неявно: например, аксиомы теории множеств при работе с предикатами, понятия истинности формул с кванторами, аксиомы Пеано.
- все остальные теоремы были доказаны, исходя из аксиом с помощью рассуждений, правильность которых, фактически, принималась на веру.
- не было определено формального понятия "доказательство" и не были сформулированы явно правила рассуждений, которые допустимо использовать в доказательствах.

Все перечисленные черты присущи *неформальным аксиоматическим теориям*, структура которых обсуждалась в § 7 главы II.

Идя по тернистому пути к матемтической строгости, математики пытаются придать математическим теориям всё более формальный характер, чтобы исключить всякую возможность использования несанкционированных аксиомами и правилами вывода рассуждений. Программа такой формализации была выдвинута Д. Гильбертом в начале XX в., и первые её шаги вселяли уверенность в скором завершении строительства незыблемого и непоколебимого здания самой точной из всех наук – математики.

Построение *формальной аксиоматической теории* , в отличие от неформальной, предполагает следующие шаги:

- задание её *алфавита*, т.е. базовых *символов аксиоматической теории*, каждый из которых лишён какого-нибудь содержательного смысла.

- указываются правила построения *формул теории* из символов алфавита, т.е. её осмысленных предложений.
- из списка формул выделяется некоторое подмножество, элементы которого называются *аксиомами формальной теории* и считаются истинными.
- формулируются *правила вывода*, т.е. используемые при доказательствах правила вывода одних формул из других.
- формулируется определение *доказательства* и определение *вывода формулы из совокупности других формул*.
- все формулы, для которых существуют доказательства, называются *доказуемыми* или *теоремами формальной теории*.

На самом деле, некоторые черты построения формальных аксиоматических теорий были присущи и изложению предыдущих глав: так, например, в этих главах были определены понятия формул исчисления высказываний и формул исчисления предикатов. Однако последовательно идея формализма в жизнь не проводилась. Таким образом, наше изложение носило эклектичный характер.

Примеры формальных аксиоматических теорий

I. Формальное исчисление высказываний. *Алфавит* этой теории – это алфавит исчисления высказываний. Он состоит из трёх групп символов: *пропозициональных переменных:* $a, b, c, d, \dots, б_{345}, v_{964}, \dots$, *логических связок:* $\overline{\bullet}$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$ и *служебных символов:* (,).

Правила построения формул исчисления высказываний известны:

(Ф1): *любая пропозициональная переменная является формулой.*

(Ф2): *если* A *и* B *– формулы, то* $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $\overline{A}$, $\overline{B}$ *– тоже формулы.*

(Ф3): *других формул нет.*

Аксиомы формального исчисления высказываний делятся на четыре группы *схем аксиом*, включающие *11* схем. Это значит, что в нижеследующих псевдоформулах буквы $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ – ***не символы алфавита теории***, вместо них можно подставлять любые формулы исчисления высказываний. Таким образом, эти *11* схем аксиом на самом деле представляют бесконечное количество аксиом.

Группа аксиом импликации:

(И1): $(\mathcal{A} \to (\mathcal{B} \to \mathcal{A}))$

(И2): $((\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})))$

Группа аксиом конъюнкции:

(К1): $(\mathcal{A} \wedge \mathcal{B}) \to \mathcal{A})$

(К2): $(\mathcal{A} \wedge \mathcal{B}) \to \mathcal{B})$

(К3): $(\mathcal{A} \to \mathcal{B}) \to ((\mathcal{A} \to C) \to (\mathcal{A} \to (\mathcal{B} \wedge C))))$

Группа аксиом дизъюнкции:

(Д1): $(\mathcal{A} \to (\mathcal{A} \vee \mathcal{B}))$

(Д2): $(\mathcal{B} \to (\mathcal{A} \vee \mathcal{B}))$

(Д3): $((\mathcal{A} \to C) \to ((\mathcal{B} \to C) \to (\mathcal{A} \vee \mathcal{B} \to C)))$

Группа аксиом отрицания:

(О1): $(\mathcal{A} \to \overline{\overline{\mathcal{A}}})$

(О2): $(\overline{\overline{\mathcal{A}}} \to \mathcal{A})$

(О3): $((\mathcal{A} \to \mathcal{B}) \to (\overline{\mathcal{B}} \to \overline{\mathcal{A}}))$

В дальнейшем будем опускать в формулах некоторые скобки, предполагая, что их можно расставить по правилам восстановления скобок § 3 главы I.

В приведённом списке аксиом отсутствует логическая связка $\leftrightarrow$. Это сделано из соображений экономии: известно, что эта связка является производной – она выражается через остальные. Желающие работать с ней, должны ввести ещё следующие две схемы аксиом:

Группа аксиом эквивалентности:

(Э1): $((\mathcal{A} \leftrightarrow \mathcal{B}) \to ((\mathcal{A} \to \mathcal{B}) \wedge (\mathcal{B} \to \mathcal{A})))$

(Э2): $(((\mathcal{A} \to \mathcal{B}) \wedge (\mathcal{B} \to \mathcal{A})) \to (\mathcal{A} \leftrightarrow \mathcal{B}))$

Единственным *правилом вывода* в формальном исчислении высказываний является уже знакомое правило *Modus ponens* ***(MP):*** $\dfrac{\mathcal{A},\ \mathcal{A} \to \mathcal{B}}{\mathcal{B}}$.

Доказательством формулы B в формальной теории исчисления высказываний называется конечная последовательность формул $B_1, \ldots, B_n$, где B_n совпадает с B, а каждая формула B_i $(1 \le i \le n)$ либо является аксиомой, либо получена из предыдущих формул B_j и B_k $(1 \le \overset{j}{k} < i)$ по правилу *Modus ponens*, т.е. $B_k = (B_j \to B_i)$ и применение правила *(MP)* таково: $\dfrac{B_j,\ B_j \to B_i}{B_i}$. Это значит, что из доказуемости формул B_j и $B_j \to B_i$ постулируется возможность сде-

лать вывод о доказуемости формулы B_i. Это далеко не очевидный логический ход, хотя многих птешит иллюзия, что он согласуется со здравым смыслом.

Формула B, для которой существует доказательство, называется *доказуемой в формальном исчислении высказываний*. В этом случае будем писать $\vdash B$. В частности, всякая аксиома A доказуема, т.к. её доказательством является последовательность формул, состоящая из единственной формулы A.

Примеры доказательств в формальном исчислении высказываний

1. $\vdash A \to A$

1 • $\underbrace{A}_{\mathcal{A}} \to (\underbrace{(A \to A)}_{\mathcal{B}} \to \underbrace{A}_{\mathcal{A}})$ ***(И1)***

2 • $(\underbrace{A}_{\mathcal{A}} \to (\underbrace{(A \to A)}_{\mathcal{B}} \to \underbrace{A}_{C})) \to ((\underbrace{A}_{\mathcal{A}} \to \underbrace{(A \to A)}_{\mathcal{B}}) \to (\underbrace{A}_{\mathcal{A}} \to \underbrace{A}_{C}))$ ***(И2)***

3 • $(\underbrace{A}_{\mathcal{A}} \to \underbrace{(A \to A)}_{\mathcal{B}}) \to (\underbrace{A}_{\mathcal{A}} \to \underbrace{A}_{C})$ ***MP(1, 2)***

4 • $\underbrace{A}_{\mathcal{A}} \to (\underbrace{A}_{\mathcal{B}} \to \underbrace{A}_{\mathcal{A}})$ ***(И1)***

5 • $\underbrace{A}_{\mathcal{A}} \to \underbrace{A}_{C}$ ***MP(3, 4)***

2. $\vdash A \wedge B \to B \wedge A$

1 • $(\underbrace{(A \wedge B)}_{\mathcal{A}} \to \underbrace{B}_{\mathcal{B}}) \to ((\underbrace{(A \wedge B)}_{\mathcal{A}} \to \underbrace{A}_{C}) \to (\underbrace{(A \wedge B)}_{\mathcal{A}} \to \underbrace{(B \wedge A)}_{\mathcal{B} \wedge C}))$ ***(К3)***

2 • $\underbrace{(A \wedge B)}_{\mathcal{A} \wedge \mathcal{B}} \to \underbrace{B}_{\mathcal{B}}$ ***(К2)***

3 • $(\underbrace{(A \wedge B)}_{\mathcal{A}} \to \underbrace{A}_{C}) \to (\underbrace{(A \wedge B)}_{\mathcal{A}} \to \underbrace{(B \wedge A)}_{\mathcal{B} \wedge C})$ ***MP(1, 2)***

4 • $\underbrace{(A \wedge B)}_{\mathcal{A} \wedge \mathcal{B}} \to \underbrace{A}_{\mathcal{A}}$ ***(К1)***

5 • $\underbrace{(A \wedge B)}_{\mathcal{A}} \to \underbrace{(B \wedge A)}_{\mathcal{B} \wedge C}$ ***MP(3, 4)***

3. $\vdash \overline{A} \to \overline{(A \wedge B)}$

1 • $(\underbrace{A \wedge B}_{\mathcal{A} \wedge \mathcal{B}}) \to \underbrace{A}_{\mathcal{A}}$ ***(К1)***

2 • $(\underbrace{A \wedge B}_{\mathcal{A}} \to \underbrace{A}_{\mathcal{B}}) \to (\underbrace{\overline{A}}_{\mathcal{B}} \to \underbrace{\overline{(A \wedge B)}}_{\overline{\mathcal{A}}})$ ***(О3)***

3 • $\underbrace{\overline{A}}_{\overline{\mathcal{B}}} \to \underbrace{\overline{(A \wedge B)}}_{\overline{\mathcal{A}}}$ ***MP(1, 2)***

II. Формальное исчисление предикатов. *Алфавит* этой теории – это алфавит исчисления предикатов. Он состоит из *пропозициональных переменных:* a, b, c_{99}, d_{345}, … , *объектных переменных:* x, y, z_{99}, t_{345}, … , *логических связок:* $\overline{\bullet}$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$, *предикатных символов:* $P^{(1)}(\_)$, $Q^{(1)}(\_)$, … , $P^{(2)}(\_\ ,\_)$, $Q^{(2)}(\_\ ,\_)$, … , *кванторов:* $\forall$, $\exists$ и *служебных символов:* $(\ ,\ )$.

Правила построения формул исчисления предикатов известны:

(Ф1): *любая формула исчисления высказываний (от пропозициональных переменных) является формулой исчисления предикатов, в которой нет объектных переменных и кванторов. В этой формуле нет вхождений объектных переменных.*

(Ф2): *если* $P^{(n)}(\_\ ,\dots,\_\ )$ *– предикатный символ от* n *переменных и* $x_1,\dots,x_n$ *– объектные переменные, то* $P^{(n)}(x_1,\dots,x_n)$ *– формула исчисления предикатов, в которой все вхождения объектных переменных* $x_1,\dots,x_n$ *свободны, а вхождений других объектных переменных нет.*

(Ф3): *если* A *и* B *– две формулы, то* $(A\wedge B)$, $(A\vee B)$, $(A\to B)$, $(A\leftrightarrow B)$, $\overline{A}$, $\overline{B}$ *– тоже формулы, в которых свободны все вхождения объектных переменных, свободные в* A *или в* B, *и связаны все вхождения объектных переменных, связанные в* A *или в* B.

(Ф4): *если* $A(x)$ *– формула* ***хотя бы с одним свободным вхождением объектной переменной*** x, *то выражения* $(\forall x\ A(x))$ *и* $(\exists x\ A(x))$ *– формулы, в которых связаны вхождения всех объектных переменных, связанных в* A, *а также все вхождения* x, *и свободны все вхождения объектных переменных, свободные в* A, *кроме переменной* x. *При этом формула* $A(x)$ *называется областью действия квантора.*

(Ф5): *других формул нет.*

Аксиомы формального исчисления предикатов получаются добавлением ко всем аксиомам формального исчисления высказываний ещё одной группы схем аксиом с кванторами:

Группа аксиом с кванторами:

$(\forall)$: $(\forall x\ A(x))\to A(t)$, $\qquad$ $(\exists)$: $A(t)\to(\exists x\ A(x))$

Здесь t ***– переменная, отличная от переменной*** x.

Таким образом, получается 13 схем аксиом, которые на самом деле представляют бесконечное количество аксиом.

Правила вывода в формальном исчислении предикатов:

$$(MP):\quad \frac{A,\ A\to B}{B},$$

$$(B\forall):\quad \frac{C\to A(x)}{C\to(\forall x\ A(x))}\quad \textbf{(введение квантора } \forall),$$

$$(B\exists):\quad \frac{A(x)\to C}{(\exists x\ A(x))\to C}\quad \textbf{(введение квантора } \exists),$$

где C не содержит вхождений переменной x.

Понятия *доказательства формулы* и *доказуемой формулы* в формальной теории исчисления предикатов такие же, как в формальном исчислении высказываний.

Примеры доказательств в формальном исчислении предикатов

1. $\vdash (\forall x\ P(x)) \to (\exists x\ P(x))$

1 • $(\forall x P(x)) \to P(t)$ ***(∀)***

2 • $P(t) \to (\exists x P(x))$ ***(∃)***

3 • $(\underbrace{P(t) \to (\exists x P(x))}_{A}) \to ((\underbrace{\forall x P(x)}_{B}) \to (\underbrace{P(t) \to (\exists x P(x))}_{A}))$ ***(И1)***

4 • $(\underbrace{\forall x P(x)}_{B}) \to (\underbrace{P(t) \to (\exists x P(x))}_{A})$ ***MP(2, 3)***

5 • $((\underbrace{\forall x P(x)}_{A}) \to (\underbrace{P(t)}_{B} \to \underbrace{(\exists x P(x))}_{C})) \to$

$\to (((\underbrace{\forall x P(x)}_{A}) \to \underbrace{P(t)}_{B}) \to ((\underbrace{\forall x P(x)}_{A}) \to \underbrace{(\exists x P(x))}_{C}))$ ***(И2)***

6 • $((\underbrace{\forall x P(x)}_{A}) \to \underbrace{P(t)}_{B}) \to ((\underbrace{\forall x P(x)}_{A}) \to \underbrace{(\exists x P(x))}_{C})$ ***MP(4, 5)***

7 • $(\underbrace{\forall x P(x)}_{A}) \to \underbrace{(\exists x P(x))}_{C}$ ***MP(1, 6)***

2. Анализ приведённого доказательства показывает, что аналогично можно обосновать правило вывода $\dfrac{\vdash A \to B\ ;\ \vdash B \to C}{\vdash A \to C}$ (***правило силлогизма***), которое можно использовать в дальнейшем. Обоснование следует доказательству примера **1**.

1 • $A \to B$ ***(дано)***

2 • $B \to C$ ***(дано)***

3 • $(B \to C) \to (A \to (B \to C))$ ***(И1)***

4 • $(A \to (B \to C))$ ***MP(2, 3)***

5 • $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ ***(И2)***

6 • $(A \to B) \to (A \to C)$ ***MP(4, 5)***

7 • $A \to C$ ***MP(1, 6)***

3. $\vdash (\forall x\ P(x)) \to (\forall y\ P(y))$

1 • $(\forall x\ P(x)) \to P(y)$ ***(∀)***

2 • $(\forall x\ P(x)) \to (\forall y\ P(y))$ ***(В ∀)(1)***

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

1 • $(\forall x (\forall y\ P(x, y))) \to (\forall y\ P(u, y))$ ***(∀)***

2 • $(\forall y\ P(u, y)) \to P(u, v)$ ***(∀)***

3 • $(\forall x (\forall y\ P(x, y))) \to P(u, v)$ ***силлогизм(1, 2)***

4 • $(\forall x (\forall y\ P(x, y))) \to (\forall u\ P(u, v))$ ***(В ∀)***

5 • $(\forall u\ P(u, v)) \to (\forall x\ P(x, v))$ ***(пример 3)***

6 • $(\forall x (\forall y\ P(x, y))) \to (\forall x\ P(x, v))$ ***силлогизм(4, 5)***

7 • $(\forall x\ P(x, v)) \to (\forall v (\forall x\ P(x, v)))$ ***(В ∀)***

8 • $(\forall x (\forall y\ P(x, y))) \to (\forall v (\forall x\ P(x, v)))$ ***силлогизм(6, 7)***

9 • $(\forall v (\forall x\ P(x, v))) \to (\forall y (\forall x\ P(x, y)))$ ***(пример 3)***

10 • $(\forall x (\forall y\ P(x, y))) \to (\forall y (\forall x\ P(x, y)))$ ***силлогизм(8, 9)***

III. Специальные формальные теории. Теория предикатов создавалась, чтобы дать возможность любой конкретной науке формулировать свойства изучаемых объектов на общем логическом языке и доказывать свои теоремы едиными средствами. Поэтому теория предикатов является неотъемлемой частью любой содержательной математической теории.

Вместе с тем, в каждой специальной математической теории рассматриваются свои, специфические предикаты, функции, объекты особого назначения и формулируются аксиомы, постулирующие свойства этих объектов, предикатов и функций. Специальная теория не имеет специфических правил вывода, а пользуется только правилами вывода теории предикатов.

Более формально, *алфавит специальной теории* состоит из нескольких групп символов:

- достаточно большое количество *переменных* $x, y, \ldots, x_{100}, \ldots$ для обозначения объектов теории,
- *символы выделенных элементов* $c, d, \ldots, c_{129}, \ldots$ *– константы –* для обозначения объектов особого назначения,
- *функциональные символы* $f_1^{(k_1)}, \ldots, f_s^{(k_s)}, \ldots$ для обозначения специфических операций и функций, используемых в аксиомах специальной теории,
- *предикатные символы* $P_1^{(k_1)}, \ldots, P_s^{(k_s)}, \ldots$ для обозначения специфических предикатов, используемых в аксиомах специальной теории,
- $\wedge, \vee, \to, \leftrightarrow, \overline{\bullet}$ *– логические связки,*
- $\forall, \exists$ *– кванторы,*
- *служебные символы* $-$ $(\ ,\ )$ (скобки).

Понятие *формулы специальной теории* несколько усложняется из-за наличия функциональных символов. Вначале от простого к сложному вводится понятие *терма (функционального выражения специальной теории) :*

(Т1): *любая объектная переменная является термом.*

(Т2): *любая константа (символ выделенного элемента) является термом.*

(Т3): *если* $t_1, \dots, t_m$ *– термы, а* $f^{(m)}$ *– один из функциональных символов теории, то* $f^{(m)}(t_1, \dots, t_m)$ *– терм.*

(Т4): *других термов нет.*

Теперь от простого к сложному строится понятие *формулы специальной теории:*

(Ф1): *если* $t_1, \dots, t_m$ *– термы, а* $P^{(m)}$ *– один из предикатных символов теории, то* $P^{(m)}(t_1, \dots, t_m)$ *– бескванторная формула, зависящая от всех переменных, участвующих в термах* $t_1, \dots, t_m$*, причём все её переменные свободны.*

(Ф2): *если* A *и* B *– две формулы, то* $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$, $\overline{A}$, $\overline{B}$ *– тоже формулы, в которых свободны все вхождения объектных переменных, свободные в* A *или в* B*, и связаны все вхождения объектных переменных, связанные в* A *или в* B*.*

(Ф3): *если* $A(x)$ *– формула* ***хотя бы с одним свободным вхождением объектной переменной*** x*, то выражения* $(\forall x\ A(x))$ *и* $(\exists x\ A(x))$ *– формулы, в которых связаны вхождения всех объектных переменных, связанных в* A*, а также все вхождения* x*, и свободны все вхождения объектных переменных, свободные в* A*, кроме переменной* x*. При этом формула* $A(x)$ *называется областью действия квантора.*

(Ф4): *других формул нет.*

Система аксиом специальной теории состоит из

- *аксиом формального исчисления предикатов,*
- *специальных аксиом теории.*

При этом, как правило, явно формулируются только специальные аксиомы, а аксиомами исчисления предикатов пользуются без лишних оговорок.

Правила вывода специальной теории, понятия *доказательства формулы* и *доказуемой формулы* те же, что и в формальной теории предикатов.

IV. Пример специальной теории: формальная арифметика. *Алфавит* состоит из нескольких групп символов:

- достаточно большое количество *переменных* $x, y, \ldots, x_{100}, \ldots$ для обозначения натуральных чисел,
- *1 – выделенный элемент*,
- $+, \cdot$ *– знаки бинарных арифметических операций сложения и умножения*,
- $=$ *– единственный предикатный символ равенства чисел*,
- $\wedge, \vee, \rightarrow, \leftrightarrow, \overline{\bullet}$ *– логические связки*,
- $\forall, \exists$ *– кванторы*,
- *(,)* – *служебные символы* (скобки).

Термы формальной арифметики – это просто *арифметические выражения*, которые строятся от простого к сложному так:

(АВ1): *любая переменная является арифметическим выражением.*

(АВ2): *1 – арифметическое выражение.*

(АВ2): *если* A *и* B *– арифметические выражения, то* $(A + B)$ *и* $(A \cdot B)$ *– тоже арифметические выражения.*

(АВ3): *других арифметических выражений нет.*

Примеры: 1. $1 + x$ – не арифметическое выражение, т.к. нет скобок.

2. $((x + 1) \cdot (z + t))$ – арифметическое выражение.

Формулы арифметики тоже определяются от простого к сложному:

(Ф1): *если* A, B *– два арифметических выражения, то* $(A = B)$ *– бескванторная формула, зависящая от всех переменных, участвующих как в* A*, так и в* B*, причём все её переменные свободны.*

(Ф2): *если* A *и* B *– две формулы, то* $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, $(A \leftrightarrow B)$, $\overline{A}$, $\overline{B}$ *– тоже формулы, в которых свободны все вхождения объектных переменных, свободные в* A *или в* B*, и связаны все вхождения объектных переменных, связанные в* A *или в* B*.*

(Ф3): *если* $A(x)$ *– формула* ***хотя бы с одним свободным вхождением объектной переменной*** x*, то выражения* $(\forall x\ A(x))$ *и* $(\exists x\ A(x))$ *– формулы, в которых связаны вхождения всех объектных переменных, связанных в* A*, а также все вхождения* x*, и свободны все вхождения объектных переменных, свободные в* A*, кроме переменной* x*. При этом формула* $A(x)$ *называется областью действия квантора.*

(Ф4): *других формул нет.*

Примеры: 1. $((x = 1) \wedge (y \cdot x+1 = 1))$ – бескванторная формула со свободными переменными x и y.

2. $((x + 1)\cdot(z + t) + 1) = (t)$ – не формула (лишние скобки в правой части).

3. $(\forall t\ ((x + 1)\cdot(z + t) + 1) = (t + x + 1))$ – формула с квантором, связывающим переменную t и свободными переменными x, z.

Аксиомы формальной арифметики кроме аксиом исчисления предикатов включают несколько групп аксиом:

Аксиомы равенства:

Рефлексивность: $(\forall\ x\ (x = x))$

Симметричность: $(\forall\ x\ (\forall y\ ((x = y)\ \rightarrow\ (y = x)))$

Транзитивность: $(\forall\ x\ (\forall\ y\ (\forall\ z\ (((x = y)\ \wedge\ (y = z))\ \rightarrow\ (x = z))))$

Схема подстановки: *для любых арифметических выражений* $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ *с выделенным вхождением выражения* $\mathcal{B}$ *в* $\mathcal{A}$ *(символически* $\mathcal{A} = \mathcal{A}(\mathcal{B})$*) следующая формула является аксиомой* $((\mathcal{B} = \mathcal{C}) \rightarrow (\mathcal{A}(\mathcal{B}) = \mathcal{A}(\mathcal{C})))$, *где* $\mathcal{A}(\mathcal{C})$ *– результат замены выделенного вхождения подвыражения* $\mathcal{B}$ *в* $\mathcal{A}$ *на* $\mathcal{C}$.

Это – очень сильная форма подстановки, её можно значительно ослабить.

Условимся для арифметических выражений $\mathcal{A}(x_1, \ldots, x_n)$ и $\mathcal{B}(y_1, \ldots, y_m)$ использовать краткую запись $\mathcal{A}(x_1, \ldots, x_n) \neq \mathcal{B}(y_1, \ldots, y_m)$ вместо отрицания $\overline{\mathcal{A}(x_1, \ldots, x_n) = \mathcal{B}(y_1, \ldots, y_n)}$.

Аксиомы операций сложения и умножения:

Существование и единственность следующего: $(\forall\ x\ (\exists!\ y\ (y = x + 1)))$

Единица – наименьший элемент: $(\forall\ x\ ((x + 1) \neq 1))$

Равенство следующих: $(\forall\ x\ (\forall\ y\ ((x + 1) = (y + 1)) \leftrightarrow (x = y)))$

Ассоциативность прибавления 1: $(\forall\ x\ (\forall\ y\ ((x + (y + 1)) = ((x + y) + 1))))$

Единица – нейтральна по умножению: $(\forall\ x\ ((x\cdot 1) = x))$

Связь сложения и умножения: $(\forall\ x\ (\forall\ y\ ((x\cdot(y + 1) = ((x\cdot y) + x)))))$

Схема формальной индукции

Для любой формулы арифметики $\mathcal{A}(x)$ *со свободной переменной* x *следующая формула является аксиомой:* $((\mathcal{A}(1) \wedge (\forall\ y\ \ (\mathcal{A}(y) \rightarrow \mathcal{A}(y + 1)))) \rightarrow (\forall\ x\ \mathcal{A}(x)))$.

Правила вывода формальной арифметики, понятия *доказательства формулы* и *доказуемой формулы* в формальной арифметике такие же, как в формальном исчислении предикатов.

Примеры теорем формальной арифметики

Введём обычные обозначения: $2 = (1 + 1)$, $3 = (2 + 1) = ((1 + 1) + 1)$, $4 = (3 + 1) = (((1 + 1) + 1) + 1)$, и.т.д.

1. $\vdash (4 = (2 + 2))$

1 • $(\forall x\ (\forall y\ ((x + (y + 1)) = ((x + y) + 1))))$ ***(аксиома ассоциативности +)***

2 • $(\forall y\ (((1 + 1) + (y + 1)) = (((1 + 1) + y) + 1)))$ ***(аксиома $\forall(x = 1+1)$)***

3 • $(((1 + 1) + (1 + 1)) = (((1 + 1) + 1) + 1))$ ***(аксиома $\forall(y = 1)$)***

4 • $(((1 + 1) + 1) + 1) = ((1 + 1) + (1 + 1)))$ ***(аксиома симметричности)***

5 • $((1 + 1) = 2)$ ***(определение)***

6 • $((1 + 1) = 2) \rightarrow (((1 + 1) + 1) + 1) = (2 + 2))$ ***(подстановка)***

7 • $(((1 + 1) + 1) + 1) = (2 + 2))$ ***MP(5, 6)***

8 • $((((1 + 1) + 1) + 1) = 4)$ ***(определение)***

9 • $((((1 + 1) + 1) + 1) = 4) \rightarrow (4 = (2 + 2)))$ ***(подстановка)***

10 • $(4 = (2 + 2))$ ***MP(8, 9)***

2. $\vdash (2\cdot2 = 4)$

1 • $(\forall x\ (\forall y\ ((x\cdot(y + 1)) = ((x\cdot y) + x))))$ ***(аксиома связи + и ·)***

2 • $(\forall y\ ((2\cdot(y + 1)) = ((2\cdot y) + 2))))$ ***(аксиома $\forall(x = 2)$)***

3 • $((2\cdot(1 + 1)) = ((2\cdot1) + 2)))$ ***(аксиома $\forall(y = 1)$)***

4 • $(\forall x\ ((x\cdot1) = x))$ ***(аксиома о нейтральности 1)***

5 • $2\cdot1 = 2$ ***(аксиома $\forall(5)$)***

6 • $((2\cdot1 = 2) \rightarrow ((2\cdot1) + 2) = (2 + 2)))$ ***(подстановка)***

7 • $(((2\cdot1) + 2) = (2 + 2))$ ***MP(5, 6)***

8 • $((2 + 2) = 4)$ ***доказано***

9 • $(((2 + 2) = 4) \rightarrow (((2\cdot1) + 2) = 4))$ ***(подстановка)***

10 • $(((2\cdot1) + 2) = 4)$ ***MP(8, 9)***

11 • $(2 = (1+ 1))$ ***(определение)***

12 • $(2 = (1+ 1)) \rightarrow ((2\cdot2) = ((2\cdot1) + 2)))$ ***(подстановка в 3)***

13 • $((2\cdot2) = ((2\cdot1) + 2))$ ***MP(11, 12)***

14 • $((2\cdot2) = ((2\cdot1) + 2)) \rightarrow (2\cdot2 = 4)$ ***(подстановка 10 в 13)***

15 • $(2\cdot2 = 4)$ ***MP(13, 14)***

Приведём ещё пример неформального доказательства в формальной арифметике, использующий правила вывода и аксиому индукции. Докажем, формулу $\forall x\ ((x = 1) \vee (\exists y\ ((x = 2\cdot y) \vee (x = 2\cdot y + 1))))$, выражающую тот факт, что любое натуральное число либо чётно, либо нечётно.

Пусть $\mathcal{A}(x) = (x = 1) \vee (\exists y\ (x = 2\cdot y) \vee (x = 2\cdot y + 1))$. Тогда ясно, что $\mathcal{A}(1)$ доказуемо, т.к. $\mathcal{A}(1) = ((1 = 1) \vee (\exists y\ (1 = 2\cdot y) \vee (1 = 2\cdot y + 1)))$, и первый аргумент этой дизъюнкции является аксиомой (?!). Теперь, чтобы воспользоваться схемой индукции, нужно доказать $(\forall z\ (\mathcal{A}(z) \to \mathcal{A}(z + 1)))$.

Если доказано $\mathcal{A}(z) = (\exists y\ ((z = 2\cdot y) \vee (z = 2\cdot y + 1)))$, то $\mathcal{A}(z+1)$ означает, что $(\exists t\ ((z + 1 = 2\cdot t) \vee (z + 1 = 2\cdot t + 1)))$. В том случае, когда $z = 2\cdot y$, имеем $z + 1 = 2\cdot y + 1$, и в качестве искомого t можно взять $t = y$. В случае $z = 2\cdot y + 1$ получаем $z + 1 = (2\cdot y + 1) + 1 = 2\cdot y + 2 = 2\cdot(y+1)$, и в качестве искомого t можно взять $t = y + 1$.

Таким образом, неформально доказана формула $(\forall z\ (\mathcal{A}(z) \to \mathcal{A}(z + 1)))$ и по схеме индукции, можно заключить, что доказана и формула $(\forall x\ \mathcal{A}(x))$.

Упражнения: 1. Что в этом доказательстве неформального ?

2. Формализуйте доказательство.

Как видно из приведённых примеров, доказательство даже простейших теорем в формальной аксиоматической теории довольно громоздко. Для того чтобы дать возможность при доказательствах теорем рассуждать менее формально и не повторять многократно одни и те же куски похожих доказательств удобно в любой специальной теории (как и в теориях формального исчисления высказываний и формального исчисления предикатов) ввести понятие *выводимости формулы из конечной совокупности формул* Γ.

Пусть $\Gamma = \{\Phi_1, \dots, \Phi_k\}$ – конечное множество формул (возможно пустое). Говорят, что формула B *выводима из множества формул* Γ, если существует конечная цепочка формул $B_1, \dots, B_n$, где B_n совпадает с B, а каждая формула B_i $(1 \le i \le n)$ либо является аксиомой, либо принадлежит Γ, либо получена из некоторых предыдущих формул B_j и B_k $(1 \le j < i,\ 1 \le k < i)$ по правилам вывода теории. Факт выводимости формулы B из совокупности Γ обозначается через $\Gamma \vdash B$.

Ясно, что формула B доказуема тогда и только тогда, когда она выводима из пустого множества формул: $\vdash B$. С другой стороны, если все формулы, входящие в $\Gamma = \{\Phi_1, \dots, \Phi_k\}$, доказуемы, а B выводима из Γ, то B доказуема.

Действительно, чтобы получить доказательство формулы B, достаточно к её выводу $B_1, \ldots, B_n$ из формул Γ присоединить доказательства формул $\Phi_1, \ldots, \Phi_k$:

$$<\text{доказательство } \Phi_1>, \ldots, <\text{доказательство } \Phi_k>, B_1, \ldots, B_n -$$

это доказательство формулы B. Таким образом, для доказательства формулы достаточно вывести её из уже доказанных ранее формул.

Понятие выводимости аналогично понятию логического следования. В дальнейшем эта аналогия будет прослежена более подробно. Так, в § 3 будет доказана эквивалентность этих понятий для формальной теории исчисления высказываний. То же справедливо и для формальной теории исчисления предикатов. Таким образом, можно пользоваться при доказательствах формул изученными ранее правилами вывода, применяя их к выводимости формул.

Для простоты изложения в дальнейшем все рассматриваемые формальные теории, кроме исчислений высказываний и предикатов, предполагаются специальными.

§ 2. Непротиворечивость аксиоматических теорий

Система аксиом формальной теории, как и сама теория, называются *непротиворечивой*, если не существует такой формулы Φ этой формальной теории, что Φ и $\overline{\Phi}$ доказуемы. При исследовании непротиворечивости теории полезно учитывать следующую теорему:

Теорема (компактности). *Система аксиом специальной теории непротиворечива тогда и только тогда, когда непротиворечива любая её конечная подсистема.*

Доказательство. Ясно, что из непротиворечивости системы аксиом следует непротиворечивость и любой конечной подсистемы аксиом.

Обратно, пусть непротиворечива каждая конечная подсита системы аксиом, но сама теория противоречива. Тогда из системы аксиом выводятся формулы Φ и $\overline{\Phi}$:

1 • *доказательство формулы* Φ $\}\ \Gamma_1$
2 • Φ
3 • *доказательство формулы* $\overline{\Phi}$ $\}\ \Gamma_2$
4 • $\overline{\Phi}$

Таким образом, $\Gamma \vdash \Phi$ и $\Gamma \vdash \overline{\Phi}$, где $\Gamma = \Gamma_1 \cup \Gamma_2 -$ конечное множество.

Теорема доказана.

По сути дела эта теорема обращает внимание на свойство конечности математических рассуждений.

Требование непротиворечивости является основным для каждой содержательной теории. Дело в том, что если теория противоречива, т.е. исходя из её аксиом с помощью допустимых в ней правил вывода можно доказать формулы Φ и $\overline{\Phi}$, то можно доказать и любую другую формулу. Формальное доказательство этого факта будет дано в § 6, где будут обоснованы доказанные в § 7 главы I правила вывода, а пока воспользуемся доказанными неформально правилами вывода расширения посылок $\dfrac{\Gamma \vdash \mathcal{B}}{\Gamma, \mathcal{A} \vdash \mathcal{B}}$ и *modus tollens*: $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma \vdash \overline{\mathcal{B}}}{\Gamma \vdash \overline{\mathcal{A}}}$. С их помощью дополним доказательства формул Φ и $\overline{\Phi}$ до доказательства произвольной формулы A: ввиду теоремы компактности, $\Gamma \vdash \Phi$ и $\Gamma \vdash \overline{\Phi}$, где Γ – некоторое конечное множество аксиом. По правилу расширения посылок, $\Gamma, \overline{A} \vdash \Phi$, и по правилу *modus tollens*, $\Gamma \vdash \overline{\overline{A}}$. Отсюда легко вывести $\Gamma \vdash A$:

- $\overline{\overline{A}}$
- $\overline{\overline{A}} \to A$ ***(аксиома)***
- A ***(MP)***

Хотя проведённое доказательство и не вполне формальное, но его можно формализовать, используя результаты следующего параграфа.

Таким образом, в противоречивой теории все формулы доказуемы, и сама такая теория не представляет интереса.

Теорема (о непротиворечивости формального исчисления высказываний). *Формальное исчисление высказываний непротиворечиво.*

Доказательство. Нетрудно проверить, что все аксиомы формального исчисления высказываний представляют из себя тождественно истинные формулы. Кроме того, по правилу *modus ponens* $\dfrac{\mathcal{A},\ \mathcal{A} \to \mathcal{B}}{\mathcal{B}}$ разрешается получать формулу $\mathcal{B}$ из уже доказанных, а потому (можно считать) тождественно истинных формул $\mathcal{A}$ и $\mathcal{A} \to \mathcal{B}$. Легко понять, что и сама формула $\mathcal{B}$ в этом случае будет тождественно истинной.

Таким образом, все доказуемые в формальном исчслении высказываний формулы являются тождественно истинными. Значит, если доказуема формула Φ, то формула $\overline{\Phi}$ доказуемой быть не может, поскольку тождественно ложна.

Теорема доказана.

Теорема (о непротиворечивости формального исчисления предикатов). *Формальное исчисление предикатов непротиворечиво.*

Доказательство этой теоремы можно получить по той же схеме, что и доказательство предыдущего результата, если аналогично предыдущему обратить внимание на то, что в формальной теории предикатов доказуемы только тождественно истинные формулы: все аксиомы тождественно истинны, а применение правил вывода *modus ponens* и введения кванторов $\dfrac{C \to A(x)}{C \to (\forall x\, A(x))}$, $\dfrac{A(x) \to C}{(\exists x\, A(x)) \to C}$ не выводит за пределы тождественно истинных формул. Таким образом, любая выполнимая формула не может быть доказана в формальной теории предикатов.

Теорема доказана.

Эта теорема Гёделя, доказанная в 1930 г. XX в., обосновывалась им, почти не опираясь на аксиоматику теории множеств, чего не скажешь о приведённом выше коротком доказательстве этой теоремы. Дело в том, что оно использует понятие тождественно истинной формулы, которое оперирует понятием интерпретации, базирующимся, в свою очередь, на понятиях множества и предиката, т.е. использует аксиомы и некоторые нетривиальные факты теории множеств. Таким образом, приведённые доказательства теорем о непротиворечивости не являются формальными доказательствами в рамках самих формальных теорий исчисления высказываний и предикатов.

Всё-таки полученные доказательства непротиворечивости простейших математических теорий вселяли надежду на то, что вскоре удастся формальными методами доказать непротиворечивость других, более содержательных, математических теорий, а затем, быть может, и всей математики. Такова была программа Д. Гильберта формального обоснования математики. Однако, этим надеждам не суждено было сбыться: в 1931 г. К. Гёдель доказал, что непротиворечивость формальной арифметики не может быть доказана средствами этой формальной теории, так же как и непротиворечивость любой конструктивно аксиоматизируемой содержательной теории, включающей в себя теорию формальной арифметики. Более точно, результат К. Гёделя формулируется так:

Теорема (обобщённая теорема Гёделя о неполноте). *Если конструктивно аксиоматизируемая формальная теория включает в себя формальную арифметику и непротиворечива, то можно указать конкретную формулу этой тео-*

рии, которая, как и её отрицание, не доказуемы в рассматриваемой формальной теории. В качестве такой формулы можно взять, например, формулу, выражающую факт недоказуемости теоремы арифметики (0 ≠ 1) в этой формальной теории, т.е. непротиворечивость этой формальной теории.

Использованный здесь термин "конструктивно аксиоматизируемая теория" не является общепринятым, подробно его обсуждать не будем. Отметим только, что в такой теории можно все её формулы так эффективно занумеровать натуральными числами, что будет существовать эффективный алгоритм, определяющий по заданному номеру формулы, является эта формула аксиомой теории или нет. Кроме того, существует аналогичная эффективная нумерация правил вывода такой теории, и утверждение о доказуемости любой формулы само записывается в виде формулы. Эти условия выполнены, например, для теории формальной арифметики и для многих других естественно возникающих теорий. Точную формулировку, доказательство и комментарии к теореме Гёделя можно найти в книге [12 ниже, стр. 67-79].

Таким образом, реализация программы формализации математики оказалась невозможной: в рамках содержательной формальной теории нельзя обосновать непротиворечивость этой теории. Это не исключает возможности обоснования этой теории средствами какой-либо более широкой теории. Однако обоснование непротиворечивости этой более широкой теории требует нового расширения теории, и.т.д. Например, непротиворечивость формальной арифметики была обоснована Г. Генценом, используя трансфинитную индукцию, применяемую в теории множеств (см. § 2 приложения). Но обоснование непротиворечивости самой теории множеств требует выхода уже за рамки теории множеств.

§ 3. Полнота аксиоматических теорий

Любая содержательная формальная теория строится для обоснования рассуждений в некоторых содержательных теориях. Возникает вопрос: насколько полно описывает формальная теория соответствующую содержательную теорию ? Более точно: насколько тесно связаны понятия истинности формулы в формальной теории и в содержательной ?

Для формальной теории истинность теоремы означает, прежде всего, её доказуемость. Для содержательной теории утверждение истинно, если оно истинно в любой модели данной теории. Таким образом, и для любой формальной теории

возникают *a' priori* два понимания истинности формулы: доказуемость и *тождественная истинность* (*истинность* при любой интерпретации рассматриваемой теории).

Интерпретация формальной теории (или *модель теории*) определяется аналогично введённому выше (см. § 4 главы II) понятию интерпретации для множества формул исчисления предикатов. Не вдаваясь в формальности, ограничимся только намёком: *модель теории (или интерпретация)* – это некоторое множество вместе с зафиксированными на нём конкретными константами, предикатами и функциями для всех выделенных константных, предикатных и функциональных символов, участвующих в аксиомах теории. При этом ***требуется, чтобы все аксиомы теории в любой интерпретации этой теории представляли собой истинные в этой модели утверждения***.

Если фиксирована интерпретация теории, то любая *замкнутая* формула теории после замены всех участвующих в ней символов на соответствующие конкретные высказывания, объекты, предикаты и функции этой интерпретации становится высказыванием, которое может быть истинным или ложным. Под *замкнутой формулой* здесь и далее понимается формула, все вхождения объектных переменных которой связаны. Таким образом, можно говорить об истинности или ложности замкнутой формулы теории на модели теории.

Для незамкнутой формулы $A(x_1, \dots, x_n)$ теории со свободными объектными переменными $x_1, \dots, x_n$ можно ввести понятие *интерпретации формулы теории*: это – любая модель теории вместе с фиксированными объектами $o_1, \dots, o_n$ для свободных переменных. После замены в этой формуле всех участвующих в ней символов на соответствующие конкретные высказывания, объекты, предикаты и функции модели, а переменных $x_1, \dots, x_n$ – на объекты $o_1, \dots, o_n$ получится высказывание, которое может быть истинным или ложным. Значит, можно говорить о *значениях формулы теории при её интерпретациях*, и о *тождественно истинных формулах теории* – формулах, принимающих значение *истина* при любой интерпретации. При этом незамкнутая формула $A(x_1, \dots, x_n)$ теории со свободными объектными переменными $x_1, \dots, x_n$ тождественно истинна тогда и только тогда, когда тождественно истинна замкнутая формула той же теории $(\forall x_1 (\forall x_2 (\dots (\forall x_n \; A(x_1, \dots, x_n)))))$.

Замечания: 1. ***При интерпретации специальной теории все логические связки и кванторы интерпретируются стандартным образом*** (в соответствии с неформальными аксиомами § 3 главы I и § 1 главы II).

2. ***При интерпретации формальных теорий исчисления высказываний и предикатов сами истинностные значения логических связок, как и истинностные значения формул, полученных навешиванием кванторов, могут изменяться*** (подробнее об этом см. § 5).

Ясно, что правила вывода теории предикатов, применённые к тождественно истинным формулам, снова приводят к тождественно истинным формулам. Поэтому ***любая доказуемая формула специальной теории является тождественно истинной***. Таким образом, сформулированный выше вопрос полноты можно поставить так: *верно ли, что любая тождественно истинная формула* ***специальной*** *формальной теории доказуема ?* Этот вопрос нетривиален даже для формальной теории исчисления предикатов (для формальной теории исчисления высказываний он будет решён положительно (но не просто) в § 6).

Система аксиом формальной теории, как и сама теория, называется *полной в широком смысле*, если любая тождественно истинная формула этой формальной теории доказуема.

Теорема (о полноте в широком смысле). *Любая непротиворечивая специальная теория полна в широком смысле.*

Доказательство. Используем (без доказательства) следующую нетривиальную теорему:

Теорема (о существовании модели). *Теория непротиворечива тогда и только тогда, когда она имеет модель.*

Если теперь A – некоторая недоказуемая, но тождественно истинная формула некоторой специальной теории, то формула $\overline{A}$ также недоказуема: если бы она была доказуема, то $\overline{A}$ была бы истинной в каждой модели, вопреки тождественной истинности формулы A. Более того, присоединение к аксиомам рассматриваемой теории формулы $\overline{A}$ приводит к противоречивой теории: если бы эта новая теория была бы непротиворечива, то у неё существовала бы модель, в которой была бы истинна формула $\overline{A}$, что невозможно ввиду тождественной истинности формулы A. Итак, существует такое конечное множество Γ аксиом исходной теории, что $\Gamma,\ \overline{A} \vdash \Phi$ и $\Gamma,\ \overline{A} \vdash \overline{\Phi}$. По правилу опровержения $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma, \mathcal{A} \vdash \overline{\mathcal{B}}}{\Gamma \vdash \overline{\mathcal{A}}}$ отсюда получим $\Gamma \vdash \overline{\overline{A}}$, т.е. (с учётом аксиомы $\overline{\overline{A}} \to A$ и правила силлогизма) $\Gamma \vdash A$.

Теорема доказана.

Итак, понятие доказуемости формулы формальной теории совпадает с понятием тождественной истинности. Этот факт укреплял уверенность математиков в том, что программа Гильберта обоснования математики путём формализации приведёт к успеху.

Систему аксиом или саму теорию назовём *полной*, если для любой замкнутой формулы Φ этой теории доказуема либо сама формула Φ, либо её отрицание $\overline{\Phi}$. Система аксиом формальной теории, как и сама теория, называется *полной в узком смысле*, если добавление любой недоказуемой в этой теории замкнутой формулы к списку аксиом теории приводит к противоречивой теории. Наконец, теорию или её систему аксиом назовём *ф-категоричной*, если для любой её модели множества истинных в этой модели замкнутых формул теории одно и то же. Приведённое определение ϕ-категоричности не совпадает с общепринятым определением *категоричности* теории, которое требует понятия изоморфизма моделей, не рассматриваемое в этих лекциях.

Следует отметить, что далеко не каждая содержательная математическая теория полна: утверждение о доказуемости отрицания недоказуемого математического утверждения не верно. Например, утверждение, представляющее аксиому параллельности Евклида (через каждую точку плоскости, не лежащую на заданной прямой, проходит ровно одна прямая, параллельная этой прямой) недоказуемо в системе аксиом абсолютной геометрии, как и его отрицание.

Теорема (о взаимосвязях понятий полноты). *Следующие утверждения для любой специальной теории эквивалентны:*

(1) теория полна,

(2) теория полна в узком смысле,

(3) теория ф-категорична.

Доказательство. Ясно, что противоречивая теория полна, полна в узком смысле и ϕ-категорична (?!). Для непротиворечивой теории используем следующую схему доказательства:

$$\begin{array}{ccc} (1) & = & (1) \\ \Uparrow & & \Downarrow \\ (3) & \Leftarrow & (2) \end{array}.$$

(1) $\Rightarrow$ *(2)* Пусть теория полна, и замкнутая формула Φ не доказуема в этой теории. Тогда доказуема формула $\overline{\Phi}$, т.е. $\Gamma \vdash \overline{\Phi}$, где Γ – некоторое конечное множество аксиом теории. Нужно понять, что добавление формулы Φ к списку аксиом приводит к противоречивой теории. Действительно, $\Gamma, \Phi \vdash \overline{\Phi}$ и $\Gamma, \Phi \vdash \Phi$, что и требовалось доказать.

(2) ⇒ (3) Пусть специальная теория полна в узком смысле, но существует замкнутая формула Φ этой теории, истинная в одной модели этой теории и ложная в другой. Тогда формула Φ недоказуема, т.к. доказуемые формулы не могут быть ложными в моделях, причём добавление к исходной теории недоказуемой замкнутой формулы Φ не привело к противоречивой теории ввиду наличия модели расширенной теории. Это противоречие доказывает *(3)*.

(3) ⇒ (1) Пусть теория ϕ-категорична, но Φ – недоказуемая замкнутая формула этой теории, для которой $\overline{\Phi}$ также недоказуема. Присоединим недоказуемую формулу $\overline{\Phi}$ к списку аксиом теории.

Если полученная теория будет непротиворечива, то по теореме о существовании модели у неё существует модель, в которой $\overline{\Phi}$ истинна. Ввиду ϕ-категоричности $\overline{\Phi}$ тождественно истинна, и по теореме о полноте в широком смысле, $\overline{\Phi}$ доказуема – противоречие.

Если же полученная теория будет противоречива, то существует такое конечное множество Γ аксиом теории, что $\Gamma, \overline{\Phi} \vdash A$ и $\Gamma, \overline{\Phi} \vdash \overline{A}$ для некоторой формулы A. Отсюда по правилу опровержения $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma, \mathcal{A} \vdash \overline{\mathcal{B}}}{\Gamma \vdash \overline{\mathcal{A}}}$ получаем $\Gamma \vdash \overline{\overline{\Phi}}$, т.е. Φ доказуема (?!) – снова противоречие. Таким образом, либо Φ, либо $\overline{\Phi}$ доказуема, и теория полна.

Теорема доказана.

Как же обстоит дело со свойством полноты в трёх рассматриваемых модельных формальных теориях исчислений высказываний, предикатов и формальной теории арифметики ?

Для теорий исчисления высказываний и предикатов условие полноты не выполнено, что и неудивительно: это универсальные теории общего назначения, используемые в различных областях знания. Поэтому одна и та же формула (например, формула $(a \vee b)$ исчисления высказываний или формула $(\exists x\, P(x))$ исчисления предикатов) может быть истинна в одной модели, а в другой ложна. Таким образом, эти теории имеют много различных моделей, отличающихся истинными в них формулами, а потому не полны.

Теорема (о неполноте в узком смысле исчислений высказываний и предикатов). *Формальные теории исчисления высказываний и предикатов не полны в узком смысле, не ф-категоричны, но полны в широком смысле.*

Упражнения: 1. Докажите, что присоединение к исчислению высказываний в качестве аксиомы формулы x, где x – пропозициональная переменная, приводит к непротиворечивой теории.

2. Докажите, что присоединение к исчислению предикатов в качестве аксиомы формулы $(\exists\, x\, P(x))$, где x – объектная переменная, а $P(\_)$ – предикатный символ, приводит к непротиворечивой теории.

3. Докажите, что присоединение к аксиомам формальной арифметики формулы $(2\times 2=5)$ приводит к противоречивой теории.

Теорема (Линдебаума о пополнении теории). *Если специальная теория непротиворечива, то существует её полное непротиворечивое расширение.*

Доказательство. Докажем теоерему только в предположении, что все формулы теории можно перенумеровать натуральными числами (т.е. для счётных теорий), хотя её можно доказать и в общем случае, используя трансфинитную индукцию.

Пусть $\{\Phi_1, \Phi_2, \dots\}$ – множество всех замкнутых формул рассматриваемой непротиворечивой теории T. Построим последовательность непротиворечивых теорий $T = T_0 \subseteq T_1 \subseteq T_2 \subseteq \dots$, объединение которых $T_\infty = \bigcup_{i=0}^{\infty} T_i$ и будет искомой непротиворечивой полной теорией, содержащей исходную теорию T.

Полагаем $T_0 = T$ – непротиворечивая теория. Если уже построена непротиворечивая теория T_n $(n \geq 0)$, то для построения теории T_{n+1} рассмотрим формулу $\overline{\Phi_{n+1}}$. Если эта формула доказуема в теории T_n, то положим $T_{n+1} = T_n$, получая снова непротиворечивую теорию. Если же $\overline{\Phi_{n+1}}$ не доказуема в теории T_n, то добавим Φ_{n+1} к списку аксиом теории T_n, получая новую теорию T_{n+1}. Эта теория тоже непротиворечива. Действительно, если она противоречива, то любая формула в ней доказуема, в частности, $\overline{\Phi_{n+1}}$ выводима из конечного множества аксиом теории T_{n+1}. Если в этом конечном множестве аксиом отсутствует Φ_{n+1}, то $\overline{\Phi_{n+1}}$ доказуема в теории T_n, что противоречит условию непротиворечивости T_n при построении теории T_{n+1}. Таким образом, для некоторого конечного множества Γ аксиом теории T_n верно $\Gamma, \Phi_{n+1} \vdash \overline{\Phi_{n+1}}$. Учитывая очевидный факт $\Gamma, \Phi_{n+1} \vdash \Phi_{n+1}$, и применяя правило опровержения $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma, \mathcal{A} \vdash \overline{\mathcal{B}}}{\Gamma \vdash \overline{\mathcal{A}}}$, получим $\Gamma \vdash \overline{\Phi_{n+1}}$ – противоречие с построением теории T_{n+1}.

Докажеми теперь, что теория $T_\infty = \bigcup_{i=0}^{\infty} T_i$ и будет искомой непротиворечивой полной теорией, содержащей исходную теорию T. Она непротиворечива ввиду теоремы компактности: если противоречие есть, то оно получается из некоторого конечного списка аксиом, т.е. должно присутствовать и в некоторой теории T_n, что противоречит доказанной непротиворечивости всех теорий T_n $(n \geq 0)$.

Пусть теперь Φ – произвольная замкнутая формула теории T_∞, являющаяся, конечно, и формулой теории T. Значит $\Phi = \Phi_m$ для некоторого $m \in \boldsymbol{N}$, и поэтому представляются следующие возможности: либо $\overline{\Phi_m}$ доказуема в теории T_m, а значит и в T_∞, либо $\overline{\Phi_m}$ недоказуема в теории T_m, но тогда Φ_m является аксиомой теории T_{m+1}, доказуема в T_{m+1}, а значит и в T_∞. Таким образом, для любой замкнутой формулы Φ теории T_∞ одна из формул Φ, $\overline{\Phi}$ доказуема в этой теории.

Теорема о пополнении доказана.

В отличие от формальных теорий исчисления высказываний и предикатов, которые слишком общи, чтобы быть полными, формальная теория арифметики имеет дело с конкретными объектами – натуральными числами, изучаемыми с детства. Поэтому доказанная К. Гёделем в 1931 г. теорема о неполноте арифметики вызвала эффект разорвавшейся бомбы.

Теорема (Гёделя о неполноте формальной арифметики). *Если формальная арифметика непротиворечива, то можно указать конкретную замкнутую формулу, которая, как и её отрицание, не доказуемы в формальной арифметике, т.е. формальная арифметика не полна. В качестве такой формулы можно взять, например, формулу, выражающую факт недоказуемости теоремы арифметики* $(0 \neq 1)$.

Таким образом, натуральные числа, изучаемые в школе – это лишь одна из возможных моделей формальной арифметики. Оказывается, что существует модель формальной арифметики даже на множестве $\boldsymbol{R}$ всех действительных чисел. К сожалению, приходится сделать вывод: аксиомы не могут выразить адекватно все свойства формализуемого математического объекта; полученные модели аксиоматической теории могут иметь свойства, не предусмотренные в аксиомах и далёкие от первоначального замысла их создателя. Теперь математик, пытающийся доказать какую-либо теорему, должен учитывать возможность того, что она, как и её отрицание, могут быть недоказуемыми в рамках аксиоматики изучаемой теории.

Заметим ещё, что упомянутая в прошлом параграфе обобщённая теоерема Гёделя о неполноте не противоречит теореме о пополнении: просто полное непротиворечивое расширение арифметики (как и любой конструктивно аксиоматизируемой теории, о которой идёт речь) уже не будет конструктивно аксиоматизируемым. Причина этого кроется в том, что, не всегда возможно эффективно определить, доказуема ли в данной теории заданная замкнутая формула.

§ 4. Разрешимость аксиоматических теорий

Проблема разрешимости теории может быть сформулирована несколькими способами:

(Проблема доказуемости): *Существует ли алгоритм, позволяющий за конечное число шагов эффективно определить, является ли заданная замкнутая формула теории доказуемой, или нет.*

(Проблема общезначимости): *Существует ли алгоритм, позволяющий за конечное число шагов эффективно определить, является ли заданная замкнутая формула теории общезначимой (т.е. тождественно истинной), или нет.*

(Проблема выполнимости): *Существует ли алгоритм, позволяющий за конечное число шагов эффективно определить, является ли заданная замкнутая формула теории выполнимой (т.е. не тождественно истинной и не тождественно ложной), или нет.*

В этих формулировках участвует понятие алгоритма, которое строго определяется в курсе “Теория алгоритмов”, а пока будем воспринимать его на интуитивном уровне, считая, что алгоритм – это программа, написанная на некотором языке программирования и выполняемая на какой-то ЭВМ. Конечно, все формулы теории и её правила вывода предполагаются эффективно занумерованными натуральными числами, кроме того, естественно потребовать существования алгоритма, определяющего по заданному номеру формулы, является эта формула аксиомой теории или нет. Тогда будет существовать алгоритм, перечисляющий все доказуемые формулы теории (?!).

Теорема (об эквивалентности проблем доказуемости, общезначимости и выполнимости). *Три сформулированные проблемы эквивалентны, т.е. существование алгоритма, решающего одну из них влечёт существование алгоритма, решающего остальные проблемы.*

Доказательство. Предположим, что нашёлся алгоритм $A(\Phi)$, решающий проблему доказуемости т.е. программа, выдающая за конечное время по заданной замкнутой формуле теории Φ, ответ 1, если эта формула доказуема, и 0 – в противном случае. Этот же алгоритм решает и проблему общезначимости: нужно лишь вспомнить, что специальная теория полна в широком смысле, т.е. её формула тождественно истинна тогда и только тогда, когда она доказуема.

Если нашёлся алгоритм $A(\Phi)$, решающий проблему общезначимости, то для проверки выполнимости замкнутой формулы Φ применим его дважды: для Φ и для $\overline{\Phi}$. Ясно, что формула Φ выполнима тогда и только тогда, когда $A(\Phi) = 0 = A(\overline{\Phi})$.

Наконец, если нашёлся алгоритм $A(\Phi)$, решающий проблему выполнимости произвольной замкнутой формулы Φ, то для решения вопроса о доказуемости этой формулы (т.е. о её общезначимости) запустим этот алгоритм для формулы Φ. Если $A(\Phi) = 1$, то формула Φ выполнима и не общезначима. Если же $A(\Phi) = 0$, то Φ либо общезначима, либо тождественно ложна, т.е. является отрицанием общезначимой формулы. Теперь одновременно запустим алгоритмы перечисления доказуемых формул и их отрицаний (?!). Формула Φ обязательно встретится в одном из списков и её вид будет определён.

Теорема доказана.

Формальная теория называется *разрешимой*, если для неё существует алгоритм, решающий любую из трёх сформулированных эквивалентных проблем. Долгое время математики искали способы доказательства разрешимости основных математических теорий. В некоторых простейших случаях такие алгоритмы найти легко.

Теорема (о разрешимости исчисления высказываний). *Формальная теория исчисления высказываний разрешима.*

Доказательство. Это следует из возможности эффективной проверки общезначимости формулы путём построения таблицы истинности. Теорема доказана.

Основная трудность в определении общезначимости замкнутой формулы обусловлена наличием кванторов: как проверить истинность или ложность высказываний $\forall x \in M \ \mathcal{P}(x)$ или $\exists x \in M \ \mathcal{P}(x)$, если множество M бесконечно, а $\mathcal{P}(x)$ – предикат на M? Простой перебор значений объектной переменной x невозможен, т.к. может потребовать бесконечного времени. Таким образом, труд-

ности возникают уже при проверке общезначимости простейших формул вида $\forall x\ P(x)$ или $\exists x\ P(x)$. Проблемы с кванторами исчезают, если рассматривать интерпретации формул на конечных множествах.

Теорема (об элиминации кванторов на конечном множестве). *Если множество $M = \{m_1, \dots, m_k\}$ – конечно, то для любой формулы исчисления предикатов $\Phi(x)$ верно*

$(\forall x \in M\ \Phi(x)) \equiv (\Phi(m_1) \wedge \dots \wedge \Phi(m_k))$, $(\exists x \in M\ \Phi(x)) \equiv (\Phi(m_1) \vee \dots \vee \Phi(m_k))$.

Отсюда следует, что любая формула на конечном множестве равносильна некоторой бескванторной формуле.

Доказательство. Утверждения $(\forall x \in M\ \Phi(x)) \equiv \Phi(m_1) \wedge \dots \wedge \Phi(m_k)$, $(\exists x \in M\ \Phi(x)) \equiv \Phi(m_1) \vee \dots \vee \Phi(m_k)$ верны по определению истинности высказываний с кванторами. Если дана произвольная формула $F(x_1, \dots, x_n)$, то можно считать, что она является *ППНФ*, т.е. имеет вид

$F(x_1, \dots, x_n) = (Q_1 y_1 \in M\ (Q_2 y_2 \in M\ (\dots(Q_s y_s \in M\ G(x_1, \dots, x_n, y_1, \dots, y_s))\dots)))$.

Теперь с помощью доказанных утверждений можно последовательно снимать квантор за квантором, получив в итоге бескванторную формулу.

Например, для формулы $(\forall y \in M\ (\exists z \in M\ G(x, y, z)))$ имеем:

$(\forall y \in M\ (\exists z \in M\ G(x, y, z))) \equiv (\forall y \in M\ (G(x, y, m_1) \vee \dots \vee G(x, y, m_k))) \equiv$

$\equiv (G(x, m_1, m_1) \vee \dots \vee G(x, m_1, m_k)) \wedge \dots \wedge (G(x, m_k, m_1) \vee \dots \vee G(x, m_k, m_k))$.

Теорема доказана.

Следствие (об *n*-разрешимости). *Пусть n – фиксированное натуральное число. Для любой формулы исчисления предикатов существует алгоритм, выясняющий за конечное число шагов, принимает ли она значение 0 хотя бы при одной интерпретации на n-элементном множестве, или же при всех интерпретациях на n-элементных множествах эта формула принимает значение 1.*

Доказательство. Для n-элементного множества $M = \{a_1, \dots, a_n\}$ существует лишь конечное число интерпретаций заданной формулы Φ : это следует из конечности числа предикатов на множестве M. Последовательно перечисляя эти интерпретации и вычисляя значение формулы при каждой из них, либо найдём интерпретацию со значением *0*, либо получим, что при всех интерпретациях значение формулы равно *1*. Следствие доказано.

Возникает идея доказать следующее

“Утверждение” (об опровержении формул на конечных множествах). *Если формула исчисления предикатов не является тождественно истинной, то*

существует её интерпретация на конечном множестве, при которой эта формула принимает значение 0.

Отсюда уже почти был бы виден алгоритм проверки заданной замкнутой формулы исчисления предикатов на общезначимость. Просто нужно последовательно вычислять значения формулы при её интерпретациях сначала на одноэлементных множествах, затем на двухэлементных, и.т.д. Если она не общезначима, то на некотором конечном шаге обязательно получится значение *ложь*. Правда, этот алгоритм может работать бесконечно, если формула общезначима. Но, кажется, – ещё чуть-чуть – и проблема будет решена… Однако, надеждам на доказательство сформулированного выше утверждения не суждено сбыться:

Утверждение (о выполнимой формуле, истинной на всех конечных моделях). *Формула исчисления предикатов*

$$(\exists\, x\ (\forall\, y\ (\exists\, z\ ((P(y, z) \to P(x, z)) \to (P(x, x) \to P(y, x))))))$$

истинна на любой конечной модели, но не тождественно истинна.

Доказательство. Прежде всего, эта формула принимает значение *ложь* при интерпретации $(\boldsymbol{N},\ \leq)$:

$$(\exists\, x \in \boldsymbol{N}\ (\forall\, y \in \boldsymbol{N}\ (\exists\, z \in \boldsymbol{N}\ ((y \leq z) \to (x \leq z)) \to ((x \leq x) \to (y \leq x))))) \equiv$$

$$\equiv (\exists\, x \in \boldsymbol{N}\ (\forall\, y \in \boldsymbol{N}\ (\exists\, z \in \boldsymbol{N}\ ((y \leq z) \to (x \leq z)) \to (\boldsymbol{1} \to (y \leq x))))) \equiv$$

$$\equiv (\exists\, x \in \boldsymbol{N}\, (\forall\, y \in \boldsymbol{N}\ (\exists\, z \in \boldsymbol{N}\ ((y > z) \vee (x \leq z)) \to (y \leq x)))) \equiv$$

$$\equiv (\exists\, x \in \boldsymbol{N}\, (\forall\, y \in \boldsymbol{N}\ (\exists\, z \in \boldsymbol{N}\ ((y \leq z) \wedge (x > z)) \vee (y \leq x))))$$

и условие $(y \leq x)$ не может быть истинным при $y > x$, т.е. при $y > x$ должно выполняться $((y \leq z) \wedge (x > z))$, что невозможно (если $z < x$ и $y \leq z$, то $y < x$).

Докажем теперь, что в случае ложности формулы на модели $(M,\ \mathcal{P}(\_\ ,\ \_))$ множество M бесконечно. В самом деле, ложность этой формулы означает

$$(\forall\, x \in M\, (\exists\, y \in M\, (\forall\, z \in M\ \overline{((\mathcal{P}(y, z) \to \mathcal{P}(x, z)) \to (\mathcal{P}(x, x) \to \mathcal{P}(y, x)))}\ ))) \equiv$$

$$\equiv (\forall\, x \in M\, (\exists\, y \in M\, (\forall\, z \in M\ \overline{(\overline{(\overline{\mathcal{P}(y, z)} \vee \mathcal{P}(x, z))} \vee (\overline{\mathcal{P}(x, x)} \vee \mathcal{P}(y, x)))}\ ))) \equiv$$

$$\equiv (\forall\, x \in M\, (\exists\, y \in M\, (\forall\, z \in M\, ((\overline{\mathcal{P}(y, z)} \vee \mathcal{P}(x, z)) \wedge (\mathcal{P}(x, x) \wedge \overline{\mathcal{P}(y, x)}))))) \equiv$$

$$\equiv (\forall\, x \in M\, (\exists\, y \in M\, ((\mathcal{P}(x, x) \wedge \overline{\mathcal{P}(y, x)}) \wedge (\forall\, z \in M\, (\overline{\mathcal{P}(y, z)} \vee \mathcal{P}(x, z))))))$$

Таким образом, для любого $x \in M$ существует $y = y(x) \in M$ со свойствами: $\mathcal{P}(x, x) = 1$, $\mathcal{P}(y(x), x) = 0$ и для любого z верно $\mathcal{P}(y(x), z) = 0$ или $\mathcal{P}(x, z) = 1$.

Рассмотрим последовательность элементов множества M: $x_1 = x$, $x_{i+1} = y(x_i)$ $(i \in \boldsymbol{N})$ и докажем, что среди её элементов нет равных. В самом деле, если $x_i = x_j$ при $i < j$, то $x_j = y(x_{j-1})$ и $\mathcal{P}(x_j, x_{j-1}) = \mathcal{P}(y(x_{j-1}), x_{j-1}) = 0$, но (при $x = x_i$,

$z = x_{j-1}$) $\mathcal{P}(x_{i+1}, x_{j-1}) = 0$ или $\mathcal{P}(x_i, x_{j-1}) = 1$. Случай $\mathcal{P}(x_i, x_{j-1}) = 1$ противоречит условиям $x_i = x_j$ и $\mathcal{P}(x_j, x_{j-1}) = 0$. Значит, $\mathcal{P}(x_{i+1}, x_{j-1}) = 0$, и аналогично предыдущему при $x = x_{i+1}$, $z = x_{j-1}$ получаем $\mathcal{P}(x_{i+2}, x_{j-1}) = 0$ или $\mathcal{P}(x_{i+1}, x_{j-1}) = 1$. Отсюда $\mathcal{P}(x_{i+2}, x_{j-1}) = 0$, и процесс можно продолжить, пока не получим $\mathcal{P}(x_{j-2}, x_{j-1}) = 0$, что ведёт к противоречию: при $x = x_{j-2}$, $z = x_{j-1}$ имеем $\mathcal{P}(x_{j-1}, x_{j-1}) = 0$ или $\mathcal{P}(x_{j-2}, x_{j-1}) = 1$ (альтернатива $\mathcal{P}(x_{j-1}, x_{j-1}) = 0$ невозможна ввиду $\mathcal{P}(x, x) = 1$).

Утверждение доказано.

Таким образом, наша первая попытка построить алгоритм разрешения формальной теории предикатов успешно провалилась ! В 20-х годах прошлого века было исследовано много и значительно более тонких идей построения алгоритма проверки доказуемости формул исчисления предикатов. Все они не привели к желаемому результату. Каково же было удивление математиков, когда в *30*-х годах XX в. А. Чёрчем было доказано, что не существует алгоритма проверки заданной формулы исчисления предикатов на общезначимость.

Теорема (Чёрча о неразрешимости теории исчисления предикатов). *Не существует алгоритма, позволяющего за конечное число шагов определить, является ли заданная формула исчисления предикатов общезначимой, или нет.*

Тем не менее, для некоторых формул специального вида алгоритмы, решающие проблемы общезначимости и выполнимости существуют. Приведём для примера два результата о замкнутых формулах с одноимёнными кванторами.

Теорема (об общезначимых замкнутых $\exists$-формулах). *Замкнутая ППНФ, содержащая только кванторы существования, является общезначимой тогда и только тогда, когда она принимает значение 1 – истина во всех интерпретациях на одноэлементных множествах.*

Доказательство. Рассмотрим замкнутую ППНФ, содержащую только кванторы существования, т.е. формулу вида $(\exists\, x\, (\exists\, y\, (\dots\, (\exists\, z\ F(x, y, \dots, z))\dots)))$, не зависящую от других переменных, кроме связанных кванторами. Ясно, что если она общезначима, то во всех интерпретациях на одноэлементных множествах она принимает значение *истина*.

Обратно, если эта формула не общезначима, то она принимает значение *ложь* при интерпретации на некотором множестве M. Тогда отрицание этой формулы, т.е. формула $(\forall\, x\, (\forall\, y\, (\dots\, (\forall\, z\ \overline{F}\ (x, y, \dots, z))\dots)))$, будет при этой интерпретации иметь значение *истина*. В частности, зафиксировав $m_0 \in M$, по-

лучим $\overline{F}\,(m_0, m_0, \ldots, m_0) = 1$. Таким образом, $F(m_0, m_0, \ldots, m_0) = 0$ и значит, формула $(\exists x\,(\exists y\,(\ldots(\exists z\ F(x, y, \ldots, z))\ldots)))$ принимает значение *ложь* при интерпретации на одноэлементном множестве $\{m_0\}$.

Теорема доказана.

Теорема (об общезначимых замкнутых $\forall$-формулах). *Замкнутая ППНФ, содержащая только n кванторов всеобщности, является общезначимой тогда и только тогда, когда она принимает значение 1 во всех интерпретациях на n-элементных множествах.*

Доказательство. Рассмотрим замкнутую *ППНФ,* содержащую только n кванторов всеобщности, т.е. формулу вида $(\forall x\,(\forall y\,(\ldots(\forall z\ F(x, y, \ldots, z))\ldots)))$, не зависящую от других переменных, кроме связанных кванторами.

Ясно, что если она общезначима, то во всех интерпретациях на n-элементных множествах она принимает значение *истина*.

Обратно, если эта формула не общезначима, то она принимает значение *ложь* при интерпретации на некотором множестве M. Тогда отрицание этой формулы, т.е. формула $(\exists x\,(\exists y\,(\ldots(\exists z\ \overline{F}\ (x, y, \ldots, z))\ldots)))$, будет при этой интерпретации иметь значение *истина*. Таким образом, $\overline{F}\,(m_1, m_2, \ldots, m_n) = 1$ при некоторых $m_1, \ldots, m_n \in M$. Поэтому $F(m_1, \ldots, m_n) = 0$ и исследуемая формула $(\forall x\,(\forall y\,(\ldots(\forall z\ F(x, y, \ldots, z))\ldots)))$ принимает значение *ложь* при интерпретации на множестве $\{m_1, \ldots, m_n\}$.

Теорема доказана.

Что касается формальной теории арифметики, то после всего сказанного неудивительно, что она тоже неразрешима:

Теорема (Чёрча о неразрешимости формальной арифметики). *Не существует алгоритма, позволяющего за конечное число шагов определить, является ли заданная формула формальной арифметики доказуемой, или нет.*

Более того, в 70-х годах XX в. было доказано, что алгоритмически неразрешим вопрос о существовании целочисленных решений *диофантовых уравнений*, т.е. уравнений вида $F(x_1, \ldots, x_n) = 0$, где $F(x_1, \ldots, x_n)$ – ненулевой многочлен от переменных $x_1, \ldots, x_n$ с целыми коэффициентами. Таким образом, ***не существует алгоритма проверки доказуемости формул формальной арифметики вида*** $(\exists x_1\ (\exists x_2\ (\ldots(\exists x_n\ (F(x_1, \ldots, x_n) = 0)))))$. Можно даже конкретно указать многочлен $F(x_1, \ldots, x_n)$. Это утверждение, доказанное в 1970 г. Ю.В. Матиясевичем, решает 10-ю проблему Гильберта из списка поставлен-

ных им в 1901 г. на Международном математическом конгрессе в Париже наиболее важных математических задач XX века.

§ 5. Независимость системы аксиом теории

Создавая аксиоматическую теорию, естественно стремиться не выписывать лишних аксиом – тех, которые выводимы из остальных. Система аксиом формальной теории называется *независимой*, если ни одна аксиома этой системы не выводима из остальных. Более формально, ситема $\{A_i\}_{i \in I}$ *независима*, если для любой аксиомы A_i и любого конечного множества аксиом $\Gamma \subseteq \{A_j\}_{j \in I \setminus \{i\}}$ утверждение $\Gamma \vdash A_i$ неверно.

Конечно, требование независимости является скорее эстетическим, нежели математически необходимым, но оно побуждает к анализу взаимосвязей аксиом создаваемой теории, к отсечению лишнего, тем самым, – к более глубокому пониманию сути математической реальности. Вот почему независимость системы аксиом является "правилом хорошего тона" для создателя аксиоматики.

Если аксиоматика формальной теории состоит из схем аксиом, то, как правило, проверяют независимость друг от друга схем аксиом, а не отдельных аксиом теории.

Как доказать независимость той или иной системы аксиом ? Основным методом доказательства является *метод построения независимых моделей*, основанный на следующей теореме:

Теорема (критерий независимости системы аксиом). *Система аксиом (схем аксиом) $\{A_i\}_{i \in I}$ независима тогда и только тогда, когда для каждого $i \in I$ существует модель для системы аксиом (схем аксиом) $\{A_j\}_{j \in I \setminus \{i\}}$, в которой аксиома (схема аксиом) A_i ложна.*

Доказательство. Ясно, что существование модели с указанным в формулировке теоремы свойством показывает, что утверждение $\Gamma \vdash A_i$ для любого конечного множества аксиом $\Gamma \subseteq \{A_j\}_{j \in I \setminus \{i\}}$ неверно.

Обратно, если аксиома A_i не выводима из остальных, то непротиворечивой будет система аксиом $\Gamma_i = \{A_j\}_{j \in I \setminus \{i\}} \cup \{ \overline{A_i} \}$. Действительно, если бы эта система была противоречива, то любая формула была бы доказуема (выводима из некоторой конечной совокупности аксиом $\Gamma \cup \{ \overline{A_i} \}$, где $\Gamma \subseteq \Gamma_i$). Поэтому $\Gamma, \overline{A_i} \vdash A_i$ и, очевидно, $\Gamma, \overline{A_i} \vdash \overline{A_i}$. По правилу опровержения отсюда следу-

ет, что $\Gamma \vdash \overline{\overline{A_i}}$, т.е. (с учётом аксиомы $\overline{\overline{A_i}} \to A_i$) верно $\Gamma \vdash A_i$ – противоречие. У непротиворечивого множества аксиом $\Gamma_i = \{A_j\}_{j \in I \setminus \{i\}} \cup \{\overline{A_i}\}$ существует модель, в которой аксиома A_i ложна, что и требовалось.

Теорема доказана.

Теорема (о независимости системы аксиом исчисления высказываний). *Система аксиом формального исчисления высказываний (приведённая в § 1 главы III) независима.*

Доказательство. Используем метод построения независимых моделей: для каждой схемы аксиом построим модель, в которой эта схема аксиом ложна, а остальные истинны. Все модели будут устроены однообразно: на некотором конечном множестве M определим функции из M в M: $\wedge$, $\vee$, $\to$ от двух аргументов и $\overline{\bullet}$ – от одного, которые будут интерпретировать логические связки исчисления высказываний. В каждом случае будет выделено некоторое подмножество $И \subseteq M$, в котором находятся значения всех "истинных" в модели M схем аксиом, в отличие от независимой от них ("ложной" в M) схемы аксиом, которая принимает значения и не лежащие во множестве $И$. При этом применение правила *modus ponens* к формулам, имеющим значения только в $И$ (к "истинным" в модели формулам), приводит снова к формуле, имеющем значения снова во множестве $И$ (к "истинной" в модели формуле). Таким образом, все выводимые из "истинных" формул формулы снова будут истинными, а любая "ложная" формула не выводима из "истинных". Итак, рассматриваемая в каждом случае "ложная" схема аксиом не выводится из остальных "истинных" аксиом.

Все вычисления подробно производиться не будут (это – задание для самостоятельной работы), но конструкции моделей будут описаны точно. Поскольку связка импликации участвует во всех аксиомах исчисления высказываний, доказательство независимости аксиом группы импликации наиболее трудоёмко.

Независимость схемы (И1): $(А \to (В \to А))$. Рассмотрим трёхэлементное множество $M = \{0, 1, 2\}$ и определим на нём новое исчисление логических связок, полагая для $x, y \in M$ следующие значения связок: $x \wedge y = \min\{x, y\}$, $x \vee y = \max\{x, y\}$, $x \to y = \begin{cases} 2, \text{ если } x \le y \\ 0, \text{ если } x > y \end{cases}$, $\overline{x} = 2 - x$.

Проверим, что все схемы аксиом, кроме ***(И1)*** дают значения во множестве $И = \{2\}$, множество "истинных" формул замкнуто относительно правила *modus*

ponens, а схема аксиом ***(И1)*** принимает значения не только во множестве $И$. Всё это проверяется путём построения многочисленных таблиц истинности.

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{B} \to \mathcal{A}$	$\mathcal{A} \to (\mathcal{B} \to \mathcal{A})$
0	0	2	**2**
1	0	2	**2**
2	0	2	**2**
0	1	0	**2**
1	1	2	**2**
2	1	2	**2**
0	2	0	**2**
1	2	0	**0**
2	2	2	**2**

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \to \mathcal{B}$
0	0	2
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	2
2	2	2

Таблица слева показывает, что схема аксиом ***(И1)*** не всегда принимает значения во множестве $И = \{2\}$, а потому "ложна в рассматриваемой модели". Таблица справа доказывает, что множество "истинных" формул замкнуто относительно правила *modus ponens* (более точно, если $\mathcal{A} = 2 = (\mathcal{A} \to \mathcal{B})$, то $\mathcal{B} = 2$).

Наконец, проверим, что все остальные схемы аксиом "истинны" в этой модели, т.е. принимают значения только во множестве $И = \{2\}$:

$\mathcal{A}$	$\mathcal{B}$	C	$\mathcal{A} \to \mathcal{B}$	$\mathcal{A} \to C$	$\mathcal{B} \to C$	$\mathcal{A} \to (\mathcal{B} \to C)$	$(\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to C)$	***(И2)***	$\mathcal{B} \wedge C$	$\mathcal{A} \to (\mathcal{B} \wedge C)$	$(\mathcal{A} \to C) \to (\mathcal{A} \to (\mathcal{B} \wedge C))$	***(К3)***	$\mathcal{A} \vee \mathcal{B}$	$(\mathcal{A} \vee \mathcal{B}) \to C$	$(\mathcal{B} \to C) \to ((\mathcal{A} \vee \mathcal{B}) \to C)$	***(Д3)***
0	0	0	2	2	2	2	2	**2**	0	2	2	**2**	0	2	2	**2**
1	0	0	0	0	2	2	2	**2**	0	0	2	**2**	1	0	2	**2**
2	0	0	0	0	2	2	2	**2**	0	0	2	**2**	2	0	2	**2**
0	1	0	2	2	0	2	2	**2**	0	2	2	**2**	1	0	2	**2**
1	1	0	2	0	0	0	0	**2**	0	0	2	**2**	1	0	2	**2**
2	1	0	0	0	0	0	2	**2**	0	0	2	**2**	2	0	2	**2**
0	2	0	2	2	0	2	2	**2**	0	2	2	**2**	2	0	0	**2**
1	2	0	2	0	0	0	0	**2**	0	0	2	**2**	2	0	2	**2**
2	2	0	2	0	0	0	0	**2**	0	0	2	**2**	2	0	2	**2**
0	0	1	2	2	2	2	2	**2**	0	2	2	**2**	0	2	2	**2**
1	0	1	0	2	2	2	2	**2**	0	0	0	**2**	1	2	2	**2**
2	0	1	0	0	2	2	2	**2**	0	0	2	**2**	2	0	2	**2**
0	1	1	2	2	2	2	2	**2**	1	2	2	**2**	1	2	2	**2**
1	1	1	2	2	2	2	2	**2**	1	2	2	**2**	1	2	2	**2**
2	1	1	0	0	2	2	2	**2**	1	0	2	**2**	2	0	2	**2**
0	2	1	2	2	0	2	2	**2**	1	2	2	**2**	2	0	0	**2**
1	2	1	2	2	0	0	2	**2**	1	2	2	**2**	2	0	0	**2**
2	2	1	2	0	0	0	0	**2**	1	0	2	**2**	2	0	2	**2**
0	0	2	2	2	2	2	2	**2**	0	2	2	**2**	0	2	2	**2**
1	0	2	0	2	2	2	2	**2**	0	0	0	**2**	1	2	2	**2**
2	0	2	0	2	2	2	2	**2**	0	0	0	**2**	2	2	2	**2**

0	1	2	2	2	2	2	2	**2**	1	2	2	**2**	1	2	2	**2**
1	1	2	2	2	2	2	2	**2**	1	2	2	**2**	1	2	2	**2**
2	1	2	0	2	2	2	2	**2**	1	0	0	**2**	2	2	2	**2**
0	2	2	2	2	2	2	2	**2**	2	2	2	**2**	2	2	2	**2**
1	2	2	2	2	2	2	2	**2**	2	2	2	**2**	1	2	2	**2**
2	2	2	2	2	2	2	2	**2**	2	2	2	**2**	2	2	2	**2**

Таблица показывает, что схемы ***(И2)***, ***(К3)***, ***(Д3)*** "истинны" в этой модели.

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	**К1**	**К2**	$\mathcal{A} \vee \mathcal{B}$	**Д1**	**Д2**	$\overline{\mathcal{A}}$	$\overline{\overline{\mathcal{A}}}$	**О1**	**О2**	$\mathcal{A} \uparrow \mathcal{B}$	$\overline{\mathcal{A}} \uparrow \overline{\mathcal{B}}$	**О3**
0	0	0	**2**	**2**	0	**2**	**2**	2	0	**2**	**2**	2	2	**2**
1	0	0	**2**	**2**	1	**2**	**2**	1	1	**2**	**2**	0	0	**2**
2	0	0	**2**	**2**	2	**2**	**2**	0	2	**2**	**2**	0	0	**2**
0	1	0	**2**	**2**	1	**2**	**2**	2	0	**2**	**2**	2	2	**2**
1	1	1	**2**	**2**	1	**2**	**2**	1	1	**2**	**2**	2	2	**2**
2	1	1	**2**	**2**	2	**2**	**2**	0	2	**2**	**2**	0	0	**2**
0	2	0	**2**	**2**	2	**2**	**2**	2	0	**2**	**2**	2	2	**2**
1	2	1	**2**	**2**	2	**2**	**2**	1	1	**2**	**2**	2	2	**2**
2	2	2	**2**	**2**	2	**2**	**2**	0	2	**2**	**2**	2	2	**2**

Итак, схемы аксиом ***(К1)***, ***(К2)***, ***(Д1)***, ***(Д2)***, ***(О1)***, ***(О2)***, ***(О3)*** тоже "истинны" в построенной модели. Поэтому доказана независимость аксиомы ***(И1)*** от остальных аксиом формального исчисления высказываний.

Независимость схемы (И2): $((\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})))$**.** Возьмём $M = \{0, 1, 2\}$, $И = \{0\}$ и определим для $x, y \in M$ следующие значения связок: $x \wedge y = \max\{x, y\}$, $x \vee y = \min\{x, y\}$, $x \to y = \max\{0, y - x\}$, $\overline{x} = 2 - x$.

Проверьте самостоятельно, что все схемы аксиом, кроме ***(И2)*** принимают значения во множестве $И$, множество "истинных" формул замкнуто относительно правила *modus ponens*, а схема аксиом ***(И2)*** принимает значения не только во множестве $И$.

Независимость схемы (К1): $((\mathcal{A} \wedge \mathcal{B}) \to \mathcal{A})$**.** Возьмём $M = \{0, 1\}$, $И = \{1\}$ и определим для элементов $x, y \in M$ следующие значения логических связок: $x \wedge y = y$, а остальные связки $\vee$, $\to$, $\overline{\bullet}$ интерпретируем стандартно.

Следующие таблицы доказывают, что схема аксиом ***(К1)*** "ложна в рассматриваемой модели", а множество "истинных" формул замкнуто относительно правила *modus ponens* (более точно, если $\mathcal{A} = 1 = (\mathcal{A} \to \mathcal{B})$, то $\mathcal{B} = 1$):

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \wedge \mathcal{B}$	$(\mathcal{A} \wedge \mathcal{B}) \to \mathcal{A}$
0	0	0	**1**
1	0	0	**1**
0	1	1	**0**
1	1	1	**1**

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A} \to \mathcal{B}$
0	0	1
1	0	0
0	1	1
1	**1**	**1**

Проверим теперь истинность остальных аксиом.

A	B	$A \wedge B$	**К2**	$A \vee B$	**Д1**	**Д2**	$\overline{A}$	$\overline{\overline{A}}$	**О1**	**О2**	$A \to B$	$\overline{A} \uparrow \overline{B}$	**О3**
0	0	0	**1**	0	**1**	**1**	1	0	**1**	**1**	1	1	**1**
1	0	0	**1**	1	**1**	**1**	0	1	**1**	**1**	0	0	**1**
0	1	1	**1**	1	**1**	**1**	1	0	**1**	**1**	1	1	**1**
1	1	1	**1**	1	**1**	**1**	0	1	**1**	**1**	1	1	**1**

A	B	C	$A \to B$	$A \to C$	$B \to C$	$B \to A$	**И1**	$A \to (B \to C)$	$(A \to B) \to (A \to C)$	**И2**	$B \wedge C$	$A \to (B \wedge C)$	$(A \to C) \to (A \to (B \wedge C))$	**К3**	$A \vee B$	$(A \vee B) \to C$	$(B \to C) \to ((A \vee B) \to C)$	**Д3**
0	0	0	1	1	1	1	**1**	1	1	**1**	0	1	1	**1**	0	1	1	**1**
1	0	0	0	0	1	1	**1**	1	1	**1**	0	0	1	**1**	1	0	0	**1**
0	1	0	1	1	0	0	**1**	1	1	**1**	0	1	1	**1**	1	0	1	**1**
1	1	0	1	0	0	1	**1**	0	0	**1**	0	0	1	**1**	1	0	1	**1**
0	0	1	1	1	1	1	**1**	1	1	**1**	1	1	1	**1**	0	1	1	**1**
1	0	1	0	1	1	1	**1**	1	1	**1**	1	1	1	**1**	1	1	1	**1**
0	1	1	1	1	1	0	**1**	1	1	**1**	1	1	1	**1**	1	1	1	**1**
1	1	1	1	1	1	1	**1**	1	1	**1**	1	1	1	**1**	1	1	1	**1**

Независимость схемы (К2): $((A \wedge B) \to B)$**.** Докажите самостоятельно, видоизменив интерпретацию конъюнкции.

Независимость схемы (К3): $((A \to B) \to ((A \to C) \to (A \to (B \wedge C))))$**.** Возьмём $M = \{0, 1\}$, $И = \{1\}$ и определим для элементов $x, y \in M$ следующие значения логических связок: $x \wedge y = 0$, а остальные связки $\vee$, $\to$, $\overline{\bullet}$ интерпретируем стандартно.

Ясно, что множество “истинных” формул замкнуто относительно правила *modus ponens* (импликация стандартна).

Схема аксиом ***(К3)*** “ложна в рассматриваемой модели”, т.к. принимает значение $0 \notin И$ при $A = B = C = 1$. Среди остальных аксиом нужно проверять только схемы ***(К1)*** и ***(К2)***, которые, очевидно, будут принимать всегда значение 1, т.к. $A \wedge B = 0$ и импликация вычисляется стандартно.

Независимость схемы (Д1): $(A \to (A \vee B))$**.** Проверки аналогичны вычислениям для схемы ***(К1)***: берём $M = \{0, 1\}$, $И = \{1\}$, и для элементов $x, y \in M$ полагаем $x \vee y = y$, интерпретируя остальные связки $\wedge$, $\to$, $\overline{\bullet}$ стандартно.

Независимость схемы (Д2): $(B \to (A \vee B))$. Докажите самостоятельно, видоизменив интерпретацию дизъюнкции.

Независимость схемы (Д3): $((A \to C) \to ((B \to C) \to (A \vee B \to C)))$. Проверки аналогичны вычислениям для схемы ***(К3)***: берём $M = \{0, 1\}$, $И = \{1\}$, и для элементов $x, y \in M$ полагаем $x \vee y = 1$, интерпретируя остальные связки $\wedge$, $\to$, $\overline{\bullet}$ стандартно.

Независимость схемы (О1): $(A \to \overline{\overline{A}})$. Пусть $M = \{0, 1, 2\}$, $И = \{2\}$ и определим для $x, y \in M$ новые значения логических связок: $x \wedge y = \min\{x, y\}$, $x \vee y = \max\{x, y\}$, $x \to y = \begin{cases} 2, \text{ если } x \le y \\ y, \text{ если } x > y \end{cases}$, $\overline{x} = \begin{cases} 0, \text{ если } x > 0 \\ 2, \text{ если } x = 0 \end{cases}$. Проделайте все вычисления самостоятельно.

Независимость схемы (О2): $(\overline{\overline{A}} \to A)$. Полагаем $M = \{0, 1, 2\}$, $И = \{2\}$ и определим для $x, y \in M$ новые значения логических связок: $x \wedge y = \min\{x, y\}$, $x \vee y = \max\{x, y\}$, $x \to y = \begin{cases} 2, \text{ если } x \le y \\ y, \text{ если } x > y \end{cases}$, $\overline{x} = 2$. Проделайте все вычисления самостоятельно.

Независимость схемы (О3): $((A \to B) \to (\overline{B} \to \overline{A}))$. Здесь $M = \{0, 1\}$, $И = \{1\}$ и для элемента $x \in M$ новое значение отрицания $\overline{x} = x$, а остальные связки $\wedge$, $\vee$, $\to$ стандартны. Проделайте все вычисления самостоятельно.

Если рассматривать исчисление высказываний с эквивалентностью, то нужно доказать ещё независимость аксиом эквивалентности ***(Э1)*** и ***(Э2)***.

Независимость схемы (Э1): $((A \leftrightarrow B) \to ((A \to B) \wedge (B \to A)))$. Нужно взять $M = \{0, 1\}$, $И = \{1\}$ и определить $x \leftrightarrow y = 1$, а все остальные логические связки $\wedge$, $\vee$, $\to$ интерпретировать стандартно. Проделайте все вычисления самостоятельно.

Независимость схемы (Э2): $(((A \to B) \wedge (B \to A)) \to (A \leftrightarrow B))$. Нужно взять $M = \{0, 1\}$, $И = \{1\}$ и определить $x \leftrightarrow y = 0$, а все остальные логические связки $\wedge$, $\vee$, $\to$ интерпретировать стандартно. Проделайте все вычисления самостоятельно.

Теорема о независимости системы аксиом полностью доказана.

Теорема (о независимости аксиом исчисления предикатов). *Система аксиом формального исчисления предикатов независима.*

Доказательство. Проведём рассуждения схематично. Доказательство независимости схем аксиом исчисления высказываний остаются в силе, если значениям формул $(\forall x\ A(x))$ и $(\exists\ x\ A(x))$ с навешенными кванторами вычислять на моделях стандартным образом.

Независимость схемы $(\forall)$***:*** $((\forall\ x\ A(x)) \to A(t))$**.** Достаточно интерпретировать логические связки стандартно, как и значения формул с навешенным квантором существования, а формулы с навешенными кванторами всеобщности всегда считать истинными. Тогда, например, аксиома $((\forall x\ P(x)) \to P(t))$ будет принимать значение 0, если $P(t) = 0$. Остальные аксиомы при этом останутся тождественно истинными.

Независимость схемы $(\exists)$***:*** $(A(t) \to (\exists\ x\ A(x)))$**.** Достаточно интерпретировать логические связки стандартно, как и значения формул с навешенными кванторами всеобщности, а формулы с навешенными кванторами существования всегда считать ложными. Тогда, например, аксиома $(P(t) \to (\exists x\ P(x)))$ будет принимать значение 0, если $P(t) = 0$. Остальные аксиомы при этом останутся тождественно истинными.

Теорема о независимости системы аксиом исчисления предикатов доказана.

§ 6*. Формальное исчисление высказываний

Подробно рассмотрим формальную теорию исчисления высказываний (*ИВ*). Нашей целью будет обоснование адекватности этой теории, описанной формально в § 1 главы III, неформальной алгебре высказываний, изученной в главе I. Под адекватностью формальной теории её неформальному аналогу понимается доказательство всех основных теорем неформальной теории в соответствующей формальной теории. В частности, будет доказано, что формула доказуема в формальной теории исчисления высказываний тогда и только тогда, когда она тождественно истинна.

1. Свойства выводимости формул. Докажем некоторые основные свойства выводимости формул.

1⁰. *Всякая доказуемая формула выводима из любой совокупности формул. В частности, любая аксиома выводима из любой совокупности формул.*

* При первом чтении можно опустить.

Действительно, доказательство формулы является и её выводом из любой совокупности формул, т.к. в нём используются аксиомы и правило вывода *modus ponens*. Последовательность из одной этой аксиомы является её доказательством.

2⁰. *Из любой совокупности выводима любая формула этой совокупности.*

В самом деле, если $\Gamma = \{A_1, \dots, A_i, \dots, A_n\}$, то последовательность из одной формулы A_i является выводом формулы A_i из совокупности Γ.

3⁰. *Доказуемая формула выводима из любой совокупности формул.*

Действительно, доказательство этой формулы является её выводом из любой конечной совокупности формул.

4⁰. *Если существует квазивывод формулы B из совокупности Γ, т.е. конечная последовательность формул $B_1, \dots, B_k = B$, каждая формула которой либо выводима из Γ, либо получена из двух предыдущих по правилу modus ponens, то формула B выводима из Γ.*

Нужно просто заметить, что квазивывод расширится до вывода, если вместо каждой выводимой из Γ формулы B_i вставить её вывод из совокупности Γ.

5⁰. *Если $\Gamma \vdash \Phi$, то для любой совокупности формул Δ верно $\Gamma, \Delta \vdash \Phi$.*

В самом деле, вывод формулы $B_1, \dots, B_k = B$ из совокупности Γ является её выводом и из расширенной совокупности Γ, Δ.

6⁰. *Если $\Gamma \vdash \Phi$ и $\Gamma \vdash (\Phi \to \Psi)$, то $\Gamma \vdash \Psi$.*

Действительно, если $B_1, \dots, B_k = \Phi$ – вывод формулы Φ, а $C_1, \dots, C_m = (\Phi \to \Psi)$ – вывод формулы $(\Phi \to \Psi)$, то $B_1, \dots, B_k = \Phi$, $C_1, \dots, C_m = (\Phi \to \Psi)$, Ψ – вывод формулы Ψ, т.к. последняя формула этой цепочки получена из предыдущих Φ и $(\Phi \to \Psi)$ по правилу *modus ponens*.

Замечание: На самом деле в свойствах ***5⁰*** и ***6⁰*** обоснованы правила вывода $\dfrac{\Gamma \vdash \mathcal{B}}{\Gamma, \mathcal{A} \vdash \mathcal{B}}$ – расширения посылок и $\dfrac{\Gamma \vdash \mathcal{A};\ \Gamma \vdash \mathcal{A} \to \mathcal{B}}{\Gamma \vdash \mathcal{B}}$ – расширение *modus ponens*. Теперь ими можно пользоваться при выводе формул, сокращая длину доказательства. Дальнейший ход изложения лишь увеличит количество полезных правил вывода.

2. Теорема о дедукции: Обоснуем доказанные в главе I неформально правила дедукции: $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B}}{\Gamma \vdash \mathcal{A} \to \mathcal{B}}$, $\dfrac{\Gamma \vdash \mathcal{A} \to \mathcal{B}}{\Gamma, \mathcal{A} \vdash \mathcal{B}}$.

Теорема (о дедукции). *Для формул A, B и произвольной конечной совокупности формул Γ (возможно пустой) утверждение $\Gamma, A \vdash B$ имеет место тогда и только тогда, когда $\Gamma \vdash (A \to B)$.*

Доказательство. Вначале докажем "лёгкую" импликацию $(\Leftarrow)$. Если верно $\Gamma \vdash (A \to B)$, то (по правилу расширения посылок) $\Gamma, A \vdash (A \to B)$ и $\Gamma, A \vdash A$ (используется $\boldsymbol{2^0}$). Применяя расширение *modus ponens*, получим $\Gamma, A \vdash B$, что и требовалось.

$(\Rightarrow)$ Рассмотрим вывод $B_1, \ldots, B_k = B$ формулы B из совокупности Γ, A. Если $k = 1$, то этот вывод состоит из одной формулы B и возможны случаи:

а: ***B – аксиома.*** Тогда цепочка $(B \to (A \to B)),\ B,\ (A \to B)$ будет доказательством формулы $(A \to B)$ и выводом её из совокупности Γ. Последняя формула цепочки получена из предыдущих по правилу *modus ponens*.

б: ***B – формула совокупности Γ, A.*** Если $B = A$, то $(A \to B) = (A \to A)$ – доказуемая формула (см. пример доказательства в § 1), которая выводима из любого множества формул по свойству $\boldsymbol{1^0}$. Если же $B \in \Gamma$, то цепочка $(B \to (A \to B)),\ B,\ (A \to B)$ является выводом формулы $(A \to B)$ из Γ.

Пусть теперь $k > 1$ и неверно, что $\Gamma \vdash (A \to B)$. Можно считать, что k – наименьшее натуральное число с этим свойством. Таким образом, для любых формул Φ, Ψ со свойством $\Gamma, \Phi \vdash \Psi$ и длиной этого вывода меньше k будет верно $\Gamma \vdash (\Phi \to \Psi)$.

В случаях, когда B – аксиома или формула совокупности Γ, A применимы использованные ранее для $k = 1$ аргументы. Значит можно считать, что последняя формула B рассматриваемого вывода получена из двух предыдущих по правилу *modus ponens*. Итак, среди формул вывода B есть формулы $B_i = C$, $B_j = (C \to B)$, где $i < k$, $j < k$, т.е. $\Gamma, A \vdash C$ и $\Gamma, A \vdash (C \to B)$ с длинами выводов, меньшими k. Учитывая предположение о минимальности k, получаем $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$. Теперь можно написать квазивывод формулы $(A \to B)$ из множества формул Γ:

1	• $((A \to (C \to B)) \to ((A \to C) \to (A \to B)))$	***(И2)*** $(\mathcal{A} := A, \mathcal{B} := C, \mathcal{C} := B)$
2	• $(A \to (C \to B))$	***выводима из Γ***
3	• $((A \to C) \to (A \to B))$	***MP(1, 2)***
4	• $(A \to C)$	***выводима из Γ***
5	• $(A \to B)$	***MP(3, 4)***

Теорема о дедукции доказана.

3. Производные правила вывода. Обоснуем некоторые знакомые правила логического вывода. Остальные правила докажите самостоятельно.

Правило перестановки посылок: $\dfrac{\Gamma \vdash \mathcal{A} \to (\mathcal{B} \to C)}{\Gamma \vdash \mathcal{B} \to (\mathcal{A} \to C)}$. Запишем квазивывод формулы $(B \to (A \to C))$, предполагая, что $(A \to (B \to C))$ выводима.

1	• $\Gamma \vdash (A \to (B \to C))$	***дано***
2	• $\Gamma, A \vdash (B \to C)$	***дедукция***
3	• $\Gamma, A, B \vdash C$	***дедукция***
4	• $\Gamma, B \vdash (A \to C)$	***дедукция***
5	• $\Gamma \vdash (B \to (A \to C))$	***дедукция***

Правила силлогизма: $\dfrac{\Gamma \vdash \mathcal{B};\ \mathcal{B} \vdash C}{\Gamma \vdash C}$, $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma, \mathcal{B} \vdash C}{\Gamma, \mathcal{A} \vdash C}$.

1	• $\Gamma \vdash B$	***дано***
2	• $B \vdash C$	***дано***
3	• $\Gamma, B \vdash C$	***расширение посылок***
4	• $\Gamma \vdash (B \to C)$	***дедукция***
5	• $\Gamma \vdash C$	***MP(1, 4)***

1	• $\Gamma, A \vdash B$	***дано***
2	• $\Gamma \vdash (A \to B)$	***дедукция***
3	• $\Gamma, B \vdash C$	***дано***
4	• $\Gamma \vdash (B \to C)$	***дедукция***
5	• $((B \to C) \to (A \to (B \to C)))$	***(И1)*** $(\mathcal{A} := (B \to C),\ \mathcal{B} := A)$
6	• $\Gamma \vdash (A \to (B \to C))$	***MP(4, 5)***
7	• $((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$	***аксиома (И2)***
8	• $\Gamma \vdash ((A \to B) \to (A \to C))$	***MP(6, 7)***
9	• $\Gamma \vdash (A \to C)$	***MP(2, 8)***
10	• $\Gamma, A \vdash C$	***дедукция***

Правило объединения посылок: $\dfrac{\Gamma \vdash \mathcal{A} \to (\mathcal{B} \to C)}{\Gamma \vdash \mathcal{A} \wedge \mathcal{B} \to C}$.

1	• $\Gamma \vdash (A \to (B \to C))$	***дано***
2	• $\Gamma, A \vdash (B \to C)$	***дедукция***
3	• $((A \to A) \to ((A \to B) \to (A \to (A \wedge B))))$	***(К3)*** $(\mathcal{A} := A =: \mathcal{B},\ C := B)$
4	• $(A \to A)$	***доказуема***
5	• $((A \to B) \to (A \to (A \wedge B)))$	***MP(3, 4)***
6	• $(A \wedge B) \to A$	***(К1)***
7	• $(A \wedge B) \vdash A$	***дедукция***
8	• $\Gamma, (A \wedge B) \vdash A$	***расширение посылок***

9 • $\Gamma, (A \wedge B) \vdash (B \to C)$ ***силлогизм(2, 8)***
10 • $\Gamma, (A \wedge B), B \vdash C$ ***дедукция***
11 • $((A \wedge B) \to B)$ ***(К2)***
12 • $(A \wedge B) \vdash B$ ***дедукция***
13 • $\Gamma, (A \wedge B) \vdash B$ ***расширение посылок***
14 • $\Gamma, (A \wedge B) \vdash C$ ***силлогизм(10, 13)***
15 • $\Gamma \vdash ((A \wedge B) \to C)$ ***дедукция***

Правило разделения посылок: $\dfrac{\Gamma \vdash \mathcal{A} \wedge \mathcal{B} \to C}{\Gamma \vdash \mathcal{A} \to (\mathcal{B} \to C)}$.

1 • $\Gamma \vdash ((A \wedge B) \to C)$ ***дано***
2 • $\Gamma, (A \wedge B) \vdash C$ ***дедукция***
3 • $\Gamma, A, (A \wedge B) \vdash C$ ***расширение посылок***
4 • $((A \to A) \to ((A \to B) \to (A \to (A \wedge B))))$ ***(К3)*** $(\mathcal{A} := A, \mathcal{B} := A, C := B)$
5 • $(A \to A)$ ***доказуема***
6 • $((A \to B) \to (A \to (A \wedge B)))$ ***MP(4, 5)***
7 • $B, A \vdash B$ 2^0
8 • $B \vdash (A \to B)$ ***дедукция***
9 • $B \vdash (A \to (A \wedge B))$ ***MP(6, 8)***
10 • $B, A \vdash (A \wedge B)$ ***дедукция***
11 • $\Gamma, B, A \vdash (A \wedge B)$ ***расширение посылок***
12 • $\Gamma, A, B \vdash C$ ***силлогизм(3, 11)***
13 • $\Gamma, A \vdash (B \to C)$ ***дедукция***
14 • $\Gamma \vdash (A \to (B \to C))$ ***дедукция***

Правила удаления конъюнкции: $\dfrac{\Gamma \vdash \mathcal{A} \wedge \mathcal{B}}{\Gamma \vdash \mathcal{A}}$, $\dfrac{\Gamma \vdash \mathcal{A} \wedge \mathcal{B}}{\Gamma \vdash \mathcal{B}}$.

1 • $\Gamma \vdash (A \wedge B)$ ***дано***
2 • $(A \wedge B) \to A$ ***(К1)***
3 • $\Gamma \vdash A$ ***MP(1, 2)***

Второе правило докажите самостоятельно.

Правила введения конъюнкции: $\dfrac{\Gamma \vdash \mathcal{A};\ \Gamma \vdash \mathcal{B}}{\Gamma \vdash \mathcal{A} \wedge \mathcal{B}}$.

1 • $\Gamma \vdash A$ ***дано***
2 • $\Gamma \vdash B$ ***дано***
3 • $\Gamma, A \vdash B$ ***расширение посылок***
4 • $\Gamma \vdash (A \to B)$ ***дедукция***
5 • $((A \to A) \to ((A \to B) \to (A \to (A \wedge B))))$ ***(К3)*** $(\mathcal{A} := A, \mathcal{B} := A, C := B)$

6 • $(A \to A)$ ***доказуема***
7 • $((A \to B) \to (A \to (A \wedge B)))$ ***MP(5, 6)***
8 • $\Gamma \vdash (A \to (A \wedge B))$ ***MP(4, 7)***
9 • $\Gamma \vdash (A \wedge B)$ ***MP(1, 8)***

Правила введения дизъюнкции: $\dfrac{\Gamma \vdash \mathcal{A}}{\Gamma \vdash \mathcal{A} \vee \mathcal{B}}, \dfrac{\Gamma \vdash \mathcal{B}}{\Gamma \vdash \mathcal{A} \vee \mathcal{B}}$.

1 • $\Gamma \vdash A$ ***дано***
2 • $(A \to (A \vee B))$ ***(ДЗ)***
3 • $\Gamma \vdash (A \vee B)$ ***MP(1, 2)***

Второе правило докажите самостоятельно.

Правило modus tollens: $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma \vdash \overline{\mathcal{B}}}{\Gamma \vdash \overline{\mathcal{A}}}$.

1 • $\Gamma, A \vdash B$ ***дано***
2 • $\Gamma \vdash (A \to B)$ ***дедукция***
3 • $\Gamma \vdash \overline{B}$ ***дано***
4 • $((A \to B) \to (\overline{B} \to \overline{A}))$ ***(ОЗ)***
5 • $\Gamma \vdash (\overline{B} \to \overline{A})$ ***MP(2, 4)***
6 • $\Gamma \vdash \overline{A}$ ***MP(3, 5)***

Правило контрапозиции: $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B}}{\Gamma, \overline{\mathcal{B}} \vdash \overline{\mathcal{A}}}$.

1 • $\Gamma, A \vdash B$ ***дано***
2 • $\Gamma \vdash (A \to B)$ ***дедукция***
3 • $((A \to B) \to (\overline{B} \to \overline{A}))$ ***аксиома (ОЗ)***
4 • $\Gamma \vdash (\overline{B} \to \overline{A})$ ***MP(2, 3)***
5 • $\Gamma, \overline{B} \vdash \overline{A}$ ***дедукция***

Правило опровержения: $\dfrac{\Gamma, \mathcal{A} \vdash \mathcal{B};\ \Gamma, \mathcal{A} \vdash \overline{\mathcal{B}}}{\Gamma \vdash \overline{\mathcal{A}}}$.

1 • $\Gamma, A \vdash B$ ***дано***
2 • $\Gamma, A, A \vdash B$ ***расширение посылок***
3 • $\Gamma, A \vdash \overline{B}$ ***дано***
4 • $\Gamma, A \vdash \overline{A}$ ***modus tollens(2, 3)***
5 • $\Gamma, A \vdash A$ ***2^0***
6 • $\Gamma, A \vdash (A \wedge \overline{A})$ ***введение $\wedge$***

7	• $(A \wedge \overline{A}) \vdash A$	***(К1)***
8	• $(A \wedge \overline{A}),\ \overline{\overline{(A \to A)}} \vdash A$	***расширение посылок***
9	• $(A \wedge \overline{A}) \vdash \overline{A}$	***(К2)***
10	• $(A \wedge \overline{A}) \vdash \overline{\overline{(A \to A)}}$	***modus tollens(8, 9)***
11	• $\overline{\overline{(A \to A)}} \to \overline{(A \to A)}$	***(О2)***
12	• $(A \wedge \overline{A}) \vdash \overline{(A \to A)}$	***силлогизм(10,11)***
13	• $\overline{\overline{(A \to A)}} \vdash \overline{(A \wedge \overline{A})}$	***контрапозиция(10)***
14	• $(A \to A) \to \overline{\overline{(A \to A)}}$	***(О1)***
15	• $(A \to A) \vdash \overline{\overline{(A \to A)}}$	***дедукция***
16	• $(A \to A) \vdash \overline{(A \wedge \overline{A})}$	***силлогизм(13, 15)***
17	• $(A \to A) \to \overline{(A \wedge \overline{A})}$	***дедукция***
18	• $(A \to A)$	***доказуема***
19	• $\overline{(A \wedge \overline{A})}$	***MP(17, 18)***
20	• $\Gamma \vdash \overline{(A \wedge \overline{A})}$	***расширение посылок***
21	• $\Gamma \vdash \overline{A}$	***modus tollens(6, 20)***

4. Основные равносильности ИВ. Две формулы A и B исчисления высказываний назовём *равносильными* и будем писать $A \sim B$, если доказуемы обе формулы $A \to B$ и $B \to A$. Это понятие, конечно, аналогично понятию равносильности $\equiv$ формул, изученному в главе I, и как будет показано далее, на самом деле совпадает с ним.

Докажем формально самые важные из знакомых основных равносильностей.

Закон идемпотентности: $(A \wedge A) \sim A$, $(A \vee A) \sim A$.

1	• $(A \wedge A) \to A$	***(К1)***
2	• $((A \to A) \to ((A \to A) \to (A \to (A \wedge A))))$	***(К3)***
3	• $(A \to A)$	***доказуема***
4	• $((A \to A) \to (A \to (A \wedge A)))$	***MP(1, 2)***
5	• $(A \to (A \wedge A))$	***MP(3, 2)***

Для дизъюнкции докажите самостоятельно.

Коммутативность: $(A \wedge B) \sim (B \wedge A)$, $(A \vee B) \sim (B \vee A)$.

1	• $(A \to (A \vee B))$	***(Д1)***
2	• $(B \to (A \vee B))$	***(Д2)***
3	• $((B \to (A \vee B)) \to ((A \to (A \vee B)) \to ((B \vee A) \to (A \vee B))))$	***(Д3)***
4	• $((A \to (A \vee B)) \to ((B \vee A) \to (A \vee B)))$	***MP(2, 3)***
5	• $((B \vee A) \to (A \vee B)))$	***MP(1, 4)***

Импликация $((A \vee B) \to (B \vee A))$ доказывается аналогично.

Для конъюнкции докажите самостоятельно.

Ассоциативность: ***((A ∧ B) ∧ C) ~ (A ∧ (B ∧ C)), ((A ∨ B) ∨ C) ~ (A ∨ (B ∨ C)).***

1	• $(((A \wedge B) \wedge C) \to (A \wedge B))$	***(К1)***
2	• $((A \wedge B) \wedge C) \vdash (A \wedge B)$	***дедукция***
3	• $(((A \wedge B) \wedge C) \to C)$	***(К2)***
4	• $((A \wedge B) \wedge C) \vdash C$	***дедукция***
5	• $((A \wedge B) \to A)$	***(К1)***
6	• $(A \wedge B) \vdash A$	***дедукция***
7	• $((A \wedge B) \to B)$	***(К2)***
8	• $(A \wedge B) \vdash B$	***дедукция***
9	• $((A \wedge B) \wedge C) \vdash A$	***силлогизм(2, 6)***
10	• $((A \wedge B) \wedge C) \vdash B$	***силлогизм(2, 8)***
11	• $((A \wedge B) \wedge C) \vdash (B \wedge C)$	***введение ∧ (4, 10)***
12	• $((A \wedge B) \wedge C) \vdash (A \wedge (B \wedge C))$	***введение ∧ (9, 11)***
13	• $((A \wedge B) \wedge C) \to (A \wedge (B \wedge C))$	***дедукция***

Импликация $((A \wedge (B \wedge C)) \to ((A \wedge B) \wedge C))$ доказывается аналогично.

Для дизъюнкции докажите самостоятельно.

Дистрибутивность: ***((A ∧ B) ∨ C) ~ ((A ∨ C) ∧ (B ∨ C))),***
((A ∨ B) ∧ C) ~ ((A ∧ C) ∨ (B ∧ C))).

1	• $((A \wedge B) \to A)$	***(К1)***
2	• $(A \wedge B) \vdash A$	***дедукция***
3	• $((A \wedge B) \to B)$	***(К2)***
4	• $(A \wedge B) \vdash B$	***дедукция***
5	• $(A \to (A \vee C))$	***(Д1)***
6	• $A \vdash (A \vee C)$	***дедукция***
7	• $(A \wedge B) \vdash (A \vee C)$	***силлогизм (2, 6)***
8	• $(B \to (B \vee C))$	***(Д1)***
9	• $B \vdash (B \vee C)$	***дедукция***
10	• $(A \wedge B) \vdash (B \vee C)$	***силлогизм (4, 9)***
11	• $(A \wedge B) \vdash ((A \vee C) \wedge (B \vee C))$	***введение ∧ (7, 10)***
12	• $((A \wedge B) \to ((A \vee C) \wedge (B \vee C)))$	***дедукция***
13	• $(C \to (A \vee C))$	***(Д2)***
14	• $C \vdash (A \vee C)$	***дедукция***
15	• $(C \to (B \vee C))$	***(Д2)***
16	• $C \vdash (B \vee C)$	***дедукция***
17	• $C \vdash ((A \vee C) \wedge (B \vee C))$	***введение ∧ (14, 16)***
18	• $(C \to ((A \vee C) \wedge (B \vee C)))$	***дедукция***
19	• $(((A \wedge B) \to ((A \vee C) \wedge (B \vee C))) \to ((C \to ((A \vee C) \wedge (B \vee C))) \to$ $\to (((A \wedge B) \vee C) \to ((A \vee C) \wedge (B \vee C)))))$	***(Д3)***

20 • $((C \to ((A \vee C) \wedge (B \vee C))) \to (((A \wedge B) \vee C) \to ((A \vee C) \wedge (B \vee C))))$ ***MP(12, 19)***

21 • $(((A \wedge B) \vee C) \to ((A \vee C) \wedge (B \vee C)))$ ***MP(18, 20)***

1 • $B, A \vdash (A \wedge B)$ ***(почему ?!)***

2 • $B, A \vdash (A \wedge B) \vee C$ ***(почему ?!)***

3 • $B \vdash (A \to ((A \wedge B) \vee C))$ ***(дедукция)***

4 • $(C \to ((A \wedge B) \vee C)))$ ***(почему ?!)***

5 • $B \vdash ((A \to ((A \wedge B) \vee C)) \to ((C \to ((A \wedge B) \vee C))) \to$
$\to ((A \vee C) \to ((A \wedge B) \vee C))))$ ***(Д3)***

6 • $B \vdash ((C \to ((A \wedge B) \vee C))) \to ((A \vee C) \to ((A \wedge B) \vee C)))$ ***MP(3, 5)***

7 • $B \vdash ((A \vee C) \to ((A \wedge B) \vee C))$ ***MP(4, 6)***

8 • $B, (A \vee C) \vdash ((A \wedge B) \vee C)$ ***дедукция***

9 • $(A \vee C) \vdash (B \to ((A \wedge B) \vee C))$ ***дедукция***

10 • $(A \vee C) \vdash (C \to ((A \wedge B) \vee C))$ ***(почему ?!)***

11 • $(A \vee C) \vdash ((B \to ((A \wedge B) \vee C)) \to ((C \to ((A \wedge B) \vee C)) \to$
$\to ((B \vee C) \to ((A \wedge B) \vee C))))$ ***(Д3)***

12 • $(A \vee C) \vdash ((C \to ((A \wedge B) \vee C)) \to ((B \vee C) \to ((A \wedge B) \vee C)))$ ***MP(9, 11)***

13 • $(A \vee C) \vdash ((B \vee C) \to ((A \wedge B) \vee C))$ ***MP(10, 12)***

14 • $(A \vee C) \wedge (B \vee C) \vdash (A \vee C)$ ***(почему ?!)***

15 • $(A \vee C) \wedge (B \vee C) \vdash ((B \vee C) \to ((A \wedge B) \vee C))$ ***силлогизм (13, 14)***

16 • $(A \vee C) \wedge (B \vee C) \vdash (B \vee C)$ ***(почему ?!)***

17 • $(A \vee C) \wedge (B \vee C) \vdash ((A \wedge B) \vee C)$ ***MP(15, 16)***

18 • $((A \vee C) \wedge (B \vee C) \to ((A \wedge B) \vee C))$ ***дедукция***

Законы де Моргана: $\overline{(A \wedge B)} \sim \overline{A} \vee \overline{B}$, $\overline{(A \vee B)} \sim \overline{A} \wedge \overline{B}$.

1 • $(A \wedge B) \vdash A$ ***(почему ?!)***

2 • $\overline{A} \vdash \overline{(A \wedge B)}$ ***контрапозиция***

3 • $\overline{A} \to \overline{(A \wedge B)}$ ***дедукция***

4 • $(A \wedge B) \vdash B$ ***(почему ?!)***

5 • $\overline{B} \vdash \overline{(A \wedge B)}$ ***контрапозиция***

6 • $\overline{B} \to \overline{(A \wedge B)}$ ***дедукция***

7 • $((\overline{A} \to \overline{(A \wedge B)}) \to ((\overline{B} \to \overline{(A \wedge B)}) \to ((\overline{A} \vee \overline{B}) \to \overline{(A \wedge B)})))$ ***(?!)***

8 • $((\overline{B} \to \overline{(A \wedge B)}) \to ((\overline{A} \vee \overline{B}) \to \overline{(A \wedge B)}))$ ***MP(3, 7)***

9 • $((\overline{A} \vee \overline{B}) \to \overline{(A \wedge B)})$ ***MP(6, 8)***

1 • $(\overline{A} \to (\overline{A} \vee \overline{B}))$ ***(Д1)***

2 • $(\overline{(\overline{A} \vee \overline{B})} \to \overline{\overline{A}})$ ***контрапозиция***

3 • $\overline{(\overline{A} \vee \overline{B})} \vdash \overline{\overline{A}}$ ***дедукция***

4 • $\overline{\overline{A}} \vdash A$ ***(?!)***

5 • $\overline{(\overline{A} \vee \overline{B})} \vdash A$ ***силлогизм***

6 • $\overline{(\overline{A} \vee \overline{B})} \vdash B$ ***аналогично (?!)***

7 • $\overline{(\overline{A} \vee \overline{B})} \vdash A \wedge B$ ***(?!)***

8 • $\overline{(A \wedge B)} \vdash \overline{\overline{(\overline{A} \vee \overline{B})}}$ ***контрапозиция***

9 • $\overline{(A \wedge B)} \vdash (\overline{A} \vee \overline{B})$ ***(?!)***

10 • $(\overline{(A \wedge B)} \rightarrow (\overline{A} \vee \overline{B}))$ ***дедукция***

Закон выражения импликации: $(A \rightarrow B) \sim (\overline{A} \vee B)$

1 • $\overline{B}, (A \rightarrow B) \vdash (A \rightarrow B)$ 2^0

2 • $A, \overline{B}, (A \rightarrow B) \vdash B$ ***дедукция***

3 • $A, \overline{B}, (A \rightarrow B) \vdash \overline{B}$ 2^0

4 • $A, \overline{B} \vdash \overline{(A \rightarrow B)}$ ***приведение к противоречию***

5 • $A \vdash (\overline{B} \rightarrow \overline{(A \rightarrow B)})$ ***дедукция***

6 • $(A \wedge \overline{B}) \vdash A$ ***(?!)***

7 • $(A \wedge \overline{B}) \vdash (\overline{B} \rightarrow \overline{(A \rightarrow B)})$ ***силлогизм (5, 6)***

8 • $((A \wedge \overline{B}) \rightarrow (\overline{B} \rightarrow \overline{(A \rightarrow B)}))$ ***дедукция***

9 • $(((A \wedge \overline{B}) \rightarrow (\overline{B} \rightarrow \overline{(A \rightarrow B)})) \rightarrow$
$\rightarrow (((A \wedge \overline{B}) \rightarrow \overline{B}) \rightarrow ((A \wedge \overline{B}) \rightarrow \overline{(A \rightarrow B)})))$ ***И2)***

10 • $(((A \wedge \overline{B}) \rightarrow \overline{B}) \rightarrow ((A \wedge \overline{B}) \rightarrow \overline{(A \rightarrow B)}))$ ***MP(8, 9)***

11 • $((A \wedge \overline{B}) \rightarrow \overline{B})$ ***(K2)***

12 • $((A \wedge \overline{B}) \rightarrow \overline{(A \rightarrow B)})$ ***MP(10, 11)***

13 • $(\overline{\overline{(A \rightarrow B)}} \rightarrow \overline{(A \wedge \overline{B})})$ ***контрапозиция***

14 • $\overline{\overline{(A \rightarrow B)}} \vdash \overline{(A \wedge \overline{B})}$ ***дедукция***

15 • $(A \rightarrow B) \vdash \overline{\overline{(A \rightarrow B)}}$ ***(O1)***

16 • $(A \rightarrow B) \vdash \overline{(A \wedge \overline{B})}$ ***силлогизм***

17 • $\overline{(A \wedge \overline{B})} \vdash (\overline{A} \vee \overline{\overline{B}})$ ***де Морган***

18 • $(A \rightarrow B) \vdash (\overline{A} \vee \overline{\overline{B}})$ ***силлогизм***

19 • $(\overline{A} \vee \overline{\overline{B}}) \vdash (\overline{A} \vee B)$ ***(?!)***

20 • $(A \rightarrow B) \vdash (\overline{A} \vee B)$ ***силлогизм (18, 19)***

1 • $\overline{A}, A, \overline{B} \vdash A$ 2^0

2 • $\overline{A}, A, \overline{B} \vdash \overline{A}$ 2^0

3 • $\overline{A}, A \vdash \overline{\overline{B}}$ ***приведение к противоречию***

4 • $(\overline{\overline{B}} \rightarrow B)$ ***(O2)***

5 • $\overline{A},\ A \vdash B$ ***силлогизм (3, 4)***

6 • $\overline{A} \vdash (A \to B)$ ***дедукция***

7 • $(\overline{A} \to (A \to B))$ ***дедукция***

8 • $(B \to (A \to B))$ ***(И1)***

9 • $((\overline{A} \to (A \to B)) \to ((B \to (A \to B)) \to ((\overline{A} \vee B) \to (A \to B))))$ ***(ДЗ)***

10 • $((B \to (A \to B)) \to ((\overline{A} \vee B) \to (A \to B)))$ ***МР(7, 9)***

11 • $((\overline{A} \vee B) \to (A \to B))$ ***МР(8, 10)***

5. Некоторые свойства отношения равносильности формул. Во всех нижеперечисленных свойствах A, Φ, Ψ – *формулы ИВ.*

1⁰. *Отношение равносильности обладает свойствами*

рефлексивности: $A \sim A$,

симметричности: если $A \sim B$, *то* $B \sim A$,

транзитивности: если $A \sim B$, $B \sim C$, *то* $A \sim C$.

Свойства рефлексивности и симметричности очевидны. Транзитивность следует из правила силлогизма.

2⁰. *Если* $\Phi \sim \Psi$, *то* $(A \wedge \Phi) \sim (A \wedge \Psi)$, $(\Phi \wedge A) \sim (\Psi \wedge A)$.

В самом деле, известно, что формулы $(\Phi \to \Psi)$ и $(\Psi \to \Phi)$ доказуемы, и нужно доказать формулы $((A \wedge \Phi) \to (A \wedge \Psi))$ и $((A \wedge \Psi) \to (A \wedge \Phi))$.

1 • $(\Phi \to \Psi)$ ***дано***

2 • $((A \wedge \Phi) \to A)$

3 • $(A \wedge \Phi) \vdash \Phi$

4 • $(A \wedge \Phi) \vdash \Psi$ ***силлогизм (1, 3)***

5 • $(((A \wedge \Phi) \to A) \to (((A \wedge \Phi) \to \Psi) \to (((A \wedge \Phi) \to (A \wedge \Psi)))))$

6 • $(((A \wedge \Phi) \to \Psi) \to ((A \wedge \Phi) \to (A \wedge \Psi)))$

7 • $((A \wedge \Phi) \to (A \wedge \Psi))$

Вторая импликация доказывается аналогично.

3⁰. *Если* $\Phi \sim \Psi$, *то* $(A \vee \Phi) \sim (A \vee \Psi)$, $(\Phi \vee A) \sim (\Psi \vee A)$.

1 • $(\Phi \to \Psi)$

2 • $\Psi \vdash (A \vee \Psi)$

3 • $(\Phi \to (A \vee \Psi))$

4 • $(A \to (A \vee \Psi))$

5 • $((A \to (A \vee \Psi)) \to ((\Phi \to (A \vee \Psi)) \to ((A \vee \Phi) \to (A \vee \Psi))))$

6 • $((\Phi \to (A \vee \Psi)) \to ((A \vee \Phi) \to (A \vee \Psi)))$

7 • $((A \vee \Phi) \to (A \vee \Psi))$

Вторая импликация доказывается аналогично.

4⁰. *Если* $\Phi \sim \Psi$, *то* $(A \to \Phi) \sim (A \to \Psi)$, $(\Phi \to A) \sim (\Psi \to A)$.

Воспользуемся уже доказанными свойствами:

$(A \to \Phi) \sim (\overline{A} \vee \Phi) \sim (\overline{A} \vee \Psi) \sim (A \to \Psi)$,

$(\Phi \to A) \sim (\overline{\Phi} \vee A) \sim (\overline{\Psi} \vee A) \sim (\Psi \to A)$.

5^0. *Если* $\Phi \sim \Psi$, *то* $\overline{\Phi} \sim \overline{\Psi}$.

Следует из закона контрапозиции.

7^0. *Если формула* Φ *доказуема, то* $(A \wedge \Phi) \sim A$.

Действительно, импликация $((A \wedge \Phi) \to A)$ является аксиомой ***(К1)***, а обратная импликация доказывается так:

1	• $\vdash \Phi$	***дано***
2	• $A \vdash \Phi$	***расширение посылок***
3	• $(A \to \Phi)$	***дедукция***
4	• $(A \to A)$	***доказуема***
5	• $((A \to A) \to ((A \to \Phi) \to (A \to (A \wedge \Phi))))$	***аксиома***
6	• $((A \to \Phi) \to (A \to (A \wedge \Phi)))$	***MP***
7	• $(A \to (A \wedge \Phi))$	***MP***

8^0. *Если формула* Φ *доказуема, то* $(A \vee \Phi) \sim \Phi$.

$(\Phi \to (A \vee \Phi))$ – аксиома ***(Д2)***.

1	• $\vdash \Phi$	***дано***
2	• $A \vdash \Phi$	***расширение посылок***
3	• $(A \to \Phi)$	***дедукция***
4	• $(\Phi \to \Phi)$	***доказуема***
5	• $((A \to \Phi) \to ((\Phi \to \Phi) \to ((A \vee \Phi) \to \Phi)))$	***аксиома***
6	• $((\Phi \to \Phi) \to ((A \vee \Phi) \to \Phi))$	***MP***
7	• $((A \vee \Phi) \to \Phi)$	***MP***

9^0. *Если формула* Φ *доказуема, то* $(A \wedge \overline{\Phi}) \sim \overline{\Phi}$.

Действительно, $(A \wedge \overline{\Phi}) \sim \overline{\Phi}$ тогда и только тогда, когда $\overline{(A \wedge \overline{\Phi})} \sim \overline{\overline{\Phi}}$, что ввиду доказанных равносильностей имеет место в случае $(\overline{A} \vee \Phi) \sim \Phi$, что следует из доказанного ранее свойства 8^0.

10^0. *Если формула* Φ *доказуема, то* $(A \vee \overline{\Phi}) \sim A$.

Докажите самостоятельно аналогично свойству 9^0 .

11^0. $(A \wedge (\Phi \vee \overline{\Phi})) \sim A$

12^0. $(A \vee (\Phi \vee \overline{\Phi})) \sim (\Phi \vee \overline{\Phi})$.

13⁰. $(A \wedge (\Phi \wedge \overline{\Phi})) \sim (\Phi \wedge \overline{\Phi})$.

14⁰. $(A \vee (\Phi \wedge \overline{\Phi})) \sim A$.

Для доказательства этих свойств достаточно обосновать доказуемость формул $(\Phi \vee \overline{\Phi})$ и $\overline{(\Phi \wedge \overline{\Phi})}$, которые к тому же равносильны (?!). Доказуемость второй из этих формул была установлена при обосновании правила опровержения (найдите соответствующий фрагмент доказательства !!). Для краткости воспользуемся правилом опровержения:

1	• $(\Phi \wedge \overline{\Phi}) \vdash \Phi$	***(К1)***
2	• $(\Phi \wedge \overline{\Phi}) \vdash \overline{\Phi}$	***(К2)***
3	• $\vdash \overline{(\Phi \wedge \overline{\Phi})}$	***правило опровержения***

Упражнение: Докажите формально остальные основные равносильности.

6. Доказуемость и тождественная истинность формул. Теперь уже можно доказать основной результат этого параграфа.

Теорема (о доказуемости и тождественной истинности формул ИВ). *Формула формального исчисления высказываний доказуема тогда и только тогда, когда она тождественно истинна.*

Доказательство. То, что доказуемая формула является тождественно истинной, уже отмечалось выше: для этого нужно лишь заметить, что все аксиомы исчисления высказываний тождественно истинны и что множество всех тождественно истинных формул замкнуто относительно правила вывода *modus ponens*.

Для доказательства обратного утверждения заметим, что обоснованные выше равносильности позволяют приводить формулы исчисления высказываний к дизъюнктивной форме по тому же алгоритму, что использовался в неформальном изложении алгебры высказываний для упрощения формул:

- *избавиться от всех импликаций, выразив её через дизъюнкцию и отрицание.*
- *избавиться от "длинных отрицаний" с помощью законов де Моргана.*
- *избавиться от кратных отрицаний, применив закон двойного отрицания.*
- *использовать законы ассоциативности, коммутативности, идемпотентности, дистрибутивности для приведения формулы к дизъюнктивной форме.*
- *использовать законы поглощения, ограничения, склейки и другие для упрощения формул.*

Упражнение. Докажите законы поглощения, ограничения, склейки и другие, полезные для упрощения формул.

Примеры: 1. $\overline{\overline{\overline{(x \to y)} \vee (x \wedge \overline{y})} \to (\overline{x} \wedge (x \vee \overline{y}))} \sim$

$\sim \overline{\overline{\overline{\overline{(x \to y)} \vee (x \wedge \overline{y})} \vee (\overline{x} \wedge (x \vee \overline{y}))}} \sim$

$\sim (\overline{\overline{(x \to y)} \vee (x \wedge \overline{y})} \vee (\overline{x} \wedge (x \vee \overline{y}))) \sim$

$\sim (((\overline{\overline{x}} \wedge \overline{y}) \vee (x \wedge \overline{y})) \vee (\overline{x} \wedge (x \vee \overline{y}))) \sim$

$\sim (((x \wedge \overline{y}) \vee (x \wedge \overline{y})) \vee (\overline{x} \wedge (x \vee \overline{y}))) \sim$

$\sim ((x \wedge \overline{y}) \vee ((\overline{x} \wedge x) \vee (\overline{x} \wedge \overline{y}))) \sim ((x \wedge \overline{y}) \vee (\overline{x} \wedge \overline{y}))$ *(СДНФ)* $\sim$

$\sim \overline{y} \sim$ *(?!)* $\sim (x \vee \overline{y}) \wedge (\overline{x} \vee \overline{y})$ *(СКНФ).*

2. $((a \to b) \to ((a \to c) \to (a \to (b \wedge c))) \sim ((\overline{a} \vee b) \to ((\overline{a} \vee c) \to (\overline{a} \vee (b \wedge c))) \sim$

$\sim (\overline{(\overline{a} \vee b)} \vee (\overline{(\overline{a} \vee c)} \vee (\overline{a} \vee (b \wedge c)))) \sim ((a \wedge \overline{b}) \vee ((a \wedge \overline{c}) \vee (\overline{a} \vee (b \wedge c)))) \sim$

$\sim (a \wedge \overline{b}) \vee (a \wedge \overline{c}) \vee \overline{a} \vee (b \wedge c) \sim (a \wedge \overline{b}) \vee ((a \vee \overline{a}) \wedge (\overline{c} \vee \overline{a})) \vee (b \wedge c) \sim$

$\sim (a \wedge \overline{b}) \vee \overline{c} \vee \overline{a} \vee (b \wedge c) \sim ((a \wedge \overline{b}) \vee \overline{a}) \vee (\overline{c} \vee (b \wedge c)) \sim$

$\sim ((a \vee \overline{a}) \wedge (\overline{b} \vee \overline{a})) \vee ((\overline{c} \vee b) \wedge (\overline{c} \vee c)) \sim (\overline{b} \vee \overline{a}) \vee (\overline{c} \vee b) \sim$

$\sim (\overline{a} \vee \overline{c}) \vee (b \vee \overline{b}) \sim (b \vee \overline{b}) \sim$ *(?!)* $\sim$

$\sim (a \wedge b \wedge c) \vee (a \wedge b \wedge \overline{c}) \vee (a \wedge \overline{b} \wedge c) \vee (a \wedge \overline{b} \wedge \overline{c}) \vee$

$\vee (\overline{a} \wedge b \wedge c) \vee (\overline{a} \wedge b \wedge \overline{c}) \vee (\overline{a} \wedge \overline{b} \wedge c) \vee (\overline{a} \wedge \overline{b} \wedge \overline{c})$ *(СДНФ).*

Рассуждая в общем виде, можно доказать теорему о *СДНФ* и *СКНФ*:

Теорема (о СДНФ и СКНФ). *(1) Любая формула ИВ равносильна либо противоречию* $(x \wedge \overline{x})$*, либо единственной СДНФ.*

(2) Любая формула ИВ равносильна либо тождественно истинной формуле $(x \vee \overline{x})$*, либо единственной СКНФ.*

Хотя сейчас вопросы о единственности получаемых форм нас не интересуют, подумайте, как это можно доказать.

Вернёмся теперь к доказательству теоремы о доказуемости и тождественной истинности формул. Поймём, что любая тождественно истинная формула Φ доказуема в формальном исчислении высказываний. По теореме о *СДНФ* либо $\Phi \sim (x \wedge \overline{x})$, либо $\Phi \sim D(x_1, \dots, x_n) = \bigvee\limits_{(\varepsilon_1; \dots; \varepsilon_n)} (x_1^{\varepsilon_1} \wedge \dots \wedge x_n^{\varepsilon_n})$. Поскольку равносильность $\sim$ формул сохраняет тождественную истинность (?!), то полученная формула тоже тождественно истинна. Поэтому первый случай невозможен, и $D(x_1, \dots, x_n)$ является тождественно истинной дизъюнктивной формой указанного выше вида.

Когда *СДНФ* тождественно истинна ? Докажем, что это возможно только в случае $D(x_1, \dots, x_n) \sim (x \vee \overline{x})$. Отсюда будет следовать (?!) доказуемость формулы $D(x_1, \dots, x_n)$, а значит, доказуемость и исходной тождественно истинной формулы Φ.

Если в $D(x_1, \dots, x_n)$ участвует некоторая переменная x, то группируя с помощью закона дистрибутивности все конъюнкции, содержащие x и $\overline{x}$ соответственно, *СДНФ* можно записать в виде

$$D(x, y_1, \dots, y_{n-1}) \sim (x \wedge D_x) \vee (\overline{x} \wedge D_{\overline{x}}) \vee D_0,$$

где D_x, $D_{\overline{x}}$ и D_0 – некоторые *ДНФ*, не зависящие от x и $\overline{x}$ (D_0 и $D_{\overline{x}}$ могут быть пустыми, а D_x – нет). Можно считать, что D_0 отсутствует:

$$(x \wedge D_x) \vee (\overline{x} \wedge D_{\overline{x}}) \vee D_0 \sim (x \wedge D_x) \vee (\overline{x} \wedge D_{\overline{x}}) \vee (x \wedge D_0 \vee \overline{x} \wedge D_0) \sim$$

$$\sim (x \wedge (D_x \vee D_0)) \vee (\overline{x} \wedge (D_{\overline{x}} \vee D_0)).$$

Значит, можно сразу считать, что $D(x, y_1, \dots, y_{n-1}) \sim (x \wedge D_x) \vee (\overline{x} \wedge D_{\overline{x}})$. При этом формулы D_x и $D_{\overline{x}}$ непусты: если, например, D_x отсутствует, то получаем противоречие с тождественной истинностью формулы D:

$$D(1, y_1, \dots, y_{n-1}) = \overline{1} \wedge D_{\overline{x}} = 0.$$

Подставляя $x = 0$, получим тождественно истинную *ДНФ* $D_{\overline{x}}(y_1, \dots, y_{n-1})$ от меньшего количества переменных, так что $D_{\overline{x}}(y_1, \dots, y_{n-1}) \sim (y \vee \overline{y})$ и

$$D(x, y_1, \dots, y_{n-1}) \sim (x \wedge D_x) \vee (\overline{x} \wedge (y \vee \overline{y})) \sim (x \wedge D_x) \vee \overline{x}.$$

Аналогично, подставив $x = 1$, придём к $D_x(y_1, \dots, y_{n-1}) \sim (z \vee \overline{z})$,

$$D(x, y_1, \dots, y_{n-1}) \sim (x \wedge D_x) \vee \overline{x} \sim ((x \wedge (z \vee \overline{z})) \vee \overline{x}) \sim (x \vee \overline{x}),$$

что и требовалось.

Итак, исходная тождественно истинная формула равносильна доказуемой формуле $(x \vee \overline{x})$, а потому и сама доказуема.

Теорема полностью доказана.

Итак, обоснована адекватность формальной аксиоматической теории исчисления высказываний её неформальному варианту.

ПРИЛОЖЕНИЕ: ФОРМАЛЬНАЯ ТЕОРИЯ МНОЖЕСТВ

§ 1. Азы наивной теории множеств

В фундаменте современных математических теорий лежат понятия *множества, элемента множества, отношения принадлежности элемента множеству*. Интуитивный смысл этих понятий ясен: под множеством понимают *совокупность некоторых объектов (которые называются элементами данного множества), мыслимых как единое целое*. Для обозначения того, что объект a является элементом множества A, пишут $a \in A$ *(a принадлежит A)*. Вместо отрицания $\overline{a \in A}$ используется запись $a \notin A$ *(a не принадлежит A)*.

Наиболее употребительны следующие два способа задания множеств:

- *перечисление элементов* (используется в основном для множеств, состоящих из конечного числа элементов). Например, $A = \{1, 2, -5, 3\}$ – множество A состоит из элементов $1, 2, -5, 3$. Элементами множеств могут быть и объекты различной природы. Так, множество $A = \{1, \{1\}, a\}$ состоит из числа 1, одноэлементного множества $\{1\}$ (содержащего единственный элемент – число 1) и буквы a.
- *выделение множества в другом множестве с помощью характеристического свойства его элементов*: если B – множество и $P(x)$ – некоторое свойство (высказывание о произвольном элементе $x \in B$), то можно определить новое множество A всех элементов x множества B, удовлетворяющих свойству P, написав $A = \{x \in B \mid P(x)\ (= 1)\}$. Так, $\boldsymbol{R}_+ = \{x \in \boldsymbol{R} \mid x > 0\}$ – множество всех положительных действительных чисел.

Замечание: одно и то же множество можно задать различными способами: например, $\{-1, 1\} = \{r \in \boldsymbol{R} \mid r^2 = 1\} = \{n \in \boldsymbol{Z} \mid |n| = 1\}$. Поэтому важно ввести понятие равенства двух множеств.

Два множества A и B называются *равными* (символически $A = B$), если они состоят из одних и тех же элементов. Это значит, что для любого элемента $a \in A$ выполнено $a \in B$, и для любого элемента $b \in B$ выполняется $b \in A$. В противном случае множества A и B называются *неравными*: $A \neq B$.

Множество A называют *подмножеством множества* B (говорят также, что A *содержится в* B или B *содержит* A) и записывают $A \subseteq B$, если любой элемент множества A принадлежит множеству B.

Для удобства вводят в рассмотрение *пустое множество* $\varnothing$, не имеющее ни одного элемента. Ясно, что для любого множества A верно $\varnothing = \{x \in A \mid x \notin A\}$.

Примеры: 1. $\{1, 2, 3\} = \{3, 1, 2\}$. Хотя порядки перечисления элементов этих множеств и различны, но каждый элемент одного множества является элементом другого множества, что и обеспечивает их равенство.

2. $\{1, 2, 3\} = \{1, 1, 2, 3, 2, 1, 3\}$. Второе множество, хотя и выглядит толще первого, но на самом деле состоит их тех же элементов.

3. $\{1, 2, 3\} \neq \{3, \{1\}, 2\}$. Элемент 1 первого множества не является элементом второго множества. Точно так же Элемент $\{1\}$ второго множества не является элементом первого множества. Кстати, почему $1 \neq \{1\}$?

4. $A = \{1, 2\} \neq \{1, 2, -1\} = B$, т.к. $-1 \in B$, но $-1 \notin A$, но $\{1, 2\} \subseteq \{1, 2, -1\}$, т.к. $1 \in B$ и $2 \in B$.

5. $\boldsymbol{N} = \{1, 2, 3, \ldots\} \subseteq \boldsymbol{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \subseteq \boldsymbol{Q} = \{\frac{m}{n} \in \boldsymbol{R} \mid m \in \boldsymbol{Z} \wedge n \in \boldsymbol{N}\} \subseteq \boldsymbol{R}$.

Основные операции над множествами

I. *Если A, B – множества, то существует множество $A \cup B$ – объединение множеств A и B, которое состоит из всех элементов, являющихся элементами либо множества A, либо множества B: $x \in A \cup B \leftrightarrow x \in A \vee x \in B$.*

Примеры: 1. Если $A = \{1, 2, 5, \varnothing\}$, $B = \{\{1\}, 2, 5, \varnothing\}$, то $A \cup B = \{1, 2, 5, \varnothing, \{1\}\}$.

2. Если $A = \{x \in \boldsymbol{R} \mid 1 < x \leq 5\}$, $B = \{x \in \boldsymbol{R} \mid -1 \leq x < 2\}$, то $A \cup B = [-1; 5]$, где $[-1; 5] = \{x \in \boldsymbol{R} \mid -1 \leq x \leq 5\}$.

II. *Если A, B – множества, то существует множество $A \cap B$ – пересечение множеств A и B, которое состоит из всех элементов, являющихся одновременно элементами и множества A, и множества B: $x \in A \cap B \leftrightarrow x \in A \wedge x \in B$.*

Примеры: 1. Если $A = \{1, 2, 5, \varnothing\}$, $B = \{\{1\}, 2, 5, \varnothing\}$, то $A \cap B = \{2, 5, \varnothing\}$.

2. Если $A = \{x \in \boldsymbol{R} \mid 1 < x \leq 5\}$, $B = \{x \in \boldsymbol{R} \mid -1 \leq x < 2\}$, то $A \cap B = (1; 2)$, где $(1; 2) = \{x \in \boldsymbol{R} \mid 1 < x < 2\}$.

3. $A \cap B = \{a \in A \mid a \in B\}$.

На основе понятий пересечения и объединения двух множеств можно ввести аналогичные операции над несколькими множествами:

$$A_1 \cap \ldots \cap A_n = (\ldots((A_1 \cap A_2) \cap A_3) \cap \ldots) \cap A_n ,$$

$$A_1 \cup \ldots \cup A_n = (\ldots((A_1 \cup A_2) \cup A_3) \cup \ldots) \cup A_n .$$

III. *Если A, B – множества, то существует множество $A \setminus B$ – разность множеств A и B, которое состоит из всех элементов, принадлежащих множеству A, но не принадлежащих множеству B: $x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B$.*

Примеры: 1. Если $A = \{1, 2, 5, \varnothing\}$, $B = \{\{1\}, 2, 5, \varnothing\}$, то $A \setminus B = \{1\}$.

2. Если $A = \{x \in \boldsymbol{R} \mid 1 < x \leq 5\}$, $B = \{x \in \boldsymbol{R} \mid -1 \leq x < 2\}$, то $A \setminus B = [2; 5]$.

3. $A \setminus B = \{a \in A \mid a \notin B\}$.

IV. *Если A – множество, то существует множество всех его подмножеств $\mathcal{B}(A)$, называемое также булеаном множества A, и состоящее из всех подмножеств множества A: $X \in \mathcal{B}(A) \leftrightarrow X \subseteq A$.*

Важно отметить, что булеан $\mathcal{B}(A)$ состоит из множеств (подмножество множества A само является множеством) и содержит в качестве элементов пустое множество $\varnothing$ и само множество A (которые в случае $A = \varnothing$ совпадают).

Примеры: 1. Если $A = \varnothing$, то $\mathcal{B}(A) = \{\varnothing\}$.

2. Если $A = \{1\}$, то $\mathcal{B}(A) = \{\varnothing, \{1\}\}$.

3. Если $A = \{1, 2\}$, то $\mathcal{B}(A) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

4. Если $A = \{1, 2, 3\}$, то $\mathcal{B}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

5. Можно доказать, что булеан n-элементного множества A состоит из 2^n элементов. Поэтому булеан часто называют *степенью множества* A и обозначают 2^A.

V. *Если A, B – множества, то существует их прямое (декартово) произведение $A\times B$, состоящее из всех упорядоченных пар $(a; b)$, где $a \in A$, $b \in B$:*

$$A\times B = \{(a; b) \mid a \in A \wedge b \in B\}.$$

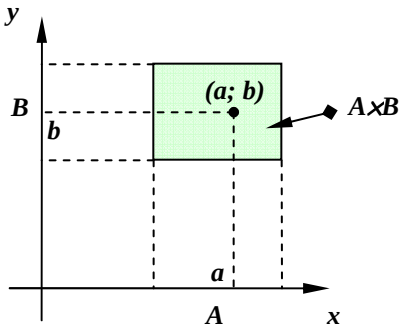
Примеры: 1. Если $A = \{1\}$, $B = \{0, 5\}$, то $A\times B = \{(1; 0), (1; 5)\}$.

2. Если $A = \{0, 2\}$, $B = \{0, 5\}$, то $A\times B = \{(0; 0), (0; 5), (2; 0), (2; 5)\}$.

3. Если множество A состоит из m элементов, а множество B – из n элементов, то можно доказать, что множество $A\times B$ состоит из $m\times n$ элементов. По этой причине в названии множества $A\times B$ используется термин “произведение”. Если $A = B$, то множество $A\times A$ состоит из m^2 элементов и называется *декартовым квадратом множества* A и обозначается через A^2.

Вслед за декартовым произведением двух можно ввести и *декартово произведение* $A_1 \times \ldots \times A_n = (\ldots((A_1 \times A_2) \times A_3)\times \ldots)\times A_n$ *n множеств* $A_1, \ldots, A_n$. Множество $\underbrace{A\times\ldots\times A}_{n}$ называется *декартовой степенью множества* A и обозначается A^n.

Декартово произведение $A\times B = \{(a; b) \mid a \in A \wedge b \in B\}$ двух множеств A и B иногда условно изображают на плоскости, трактуя компоненты упорядоченной пары $(a; b)$ как координаты: a – координата по оси x, на которой отмечают множество A, а b – координата по оси y, на которой отмечают множество B. Таким образом, элементы $(a; b) \in A\times B$ условно изображаются точками на плоскости с “координатами” a и b.



Особенно удобно графическое изображение декартова произведения $A\times B$ в случае, когда A и B – числовые множества, т.е. $A \subseteq \mathbf{R}$, $B \subseteq \mathbf{R}$. Тогда изображение принимает не условный характер, а имеет вполне конкретный геометрический смысл: множество $A\times B$ представляет из себя множество точек $M(a; b)$ декартовой плоскости, первая координата a которых принадлежит множеству A, а вторая b – принадлежит множеству B.

§ 2. Аксиоматика Цермело-Френкеля теории множеств

В § 1 приложения были даны основные понятия теории множеств. Однако развиваемая на этом основании Г. Кантором наивная теория множеств столкнулась в конце XIX в. с трудностями. Вот – лишь один пример парадокса наивной теории множеств.

Парадокс Рассела: *Пусть U – множество всех множеств. Рассмотрим множество $M = \{A \in U \mid A \notin A\}$ и попробуем ответить на вопрос: верно ли, что $M \in M$?* Если это утверждение истинно, т.е. $M \in M$, то получаем противоречие с определением множества M – оно образовано только из тех множеств, которые не являются элементами самих себя. Однако и предположение $M \notin M$ тоже ведёт к противоречию, т.к. в этом случае (по определению множества M) должно быть выполнено $M \in M$. Итак, получено противоречие.

Выход из создавшейся ситуации только один – нельзя считать "множество всех множеств" U множеством: если U – не множество, то не является множеством и образованное из U с помощью конструкции выделения "множество" M, а значит, к нему не применимы дальнейшие рассуждения о множествах, и противоречие исчезает. Однако наивное изложение теории множеств не позволяет строго определить, является ли та или иная совокупность объектов множеством. Таким образом, требуется более строгий подход при определении операций над множествами.

Ниже неформально излагается система аксиом Цермело-Френкеля для формальной теории множеств, предложенная в *1908* г. Э. Цермело и усовершенствованная к *1922* г. А. Френкелем. Хотя за всё время пользования этой аксиоматикой не выявлено ни одного парадокса, её непротиворечивость невозможно доказать внутренними средствами теории множеств (теорема К. Гёделя). Поэтому математики и в настоящее время не могут спать спокойно, ибо почва под их ногами постоянно колышется и даже не видно средств хоть как-то её укрепить.

Неопределяемыми понятиями теории множеств будут *"множество"*, *"элемент"*, двухместный *предикат принадлежности* $\in$ и двухместный предикат *равенства элементов* $=$. Как и при построении всякой математической теории, зафиксируем *алфавит теории множеств,* состоящий из объектных переменных, обозначаемых большими и малыми буквами латинского алфавита, двухместных предикатных символов $\in$ и $=$, логических связок $\wedge$, $\vee$, $\to$, $\leftrightarrow$, $\overline{\bullet}$, кванторов $\forall$, $\exists$ и служебных символов $(\ ,\ )$ – скобок. На этом этапе совокупность всех этих символов не рассматривается как множество, чтобы не возникало замкнутого круга, порочащего создаваемую теорию.

Хотя большие буквы, как правило, обозначают множества, а малые – элементы множеств, строгого разделения в обозначениях на элементы и множества не будет, ибо *a'priori* невозможно сказать, является ли элемент некоторого множества множеством: большие буквы будут использованы для обозначения множеств лишь в случаях, не вызывающих сомнения.

Как и в любой специальной математической теории, вводится понятие *формулы теории множеств* – подмножество "осмысленных" предложений в алфавите. Кроме того, введём следующие общеупотребительные сокращения: $x \notin A$ будет обозначать $\overline{(x \in A)}$, $A \neq B$ будет употребляться вместо $\overline{(A = B)}$, формулы $(\forall x \in A\ \Phi(x))$ и $(\forall x \notin A\ \Phi(x))$ – вместо $(\forall x\ ((x \in A) \to \Phi(x)))$ и $(\forall x\ (x \notin A \to \Phi(x)))$ соответственно, а $(\exists x \in A\ \Phi(x))$ и $(\exists x \notin A\ \Phi(x))$ – вместо $(\exists x\ ((x \in A) \wedge \Phi(x)))$ и $(\exists x\ (x \notin A \wedge \Phi(x)))$. Запись $(\exists ! x \in A\ P(x))$ является синонимом более длинного выражения $((\exists x \in A\ P(x)) \wedge (\forall y \in A\ (P(y) \to (y = x))))$. В формулах теории множеств будем для краткости опускать внешние скобки, которые не несут информации.

Теперь рассмотрим аксиомы теории множеств.

1⁰. аксиома объёмности : $\forall A, B\ ((A = B) \leftrightarrow (\forall x\ (x \in A \leftrightarrow x \in B)))$

Эта аксиома говорит о том, что два множества равны тогда и только тогда, когда они имеют одинаковые элементы. В наивной теории множеств именно так определялось равенство двух множеств.

2⁰. аксиома равенства : $\forall a, A, b\ ((a = b \wedge a \in A) \to b \in A)$

Эта аксиома согласовывает понятия равенства элементов с предикатом принадлежности: было бы странным, если бы равные элементы отличались бы принадлежностью к какому-нибудь множеству. Наивная теория множеств на такие "мелочи" внимания не обращает.

Назовём множество B *подмножеством множества* A, если $\forall x\ (x \in B \to x \in A)$. В этом случае будем говорить также, что A *содержит* B *(*A *включает* B *или* A *– надмножество* B*)* и писать $B \subseteq A$. Ясно, что $\forall A, B\ ((A = B) \leftrightarrow ((A \subseteq B) \wedge (B \subseteq A))$. Для двух множеств X, Y будем писать коротко $X \subset Y$, если $(X \subseteq Y \wedge X \neq Y)$.

3⁰. аксиома выделения : $\forall A\ (\exists B\ (\forall x\ (x \in B \leftrightarrow (x \in A \wedge P(x)))))$, *где* $P(x)$ *– произвольная формула теории множеств со свободной переменной* x, *в которую не входят предметные переменные* A *и* B.

Заметим, что при фиксированных значениях свободных переменных в формуле $P(x)$ множество B определено однозначно: если C – другое множество, удовлетворяющее ***3⁰***, то $\forall x\ (x \in B \leftrightarrow (x \in A \wedge P(x)))$ и $\forall x\ (x \in C \leftrightarrow (x \in A \wedge P(x)))$, так что $\forall x\ ((x \in B) \leftrightarrow (x \in C))$, т.е. $B = C$ по аксиоме объёмности. Множество B будет в дальнейшем обозначаться через $\{x \in A \mid P(x)\}$. Ограничение, накладываемое на формулу $P(x)$ существенно ограничивает возможности принципа выделения.

Из аксиомы выделения следует, в частности, существование множества, не имеющего элементов, которое называется *пустым* множеством, и будет обозначаться символом $\varnothing$. Его можно задать, например, так: $\varnothing = \{x \in A \mid x \neq x\}$, где A – любое множество. Легко понять, что пустое множество определено однозначно: если E – любое множество без элементов, то $\forall x\ (x \in E \leftrightarrow x \in \varnothing)$ и, по аксиоме объёмности, $E = \varnothing$.

Кроме того, аксиома выделения позволяет построить пересечение и разность двух множеств: $A \cap B = \{x \in A \mid x \in B\}$, $A \setminus B = \{x \in A \mid x \notin B\}$. Следует отметить, что эти

множества корректно определены, если A и B – разные буквы. Если же $A = B$, то дополнительно нужно положить $A \cap A = A$, $A \setminus A = \varnothing$. Аксиома выделения не позволяет образовать объединение двух множеств $A \cup B = \{x \in ? \mid x \in A \vee x \in B\}$, т.к. не известно, из какого множества нужно брать элементы объединения. В то же время, если $A \subseteq C$, $B \subseteq C$ для некоторого множества C, то по аксиоме выделения уже можно создать объединение $A \cup B = \{x \in C \mid x \in A \vee x \in B\}$.

4⁰. аксиома существования булеана (множества всех подмножеств) :

$$\forall A\ (\exists B\ (\forall X\ (X \in B \leftrightarrow X \subseteq A)))$$

Введённое множество B будем в дальнейшем обозначать через $\mathcal{B}(A)$ и называться *булеаном множества* A или *множеством всех подмножеств множества* A. Проверьте самостоятельно, что булеан определён однозначно.

5⁰. аксиома (неупорядоченной) пары :

$$\forall a, b\ (\exists A\ (\forall x\ (x \in A \leftrightarrow (x = a \vee x = b))))$$

Содержательно здесь говорится о возможности образовывать множество $A = \{a, b\}$, состоящее из любых объектов a, b. Построенное множество тоже определено однозначно (?!). Оно не обязательно двухэлементно: если $a = b$, то $\{a, b\}$ содержит один элемент, и в этом случае будет обозначаться просто через $\{a\}$.

Эта аксиома позволяет ввести понятие *упорядоченной пары* – математического объекта $(a; b)$, удовлетворяющего следующему свойству упорядоченной пары $\forall a, b, c, d\ (((a; b) = (c; d)) \rightarrow ((a = b) \wedge (c = d)))$. Именно, назовём *упорядоченной парой объектов* a *и* b множество $(a; b) = \{\{a\}, \{a, b\}\}$, существование которого гарантируется аксиомой (неупорядоченной) пары. Проверим, что при этом выполняется свойство упорядоченной пары. В самом деле, согласно аксиомам объёмности и неупорядоченной пары, если $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, то возможны следующие случаи:

1) $\{a\} = \{c\}$. Тогда $a = c$. Если при этом $\{a, b\} = \{c, d\}$, то $\{a, b\} = \{a, d\}$ и $b = d$ (возможно, $b = a = d$). Если же $\{a, b\} = \{c\}$, то $a = c = b$ и $\{a\} = \{a, b\} = \{c, d\}$, т.е. $\{a, d\} = \{a\}$, и последнее равенство опять даёт $b = a = d$, что и требовалось.
2) $\{a\} \neq \{c\}$, т.е. $a \neq c$. Тогда $\{a\} = \{c, d\}$, что невозможно, т.к. $c \notin \{a\}$.

Итак, определено понятие упорядоченной пары, которое не задаёт объект "упорядоченная пара" однозначно: например, множество $\{\{\{a\}, \{a, b\}\}\}$ тоже удовлетворяет свойству упорядоченной пары. Проверьте это и придумайте другие упорядоченные пары. Всюду далее обозначение $(a; b)$ будет означать, что $(a, b) = \{\{a\}, \{a, b\}\}$.

6⁰. аксиома объединения : $\forall A\ (\exists U\ (\forall x\ (x \in U \leftrightarrow (\exists C\ (C \in A \wedge x \in C)))))$

Множество U состоит из всех элементов, принадлежащих хотя бы одному множеству, являющемуся элементом множества A.

Эта аксиома значительно сильнее, чем утверждение о существовании объединения двух множеств: она постулирует существование объединения U всех множеств, входящих в качестве элементов в заданное множество A. Построенное множество U оп-

ределено однозначно (?!), называется *объединением по* A и обозначается через $\cup\{C \in A\}$ или $\bigcup_{C \in A} C$.

Теперь с помощью аксиомы выделения можно определить для множества A и *пересечение по* A, полагая $\cap\{C \in A\} = \{x \in \cup\{C \in A\} \mid \forall\, C \in A \;\; x \in C\}$. Это множество состоит из всех элементов, принадлежащих одновременно всем множествам, являющимся элементами множества A и обозначается также через $\bigcap_{C \in A} C$.

Упражнение. Чему равно объединение и пересечение по пустому множеству ?

Как теперь построить объединение двух множеств A и B ? Рассмотрим неупорядоченную пару $P = \{A, B\}$ и применим к ней аксиому объединения. Тогда множество $\cup\{C \in P\}$ и будет объединением множеств A и B, которое в дальнейшем будет обозначаться просто через $A \cup B$: по аксиоме объединения $\forall\, x \;\; ((x \in \cup\{C \in \{A, B\}\}) \leftrightarrow$ $\leftrightarrow (x \in A \vee x \in B))$, что и требовалось.

С помощью конструкций пересечения и объединения двух множеств можно построить пересечение и объединение любого конечного числа множеств:

$$A_1 \cap \ldots \cap A_n = ((\ldots(A_1 \cap A_2) \cap \ldots) \cap A_{n-1}) \cap A_n ,$$
$$A_1 \cup \ldots \cup A_n = ((\ldots(A_1 \cup A_2) \cup \ldots) \cup A_{n-1}) \cup A_n .$$

Если теперь $a_1 , \ldots , a_n$ – произвольные элементы, то по аксиоме пары, существуют множества $\{a_1\}, \ldots , \{a_n\}$, объединение которых, даёт *конечное* множество $\{a_1 , \ldots , a_n\}$.

Если A и B – множества, $a \in A$, $b \in B$, то можно спросить – какому множеству принадлежит упорядоченная пара $(a; b) = \{\{a\}, \{a, b\}\}$? Ясно, что $\{a\} \in \mathcal{B}(A \cup B)$, $\{a, b\} \in \mathcal{B}(A \cup B)$, поэтому $(a; b) \in \mathcal{B}(\mathcal{B}(A \cup B))$. Теперь можно применить аксиому выделения, чтобы построить *декартово произведение*

$$A \times B = \{x \in \mathcal{B}(\mathcal{B}(A \cup B)) \mid (\exists\, a\, (\exists\, b\, (a \in A \wedge b \in B \wedge x = (a; b))))\} .$$

Так как упорядоченная пара существует для любых объектов, то $A \times B = \varnothing$ тогда и только тогда, когда $A = \varnothing$ или $B = \varnothing$.

Упражнение. Докажите следующие свойства декартова произведения:

1) $A \times B \subseteq C \times D$ тогда и только тогда, когда $A \subseteq C$ и $B \subseteq D$,
2) $A \times B = C \times D$ тогда и только тогда, когда $A = C$ и $B = D$,
3) $A \times (B \times C) = (A \times B) \times C$ тогда и только тогда, когда $A = C = \varnothing$.

7⁰. аксиома регулярности : $\forall\, A \neq \varnothing\; (\exists\, B \in A \;\; (\forall a \in A \;\; a \notin B))$

Содержательно эта аксиома говорит о том, в любом непустом множестве A существует элемент $B \in A$, не содержащий никаких элементов из A.

Важное следствие этой аксиомы заключается в том, что не существует множеств A, B со свойством $A \in B \in A$: если бы нашлись такие множества, то множество-пара $\{A, B\}$ не удовлетворяла бы аксиоме регулярности, т.к. любой из его элементов содержит хотя бы один элемент множества $\{A, B\}$, т.к. A содержит B, а B содержит A.

В частности, не существует множества, содержащего себя в качестве элемента, ибо если $A \in A$, то $A \in A \in A$, вопреки доказанному. Это ставит вне закона "множество всех множеств", ибо такой объект должен содержать как элемент сам себя.

Кроме того, аксиома регулярности позволяет решать и некоторые другие вопросы. Например, с её помощью можно доказать, что равенство $a = (a; b)$ невозможно: если допустить, что $a = (a; b) = \{\{a\}, \{a, b\}\}$, то $a \in \{a\} \in a$, что невозможно.

Упражнения: 1. Докажите, что объект $\{a, \{a, b\}\}$ также удовлетворяет свойству упорядоченной пары.

2. Докажите, что не существует множеств A, B, C со свойством $A \in B \in C \in A$.

3. Обобщите предыдущее упражнение на случай произвольного числа множеств.

Введём теперь понятие *функции* $f : ? \to ?$ *с неопределёнными областями определения и значений*, понимая под этим любое множество f, удовлетворяющее следующему *обобщённому условию функциональности*:

$$(\forall\, x \in f\ (\exists\, u, v\ \ x = (u; v))) \wedge (\forall\, u, v, w\ \ ((u; v) \in f \wedge (u; w) \in f) \to v = w).$$

При этом если $(u; v) \in f$, то будем кратко писать $f(u) = v$ и называть v *значением функции* f *на элементе* u.

Следует отметить, что для функции f с неопределёнными областями определения и значений нельзя применить аксиому выделения для построения области её определения и множества значений. Например, пытаясь задать $Im(f) = \{ b \in ? \mid \exists\ a\ \ (a; b) \in f\}$, невозможно указать из какого множества выбирать значения b. Поэтому необходима специальная аксиома, присваивающая статус множества этому объекту.

8^0. аксиома существования области значений : *для любой формулы* $\Phi(x, y)$ *со свободными переменными* x, y *справедливо свойство*

$$\forall A\ (\forall x \in A\ (\forall y, z\ (\Phi(x, y) \wedge \Phi(x, z) \to y = z))) \to (\exists\ B(\forall y\ (y \in B \leftrightarrow (\exists x \in A\ \Phi(x, y)))))$$

Эта аксиома имеет дело с более широким классом зависимостей, чем обычные функции: она утверждает существование "области значений" $B = Im_A(\Phi)$ для любого функционального на A закона, выражаемого с помощью формулы $\Phi(x, y)$, даже в том случае, если *a'priori* неизвестно, определяет ли Φ функцию на A (ведь пока не ясно, будет ли множеством объект $\{(x; y) \in ? \mid x \in A \wedge \Phi(x, y)\}$).

Теперь можно с полным основанием ввести *области значений и определения функции* f *с неопределёнными областями определения и значений на заданном множестве* A: нужно только заметить, что формула $\Phi(x, y) = ((x; y) \in f)$ функциональна на A, т.е. удовлетворяет посылке аксиомы существования области значений. Значит, определено множество $Im_A(f) = Im_A(\Phi)$, состоящее из всех тех y, для которых найдётся $x \in A$ со свойством $(x; y) \in f$. Поэтому по аксиоме выделения можно ввести *область определения функции* f *на множестве* A – множество $D_A(f) = \{a \in A \mid \exists\ b \in Im_A(f)\ \ (a; b) \in f\}$. Если $D_A(f) = A$, то будем называть функцию f *отображением на* A.

Узаконив функции, можно определить *индексированные элементами одного множества последовательности*: если I – множество, то говорят, что задана *последовательность объектов* a_i, где $i \in I$, если задана функция $a : I \to ?$, где $a_i = a(i)$. Ясно,

что можно рассматривать множество всех членов последовательности, поскольку оно является областью значений функции a: $\{a_i\}_{i\in I} = Im_I(a)$.

Возникает вопрос, зачем нужны функции с неопределёнными областями определения и значений ? Дело в том, что если A и B – два множества, то можно было бы определить понятие *функции из* A *в* B как любое множество f (обычно обозначаемое через $f : A \to B$), удовлетворяющее *свойству функциональности*:

$$(\forall\, x \in f\ (\exists\, u \in A\ (\exists v \in B\ x = (u; v)))) \wedge (\forall\, u \in A\ \forall\, v, w \in B\ ((u; v) \in f \wedge (u; w) \in f)) \to v = w).$$

Для таких функций области значений и определения существуют просто по аксиоме выделения: $Im(f) = \{b \in B \mid \exists\, a \in A\ (a; b) \in f\}$, $D(f) = \{ a \in A \mid \exists\, b \in B\ (a; b) \in f\}$.

Значение аксиомы существования области значений состоит в том, что она даёт средство с помощью формул теории множеств, обладающих свойствами функциональности получать универсальные задания "функций", определённых на всех мыслимых множествах сразу. Действительно, для любой формулы $\Phi(x, y)$ со свойством функциональности можно рассмотреть объект $f = \{(a; b) \in A \times Im_A(\Phi) \mid \Phi(a, b)\}$ являющийся множеством согласно аксиоме выделения. (Это описание не слишком формально. Вставьте в него определение декартова произведения $A \times Im_A(\Phi)$ и сформулируйте строго условие, которому должна удовлетворять формула $\Phi(x, y)$). Таким образом, на каждом множестве A рассматриваемая формула определяет функцию, но задана эта функция сразу для любого мыслимого множества.

Например, можно определить *ординальные числа* или *ординалы* как множества из "область истинности" следующего универсального "предиката"-формулы:

$$Ord(X) = (\forall Y, Z\ ((Z \in Y \wedge Y \in X) \to Z \in X))) \wedge (\forall\, Y, Z \in X\ (Z \in Y \vee Y = Z \vee Y \in Z)).$$

"Предикат" Ord является конъюнкцией двух условий: *транзитивности относительно* $\in$ и *линейной упорядоченности относительно* $\in$.

На самом деле, конечно, говорить о предикате Ord и о его области истинности можно, только ограничив действие Ord на некотором фиксированном множестве A, т.е. для соблюдения формальностей нужно ввести формулу $\Phi(x, y) = (y \in x \wedge Ord(y))$ и воспользоваться аксиомой существования области значений для получения множества $Im_A(\Phi)$ всех ординальных чисел из множества A. Это соответствует описанной выше общей схеме использования аксиомы существования области значений.

9^0. *аксиома бесконечности :* $\exists\, N\ (\varnothing \in N) \wedge (\forall X \in N\ X \cup \{X\} \in N)$

Эта аксиома впервые утверждает существование некоторого множества. До сих пор все конструкции множеств "повисали в воздухе", поскольку не было ясно, существует ли хотя бы одно множество. Интуитивно ясно, что множество N должно быть бесконечным, т.к. оно содержит попарно различные элементы $n_0 = \varnothing$, $n_1 = \varnothing \cup \{\varnothing\}$, $n_2 = \varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}$, и.т.д.

Упражнение. Упростите вид элементов $n_1, n_2, n_3, \ldots, n_i, \ldots$ и докажите, что все они попарно различны.

Говорят, что два множества X и Y *равномощны*, если существует *биективное* отображение (*биекция*) X на Y, т.е. такая функция $f: X \to Y$, для которой $D(f) = X$, $Im(f) = Y$ и выполнено *условие инъективности* $\forall a, b \in X \ (f(a) = f(b) \to a = b)$. В этом случае пишут кратко $X \approx Y$.

Примеры: 1. $\boldsymbol{Z \approx 2 \cdot Z \approx N}$.

Здесь, как обычно, $\boldsymbol{2 \cdot Z} = \{x \in \boldsymbol{Z} \mid \exists\ z \in \boldsymbol{Z}\ \ x = 2 \cdot z\}$. Можно взять следующие отображения $f : \boldsymbol{Z} \to \boldsymbol{2 \cdot Z}$, где $f(z) = 2 \cdot z$, $\varphi : \boldsymbol{N} \to \boldsymbol{Z}$, где $\varphi(n) = \begin{cases} k, \text{ если } n = 2 \cdot k \\ 0, \text{ если } n = 1 \\ k, \text{ если } n = 2 \cdot k + 1 \ (k \geq 1) \end{cases}$.

Легко понять, что f и φ – биекции, и воспользоваться следующим примером.

2. $A \approx A$; если $A \approx B$, то $B \approx A$; если $A \approx B$ и $B \approx C$, то $A \approx C$. Эти три свойства – *рефлексивность*, *симметричность* и *транзитивность* отношения равномощности.

Достаточно рассмотреть биекции $id_A : A \to A$ – тождественное отображение множества A, $f^{-1} : B \to A$, где $f : A \to B$ – биекция, и $g \circ f : A \to C$, где $f : A \to B$ и $g : B \to C$ – биекции.

Эти примеры неформальны, т.к. множества натуральных чисел $\boldsymbol{N}$, как и множества $\boldsymbol{Z}$ целых чисел и $\boldsymbol{Q}$ рациональных чисел ещё не построены.

Формализуем теперь понятия *конечного* и *бесконечного* множеств. Множество A называется *бесконечным*, если оно равномощно некоторому своему собственному подмножеству, и *конечным*, если оно не является бесконечным. Эти определения можно записать формально в несколько этапов:

$$(A - \textit{бесконечно}) \equiv (\exists\ B\ \varnothing \neq B \neq A) \wedge (\exists\ f : A \to B - \underline{\textit{би}}),$$

$$(\exists\ B\ \varnothing \neq B \neq A) \equiv (\exists\ B\ (\exists\ b \in B) \wedge (\exists\ a \in A\ \ a \notin B)),$$

$$(\exists\ f : A \to B - \underline{\textit{би}}) \equiv (\exists\ f : A \to B - \textit{функция}) \wedge (D(f) = A) \wedge (Im(f) = B) \wedge (f - \underline{\textit{инъ}}),$$

$$(\exists\ f : A \to B - \textit{функция}) \equiv (\exists\ f\ (\forall\ u \in f\ (\exists\ a \in A\ (\exists\ b \in B\ u = (a; b))))) \wedge (f - \textit{функционально}),$$

$$(f - \textit{функционально}) \equiv (\forall\ a \in A\ (\forall\ b, c \in B\ (((a; b) \in f \wedge (a; c) \in f) \to b = c))),$$

$$(D(f) = A) \equiv (\forall\ a \in A\ (\exists\ b \in B\ (a; b) \in f)),$$

$$(Im(f) = B) \equiv (\forall\ b \in B\ (\exists\ a \in A\ (a; b) \in f)),$$

$$(f - \underline{\textit{инъ}}) \equiv (\forall\ x, y \in A\ (\exists\ z \in B\ ((x; z) \in f \wedge (y; z) \in f) \to x = y)).$$

Условие бесконечности множества A можно теперь записать в виде формулы, последовательно подставив все приведённые фрагменты в самую первую из квазиформул. Взяв отрицание этой формулы, получим в виде формулы условие конечности множества A.

Упражнение. Совпадает ли введённое новое понятие конечного множества с прежним понятием конечного множества $\{a_1, \ldots, a_n\}$?

Теперь можно выделить "натуральные числа" из бесконечного множества N. Для этого запишем квазиформулу, задающую "натуральные числа":

$$Nat(y) = (Ord(y) \wedge (\forall z \in y\ (z = \varnothing \vee (\exists\ t\ \ z = t \cup \{t\}))) \wedge (y - \textit{конечно}))$$

и снова воспользуемся аксиомой существования области значений для формулы $\Phi(x, y) = (y \in x \wedge Nat(y))$, чтобы получить множество $\boldsymbol{N}$ всех "натуральных чисел", принадлежащих бесконечному множеству N. При этом элементы $\varnothing$, $\varnothing \cup \{\varnothing\}$, $\varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}$, … множества $\boldsymbol{N}$ в дальнейшем обозначаем через $1, 2, 3, \ldots$, отождествляя их с "обычными" натуральными числами.

Упражнения. 1. Докажите, что для любого конечного множества A и произвольного объекта b множество $A \cup \{b\}$ конечно. Выведите отсюда, что для любого $n \in \boldsymbol{N}$ множество $\{a_1, \ldots, a_n\}$ конечно.

3. Докажите бесконечность построенного множества $\boldsymbol{N}$.

4. Докажите, что множество, содержащее бесконечное подмножество, само бесконечно.

5. Докажите, что $\boldsymbol{N}$, $\boldsymbol{Z}$ и $\boldsymbol{Q}$ равномощны, как равномощны $\boldsymbol{R}$ и $\boldsymbol{R} \times \boldsymbol{R}$.

6. Проверьте условие функциональности для $\Phi(x,y) = y \in x \wedge Nat(y)$.

7. Докажите, что множество $\boldsymbol{N} = \{n \in N \mid Nat(n)\}$ является ординалом и что это – первый бесконечный ординал (обозначаемый обычно через ω), в котором содержатся все конечные ординалы $\varnothing$, $\varnothing \cup \{\varnothing\}$, $\varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}$, … .

Может возникнуть резонный вопрос: откуда такие определения конечных и бесконечных множеств ? Докажем неформально следующую теорему:

Теорема (об эквивалентных понятиях конечности (бесконечности) множеств). *Следующие условия эквивалентны:*

(1) либо $A = \varnothing$, *либо* $A = \{a_1, \ldots, a_n\}$,

(2) A *не содержит последовательности* $\{x_i\}_{i \in \boldsymbol{N}}$ *со свойством* $x_i \neq x_j$ *при* $i \neq j$,

(3) A *конечно.*

Эквивалентны и следующие условия:

(1′) $A \neq \varnothing$ *и не представимо в виде* $A = \{a_1, \ldots, a_n\}$,

(2′) A *содержит последовательность* $\{x_i\}_{i \in \boldsymbol{N}}$ *со свойством* $x_i \neq x_j$ *при* $i \neq j$,

(3′) A *бесконечно.*

Доказательство. Прежде всего, отметим, что если множество A бесконечно, т.е. существует биекция $f : A \to B$ на собственное подмножество $\varnothing \neq B \neq A$, то множество B тоже бесконечно. Действительно, отображение f можно рассматривать как отображение на свой образ: $f : B \to f(B) = \{c \in B \mid \exists\, b \in B \;\; c = f(b)\}$. Проверим, что $f(B)$ – собственное подмножество в B. Ясно, что $\varnothing \neq f(B) \subseteq B$. Если $f(B) = B$ и $a \in A \setminus B$, то $f(a) \in B$ и найдётся $b \in B$ со свойством $f(b) = f(a)$, откуда ввиду инъективности f получим $a = b \in B$, что невозможно.

(1) $\Rightarrow$ *(2)* Для $A = \varnothing$ утверждение *(2)* очевидно. Если $A = \{a_1, \ldots, a_n\}$, то $\forall\, x \in A \;\; (x = a_1) \vee (x = a_2) \vee \ldots \vee (x = a_n)$. Поэтому существование последовательности $\{x_i\}_{i \in \boldsymbol{N}}$ со свойством $x_i \neq x_j$ при $i \neq j$ приводит к противоречию: среди первых её n членов содержатся все элементы множества A.

(2) $\Rightarrow$ *(3)* Пусть A не содержит последовательности элементов $\{x_i\}_{i \in \boldsymbol{N}}$ со свойством $x_i \neq x_j$ при $i \neq j$. Если A не конечно, то оно бесконечно, т.е. равномощно своему

собственному подмножеству B. Приведём это предположение к противоречию. В частности, $A \neq \varnothing$, т.к. $\varnothing \neq A \setminus B \subseteq A$. Выберем элемент $x_1 \in A$. Предположим, что уже построено множество $\{x_1, \dots, x_k\}$ попарно различных элементов множества A.

Если $A \neq \{x_1, \dots, x_k\}$, то в непустом множестве $A \setminus \{x_1, \dots, x_k\}$ можно выбрать элемент x_{k+1}, который не совпадает ни с одним из элементов $x_1, \dots, x_k$, и получить новое множество $\{x_1, \dots, x_k, x_{k+1}\}$ попарно различных элементов. Если эта процедура продолжится сколь угодно долго, то ***будет построена последовательность $\{x_i\}_{i \in N}$ попарно различных элементов***, вопреки *(2)*.

Значит, на некотором шаге, получим $A = \{x_1, \dots, x_k\}$. Проверим, что это множество конечно, вопреки допущению о бесконечности множества A. Если существует биекция $f : \{x_1, \dots, x_k\} \to B$ на некоторое собственное подмножество $B \subset \{x_1, \dots, x_k\}$, то B бесконечно, т.е. $f(B) \subset B$. Поэтому получим убывающую цепь бесконечных множеств: $\{x_1, \dots, x_k\} = A \supset B \supset B_1 = f(B) \supset \dots \supset B_{k-1} = f(B_{k-2}) \supset \dots$, что невозможно, ибо множество B_{k-1} уже будет пустым (на каждом шаге включения строгие).

(3) $\Rightarrow$ *(1)* Пусть $A \neq \varnothing$ и A конечно. Рассуждая аналогично доказательству *(2)* $\Rightarrow$ *(3)*, во множестве A построим последовательность элементов $X = \{x_i\}_{i \in N}$ со свойством $x_i \neq x_j$ при $i \neq j$. Зададим функцию $f : A \to A \setminus \{x_1\}$ следующим образом: $f(a) = \begin{cases} a, \text{ если } a \notin X \\ x_{i+1}, \text{ если } a = x_i \end{cases}$. Нетрудно проверить, что это отображение биективно, вопреки конечности множества A.

Эквивалентности *(1')* $\Leftrightarrow$ *(2')* $\Leftrightarrow$ *(3')* доказываются аналогично. Теорема доказана.

10^0. аксиома выбора : $\forall X\ ((\forall Y \in X\ Y \neq \varnothing) \to (\exists M\ (\forall Y \in X\ (\exists!\ m \in M \cap Y))))$

Посылка этой аксиомы говорит о том, что множество X состоит из непустых множеств, а заключение утверждает, что в каждом из этих множеств можно выбрать по одному представителю и образовать из них некоторое множество M.

Центр тяжести здесь не в утверждении о возможности выбора в каждом множестве $Y \in X$ одного элемента (это очевидно, т.к. $Y \neq \varnothing$), а в том, что выбранные элементы образуют множество. Таким образом, аксиома выбора является ещё одним средством конструирования множеств.

Эта аксиома эквивалентна (при выполнении предыдущих аксиом теории множеств) следующему утверждению: для любого множества X, состоящего из непустых множеств, существует функция $f : X \to \cup\{Y \in X\}$ со свойством $\forall Y \in X\ f(Y) \in Y$, называемая *функцией выбора*. В самом деле, если верна аксиома выбора, то для построения искомой функции достаточно положить $f = \{(Y; m) \in X \times M \mid m \in M \cap Y\}$ по аксиоме выделения и убедиться в выполнении условия функциональности для f. Обратное утверждение тоже доказывается просто: если есть функция выбора, то в качестве M достаточно взять её образ $Im(f)$.

Отметим ещё, что условие $(\forall Y \in X\ Y \neq \varnothing)$ аксиомы выбора выполнены для множества $X = \mathcal{B}(A) \setminus \varnothing$ для любого непустого множества A. Таким образом, из аксиомы выбора следует утверждение $\forall A \neq \varnothing\ (\exists M\ (\forall Y \in \mathcal{B}(A) \setminus \varnothing\ (\exists!\ m \in M \cap Y)))$, обеспечивающее существование множества представителей непустых элементов булеана.

Оказывается, что это утверждение эквивалентно аксиоме выбора. Действительно, если задано множество X из непустых подмножеств, то его элементы будут элементами множества $\mathcal{B}(\cup\{Y \in X\}) \setminus \varnothing$, так что существует такое множество представителей M, что $\forall Y \in \mathcal{B}(\cup\{Y \in X\}) \setminus \varnothing \;\; (\exists !\;\; m \in M \cap Y)$. В частности, это условие выполнено и для любого $Y \in X$.

Рассматриваемая аксиома очевидна, когда все, участвующие в ней множества конечны, она может быть доказана для любого конечного множества X, но в общем случае высказанное в ней утверждение далеко неочевидно. Чтобы прояснить ситуацию (а может быть, окончательно запутать ?), представим, что Дед Мороз решил пересчитать подарки в своём мешке. Как он должен поступить ? Вытаскивать кульки по одному из мешка и, считая, отдавать их Снегурочке, пока мешок не опустеет. Предположим теперь, что Снегурочка, не желая ненароком рассыпать кульки, возвращает каждый кулёк обратно Деду Морозу, привязывая к нему бантик. Тогда Дед Мороз тоже сможет пересчитать подарки, ощупывая каждый вытаскиваемый кулёк, чтобы дважды не вытащить один и тот же, до тех пор, пока в мешке не останутся только кульки с бантиками. Наконец, предположим, что выключился свет, а Снегурочка не умеет завязывать бантики в темноте. Тогда Дед Мороз не сможет пересчитать свои подарки. Аналогичная ситуация и в теории множеств: мешок Деда Мороза – это множество X, подарки – его элементы $Y \in X$, а роль Снегурочки исполняет функция выбора, которая "привязывает" к каждому подарку Y бантик $f(Y) = m \in M \cap Y$. Отличие только в том, что аксиома выбора позволяет математикам и в полной темноте пересчитать подарки Деда Мороза. В этом и её неочевидность, ибо Деду Морозу невозможно объяснить – как же всё-таки осуществлять выбор подарков в темноте… Этот пример показывает также тесную связь между процессами выбора и упорядочивания: пересчёт ведёт к упорядочиванию. Как покажет приведённая ниже теорема, связь эта глубока и далеко не случайна.

Аксиома выбора многократно использовалась математиками неявно, пока Э. Цермело не придал ей точную формулировку. Кстати, доказательство предыдущей теоремы тоже опирается на аксиому выбора: выделенная жирным фраза в её доказательстве не может быть обоснована без аксиомы выбора. В ней говорится, что если для каждого натурального n построены функции $f_i : \{1, \dots, n\} \to A$, определяющие члены последовательности $x_1, \dots, x_i$ (и поэтому удовлетворяющие свойствам $f_i(k) = x_k \;\; (1 \le k \le i)$ при любом $i \in \mathbf{N}$), то существует и функция $f : \mathbf{N} \to A$, определяющая сразу всю последовательность $\{x_i\}_{i \in \mathbf{N}}$, т.е. $f(n) = x_n$ при любом $n \in \mathbf{N}$. Строгое доказательство этого факта требует использования аксиомы выбора.

Обсуждение последовавших вслед за явлением миру аксиомы выбора жарких математических дискуссий оставим без комментариев, а пока для иллюстрации приведём несколько эквивалентных формулировок этой аксиомы, напомнив предварительно некоторые понятия, связанные с отношениями порядка на множествах.

Пусть A – непустое множество. Говорят, что ρ *– бинарное отношение на* A, если ρ – непустое подмножество в $A \times A$. При этом для упорядоченной пары $(a; b)$ вместо $(a; b) \in \rho$ пишут просто $a \rho b$.

Бинарное отношение $\preceq$ на множестве A называется *частичным порядком на* A, если это отношение удовлетворяет трём условиям: *1) рефлексивность* $\forall a \in A \;\; a \preceq a$, *2) антисимметричность* $\forall a, b \in A \;\; a \preceq b \wedge b \preceq a \to a = b$ и *3) транзитивность* $\forall a, b, c \in A \;\; a \preceq b \wedge b \preceq c \to a \preceq c$. Частичный порядок $\preceq$ называется *линейным*, если $\forall a, b \in A \; (a \preceq b) \vee (b \preceq a)$. *Частично упорядоченное множество (ч.у.м.)* – это упорядоченная пара $(A, \preceq)$, где A – непустое множество, а $\preceq$ – некоторый фиксированный частичный порядок на A. Для произвольного элемента $a \in A$ назовём *начальными отрезками множества* A множества вида $A_a = \{x \in A \mid x \preceq a \wedge x \neq a\}$. Если $(A, \preceq)$ – частично упорядоченное множество, то любое его собственное подмножество $\varnothing \neq M \subseteq A$ можно рассматривать как ч.у.м. $(M, \preceq)$ с тем же отношением порядка $\preceq$, что и в A. Произвольное линейно упорядоченное подмножество $(M, \preceq)$ частично упорядоченного множества $(A, \preceq)$ называется *цепью*.

Если M – подмножество ч.у.м. A, то любой элемент $a \in A$ со свойством $\forall m \in M \; m \preceq a$ называется *верхней гранью множества* M. Элемент $m \in M$ называется *минимальным (соответственно максимальным) элементом множества* M, если $\forall x \in M \; \overline{x < m}$ (соответственно $\forall x \in M \; \overline{x > m}$). Если $\forall x \in M \;\; m \preceq x$ (или $\forall x \in M \;\; x \preceq m$), то элемент $m \in M$ называется *наименьшим (соответственно наибольшим) элементом множества* M. В случае линейного порядка понятия минимального и наименьшего (соответственно максимального и наибольшего) элементов совпадают, но в частично упорядоченном множестве условия $\overline{x < m}$ и $x \geq m$ (как $\overline{x > m}$ и $x \leq m$) не эквивалентны (?!).

Говорят, что линейный порядок $\preceq$ на ч.у.м. $(A, \preceq)$ является *полным порядком*, если любое непустое подмножество $M \subseteq A$ имеет наименьший элемент. Само множество $(A, \preceq)$ при этом называют *вполне упорядоченным (в.у.м.)*. Если на множестве X можно определить некоторое отношение линейного (полного) порядка, то говорят, что *множество* X *можно линейно (соответственно вполне) упорядочить*. Отметим, что любое подмножество B вполне упорядоченного множества $(A, \preceq)$ само вполне упорядочено: действительно, если M – непустое подмножество в B, то оно обладает наименьшим элементом как подмножество в A. Кроме того, для каждого элемента a вполне упорядоченного множества $(A, \preceq)$ однозначно определён *непосредственно следующий за ним (по порядку* $\preceq$*) элемент* $a_+ = \min\{x \in A \mid x > a\}$. В противоположность этому, непосредственно предшествующий элемент определён не всегда: например, во вполне упорядоченном множестве $(\boldsymbol{N} \cup \{+\infty\}, \preceq)$ с естественным порядком $\preceq$ у элемента $+\infty$ нет непосредственно предшествующего.

Примеры: 1. Множества $\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ линейно упорядочены обычным отношением порядка $\leq$. При этом на множестве $\boldsymbol{N}$ этот порядок является полным, а на остальных множествах – нет, т.к. их общее подмножество $\boldsymbol{Z} \subseteq \boldsymbol{Q} \subseteq \boldsymbol{R}$ не обладает минимальным элементом.

2. Для любого множества A бинарное отношение $X \subseteq Y$ является отношением частичного порядка на булеане $\mathcal{B}(A)$. Этот порядок будет линейным только для одноэле-

ментного или пустого множества A. При этом каждая цепь C – это элемент из $\mathcal{B}(\mathcal{B}(A))$, состоящий из элементов $X \in \mathcal{B}(A)$, линейно упорядоченных по включению $\subseteq$. Каждая цепь C имеет верхнюю грань $\cup\{c \in C\}$ в $\mathcal{B}(A)$: $\forall\ c \in C\ \ c \subseteq \cup\{c \in C\}$.

3. Функция $f : A \to B$ является подмножеством булеана $\mathcal{B}(A \times B)$. При этом для функции $g : A \to B$ выполняется включение $f \subseteq g$ тогда и только тогда, когда g – продолжение функции f, т.е. $D(f) \subseteq D(g)$ и $\forall a \in D(f)\ \ g(a) = f(a)$. Поэтому каждая цепь C функций из A в B имеет функцию $\cup\{c \in C\}$ в качестве верхней грани (проверьте, что $\cup\{c \in C\}$ будет функцией, если функцией является каждый элемент $c \in C$).

4. Подмножество $M = \{\{1, 3\}, \{1, 2\}, \{2, 3\}\}$ булеана $(\mathcal{B}(\{1, 2, 3\}), \subseteq)$ не содержит цепей, имеет три минимальных и три максимальных элемента, но ни одного наименьшего и наибольшего. Всё множество $\{1, 2, 3\}$ (и только оно) является верхней гранью M в $\mathcal{B}(\{1, 2, 3\})$.

Доказательство следующей теоремы при первом чтении можно опустить, хотя нужно учесть, что оно богато идеями и стандартными техническими приёмами, часто используемыми при работе с множествами.

Теорема (об эквивалентных формулировках аксиомы выбора). *Следующие условия эквивалентны в системе аксиом Цермело-Френкеля* $\mathbf{1^0\text{-}9^0}$*:*

(1) аксиома выбора: $\forall\ X\ ((\forall Y \in X\ \ Y \neq \varnothing) \to (\exists\ M\ \ (\forall Y \in X\ \ (\exists!\ \ m \in M \cap Y))))$,

(2) существование функции выбора :

$\forall\ X\ ((\forall Y \in X\ \ Y \neq \varnothing)\ \to \exists\ f\colon\ X \to \cup\{Y \in X\} \wedge\ D(f) = X \wedge (\forall Y \in X\ \ f(Y) \in Y))$,

(3) аксиома выбора для разбиений (аксиома Цермело) :

$\forall\ X\ ((\forall Y, Z \in X\ \ Y \neq \varnothing \wedge\ (Y = Z\ \leftrightarrow\ Y \cap Z \neq \varnothing)) \to (\exists\ M\ \ (\forall Y \in X\ \ (\exists!\ \ m \in M \cap Y))))$,

(4) лемма Цорна : частично упорядоченное множество, в котором каждая цепь имеет верхнюю грань, содержит максимальный элемент,

(5) принцип максимальности Куратовского-Хаусдорфа : любая цепь частично упорядоченного множества содержится в некоторой максимальной (по включению) цепи,

(6) теорема Цермело : каждое непустое множество можно вполне упорядочить.

Доказательство. Схема доказательства:

$$\begin{array}{ccccccc} (1) & \Leftarrow & (3) & \Leftarrow & (4) & \Leftarrow & (6) \\ \| & & \Uparrow & & \| & & \Uparrow \\ (1) & \Rightarrow & (2) & \Rightarrow & (4) & \Leftrightarrow & (5) \end{array}$$

Приведённая схема избыточна. Это сделано специально – чтобы предоставить возможность заинтересованным читателям познакомиться с разнообразными идеями, методами и нетривиальными математическими рассуждениями в несхожих ситуациях.

Импликация $(1) \Rightarrow (2)$ уже была доказана выше.

$(2) \Rightarrow (3)$ Пусть множество X состоит из непустых непересекающихся множеств. Тогда условие (2) гарантирует существование всюду определённой на X функции выбора $f\colon X \to \cup\{Y \in X\}$ со свойством $\forall\ Y \in X\ \ \ f(Y) \in Y$. Поэтому, если положить $M = Im(f)$, то $\forall\ Y \in X\ \ \ m = f(Y) \in M \cap Y$, причём элемент m единственен, т.к. если $n = f(Z) \in M \cap Y$ при $Z \neq Y$, то $f(Z) \in M \cap Y \cap Z = \varnothing$ – противоречие.

(3) $\Rightarrow$ *(1)* Пусть утверждение аксиомы выбора выполнено для множеств, состоящих из непустых непересекающихся множеств. Тогда оно выполнено и в общем случае.

Пусть X – множество, состоящее из непустых множеств. Образуем, по аксиоме выделения новое множество $\overline{X} = \{Y \times \{Y\} \in X \times \mathcal{B}(X) \mid Y \in X\}$. Тогда $\overline{X}$ состоит из непустых непересекающихся множеств: если $x \in Y \times \{Y\} \cap Z \times \{Z\}$, то $x = (y; \{Y\}) = (z; \{Z\})$, и по свойству упорядоченной пары, $y = z$ и $\{Y\} = \{Z\}$, откуда следует, что $Y = Z$. Условие *(3)* позволяет найти множество $\overline{M}$ со свойством $\forall\, \overline{Y} = Y \times \{Y\} \in \overline{X}\ \ (\exists!\ \overline{m} \in \overline{M} \cap \overline{Y})$. Положим $f = \{(Y; y) \in X \times (\cup \{Y \in X\}) \mid (y; Y) \in \overline{M} \cap (Y \times \{Y\})\}$. Это множество (по аксиоме выделения) будет функцией выбора на X. Действительно, очевидно, что $f \neq \varnothing$ (т.к. $\forall\, Y \in X\ \ \overline{M} \cap (Y \times \{Y\}) \neq \varnothing$), и f удовлетворяет условию функциональности: если $(Y; y),\ (Y; z) \in f$, то $(y; Y),\ (z; Y) \in \overline{M} \cap (Y \times \{Y\})$, значит $(y; Y) = (z; Y)$ и $y = z$, что и требовалось.

Таким образом, доказана эквивалентность условий *(1), (2), (3)* теоремы.

(2) $\Rightarrow$ *(4)* Пусть $(A, \leq)$ – ч.у.м., в котором каждая цепь имеет верхнюю грань. Рассмотрим множество всех цепей $L = \{S \in \mathcal{B}(A) \mid (S, \leq) – цепь\}$. Чтобы убедиться, что это – множество, нужно воспользоваться аксиомой выделения, предварительно записав условие линейной упорядоченности множества $(S, \leq)$ в виде формулы (?!). Множество L непусто, т.к. содержит одноэлементные цепи. По условию, любая цепь имеет верхнюю грань, т.е. $\forall\, S \in L\ \ B(S) = \{b \in A \mid \forall\, s \in S\ \ b \geq s\} \neq \varnothing$. Если в A нет максимального элемента, то $\forall\, S \in L\ \ B(S) \setminus S \neq \varnothing$: если $B(S) = S$, то в S есть максимальный элемент b, не максимальный в A, т.е. $\exists\, c \in A\ \ c > b$, а значит, $c \in B(S) \setminus S$ – противоречие.

Далее, рассуждая неформально, можно было бы просто сказать: “Рассмотрим семейство непустых множеств $\{ B(S) \setminus S \mid S \in L\}$ и выберем в каждом из них по одному элементу. Тем самым произвольному $S \in L$ однозначно сопоставляется элемент $t \in B(S) \setminus S$, т.е. определена такая функция $f : L \to A$, что $\forall\, S \in L\ \ \forall\, s \in S\ \ f(S) > s$, т.е. $\forall\, S \in L\ \ f(S) > S$”.

Формализация этих рассуждений такова. Рассмотрим (по аксиоме выделения) множество $g = \{(S; M) \in L \times \mathcal{B}(A) \mid M = \{b \in A \mid \forall\, s \in S\ \ b \geq s\} \setminus S\}$, являющееся на самом деле функцией $g : L \to \mathcal{B}(A)$ (проверьте функциональность !). Образ этой функции $Im(g) = \{M \in \mathcal{B}(A) \mid \exists\, S \in L\ \ M = B(S) \setminus S\}$ – множество, состоящее из непустых множеств, так что по *(2)* существует функция выбора $h : Im(g) \to \cup \{M \in Im(g)\} \subseteq A$ со свойством $\forall\, M \in Im(g)\ \ h(M) \in M$. Тогда композиция $f = h \circ g : L \to Im(g) \to A$ функций g и h – искомая: $\forall\, S \in L\ \ g(S) = B(S) \setminus S$, $f(S) = h(B(S) \setminus S) \in B(S) \setminus S > S$.

Для произвольной цепи $S \in L$ элемент $Y \in L$ назовём *начальным сегментом цепи* S, если $(Y \subseteq S) \wedge (\forall\, z \in S \setminus Y\ \ z > Y)$. В этом случае коротко будем писать Y *– н.с.* S. Теперь для любого фиксированного элемента $a \in A$ рассмотрим множество цепей

$$K_a = \{X \in L \mid (\{a\} – н.с.\ X) \wedge (\forall\, Y\ \ (Y – н.с.\ X) \wedge (Y \neq X) \to (f(Y) = inf_X(X \setminus Y)))\}.$$

Здесь через $inf_Q(P)$ для $P \subseteq Q$ обозначена точная нижняя грань множества P в Q, т.е. такой элемент $q \in Q$, что $(q \le P) \wedge (\forall\ t \in Q\ \ (t > q) \to (\exists\ p \in P\ \ p < t))$.

Множество K непусто, т.к. одноэлементная цепь $\{a\}$ принадлежат K: у неё нет собственных начальных сегментов, так что импликация в определении множества K будет истинна. Докажем, что множество K_a линейно упорядочено по включению, т.е. $\forall\ Z, T \in K\ \ (Z \subseteq T) \vee (T \subseteq Z)$. Действительно, цепи Z, T имеют общий начальный сегмент $\{a\}$. Пусть C – объединение всех общих начальных сегментов цепей Z и T. Тогда C – максимальный по включению общий начальный сегмент цепей Z и T, и если $C \ne Z$, $C \ne T$, то $inf_T(T \setminus C) = f(C) = inf_Z(Z \setminus C)$. Это значит, что $D = C \cup \{f(C)\}$ – тоже общий начальный сегмент Z и T, причём $f(C) \notin C$, т.е. $C \ne D$ – противоречие с максимальностью C.

Таким образом, множество K_a линейно упорядочено по включению, и можно рассмотреть цепь $O = \cup\{X \in K_a\}$ – наибольшую по включению цепь в K_a. Снова получается противоречие, т.к. $O \cup \{f(O)\} \in K_a$, источник которого – предположение об отсутствии максимальных элементов в A. Значит максимальные элементы в A есть.

(4) $\Rightarrow$ (5). Пусть $(A, \le)$ – ч.у.м., и C – цепь в A. Рассмотрим множество всех цепей $L = \{S \in \mathcal{B}(A) \mid\ C \subseteq S \wedge (S, \le) – цепь\}$, содержащих C. На множестве L можно рассмотреть частичный порядок $\subseteq$ – включение цепей, получив ч.у.м. $(L, \subseteq)$. Каждая цепь этого множества имеет верхнюю грань: если M – линейно упорядоченное по включению множество элементов из L, то $\cup\{X \in M\} \in L$ – верхняя грань цепи M. Значит, по *(4)*, в $(L, \subseteq)$ есть максимальный по включению элемент, который и будет максимальной цепью, содержащей C.

(5) $\Rightarrow$ (4). Пусть $(A, \le)$ – ч.у.м., каждая цепь которого содержится в некоторой максимальной цепи. Зафиксируем $a \in A$ и рассмотрим цепь $\{a\}$, которая (по *(4)*) содержится в некоторой максимальной цепи C, имеющей, по условию леммы Цорна *(5)*, верхнюю грань $u \in A$. Это значит, что $\forall c \in C\ \ c \le u$, т.е. множество $C \cup \{u\}$ также является цепью. Поскольку цепь C была максимальна, $C = C \cup \{u\}$, $u \in C$ и u – максимальный элемент множества A. Действительно, если $\exists\ x \in A\ \ x > u$, то $x \notin C$ и $C \cup \{x\}$ – строго большая, чем C, цепь, вопреки выбору C.

(5) $\Rightarrow$ (6). Пусть $A \ne \varnothing$. Рассмотрим частично упорядоченное множество O полных порядков относительно включения $\subseteq$:

$$O = \{\rho \subseteq A \times A \mid\ \rho \ne \varnothing \wedge (\rho – полный\ порядок\ на\ D(\rho) = \{a \in A \mid \exists\ x \in A\ \ a\ \rho\ x\})\}$$

(запишите формальное определение для O и убедитесь, что O – действительно множество). Множество O непусто, т.к. для любого $a \in A$ $\rho = \{(a, a)\} \in O$. Кроме того, O удовлетворяет условиям леммы Цорна. В самом деле, если C – цепь в O, то $\cup\{\rho \in C\} \in C$ (проверьте, что это объединение – снова полный порядок на множестве $\cup\{D(\rho) \mid \rho \in O\}$!). Поэтому в O есть максимальный элемент, который обозначим через $\le$. Если $D(\le) = A$, то $\le$ – полный порядок на A. Если же $\exists\ x \notin D(\le)$, то можно расширить порядок $\le$, рассмотрев полный порядок $\le \cup\{(a; x) \in A \times A \mid a \in D(\le)\} \in C$

(в этом порядке элемент x становится наибольшим), что противоречит максимальности $\leq$. Таким образом, $\leq$ – искомый полный порядок на A.

(6) $\Rightarrow$ (4). Ввиду доказанной импликации *(2) $\Rightarrow$ (4)* достаточно обосновать импликацию *(6) $\Rightarrow$ (2).* Пусть дано непустое множество X, состоящее из непустых множеств. Построим функцию выбора $f: X \to \cup\{Y \in X\} = D$. Для этого вполне упорядочим множество D отношением полного порядка $\prec$ и для каждого $Y \in X$ положим $f(Y) = \min_{\prec} Y$ – наименьший элемент множества Y относительно порядка $\prec$. Легко проверить, что это – искомая функция.

Несколько неформальное задание функции f легко сделать более строгим:

$$f = \{(Y; y) \in X \times D \mid \forall\, z \in Y\, (y \prec z) \vee (y = z)\}.$$

Убедитесь, что это равенство определяет функцию $f: X \to \cup\{Y \in X\} = D$, причём $\forall Y \in X\ f(Y) \in Y$ ввиду определения полного порядка $\prec$.

(4) $\Rightarrow$ (3). Пусть задано множество X, состоящее из непустых множеств, и предполагается верной лемма Цорна. Докажем существование множества M со свойством $\forall\ Y \in X\ \ \exists!\ m \in M \cap Y$, которое для краткости будем называть *выборкой*. Для этого рассмотрим множество частичных выборок:

$$L = \{U \in \mathcal{B}(\cup\{Y \in X\}) \mid \forall\ Y \in X\ \ (Y \cap U \neq \varnothing \to \exists!\ u \in Y \cap U)\},$$

образованное по аксиоме выделения. Оно не пусто: $\forall\ Y \in X\ \ \forall\ y \in Y\ \ \{y\} \in L$. Множество L частично упорядочено отношением включения $\subseteq$ и при этом любая цепь C (упорядоченное по включению множество) таких выборок имеет верхнюю грань – именно выборку $\cup\{U \in C\}$ (?!). По лемме Цорна множество L имеет максимальный элемент M. Нужно только проверить, что $\forall\ Y \in X\ \ Y \cap M \neq \varnothing$: если бы $\exists\ \ Y \in X$ $M \cap Y = \varnothing$, то можно было бы расширить цепь C, присоединив к ней частичную выборку $M \cup \{y\}$, где y – некоторый элемент множества Y.

Теорема об эквивалентных формулировках аксиомы выбора полностью доказана.

Упражнения: **1.** Пусть $(A, \leq)$ – линейно упорядоченное множество, M – непустое множество его подмножеств, каждое из которых вполне упорядочено отношением $\leq$. Будет ли $\cup\{X \in M\}$ вполне упорядоченным множеством, если $(M, \subseteq)$ – цепь ?

2. Изменится ли ответ упражнения **1**, если предполагать, что существует $\min M$?

3. Сколькими способами можно частично, линейно или вполне упорядочить конечное множество из n элементов ?

4. Постройте без использования аксиомы выбора и эквивалентных ей утверждений полные порядки на множествах $\boldsymbol{N} \times \boldsymbol{N}$, $\boldsymbol{Z} \times \boldsymbol{Z}$, $\boldsymbol{Q} \times \boldsymbol{Q}$.

5. Докажите, что линейно упорядоченное множество $(A, \leq)$ вполне упорядочено отношением $\leq$ тогда и только тогда, когда не существует бесконечной убывающей цепочки $a_1 > a_2 > \ldots > a_n > \ldots$

6. Проанализировав доказательство импликации *(2) $\Rightarrow$ (4)*, докажите без использования аксиомы выбора следующую лемму Бурбаки: *Пусть $(A, \leq)$ – частично упорядо-*

ченное множество, каждая цепь которого имеет верхнюю грань. Тогда всякое отображение $f: A \to A$ *со свойством* $\forall a \in A \ f(a) \geq a$ *обладает неподвижной точкой, т.е.* $\exists \ x \in A \ f(x) = x$.

Замечание: Оказывается (см. [2, стр. 93]), что аксиома выбора эквивалентна также следующему утверждению: любое бесконечное множество равномощно своему декартовому квадрату, те $A \approx A \times A$.

Аксиома выбора – последняя аксиома в списке Цермело-Френкеля. Так что построение теории множеств на этом завершено. Конечно, невозможно привести и обсудить все теоретико-множественные конструкции, встречающиеся в современной математике. Однако смею надеяться, что некоторое представление об основных деталях, возможностях и правилах использования чудесного конструктора с названием "Теория множеств" для математиков, не желающих расставаться с детскими иллюзиями о первозданной математической строгости, мы всё-таки получили.

В заключение приведём ещё пример использования доказанной теоремы, замечательный тем, что применяя несложные часто встречающиеся в математических рассуждениях построения, он даёт эквивалентную и иногда более удобную для приложений формулировку аксиомы регулярности.

Теорема (эквивалентные формулировки аксиомы регулярности). *Следующие утверждения эквивалентны в системе аксиом* $\mathbf{1^0\text{-}6^0, \ 8^0\text{-}9^0}$*:*

(1) аксиома регулярности : $\forall A \neq \varnothing \ \exists B \in A \ \forall a \in A \ a \notin B$ *(т.е.* $A \cap B = \varnothing$*),*

(2) принцип отсутствия бесконечных убывающих (по отношению $\in$*) цепей множеств: не существует бесконечной последовательности* $\{A_i\}_{i \in N}$ *множеств, удовлетворяющей условию* $\forall i \in \mathbf{N} \ A_{i+1} \in A_i$ *(т.е.* $A_1 \ni A_2 \ni A_3 \ni \ldots \ni A_i \ni \ldots$*).*

Доказательство. *(1)* $\Rightarrow$ *(2).* Докажем, что из аксиом $\mathbf{1^0\text{-}9^0}$ и *(1)* следует *(2)*. Будем рассуждать от противного: пусть существует последовательность $\{A_i\}_{i \in N}$ с указанным свойством. Эта последовательность задаётся некоторой функцией $A: \mathbf{N} \to ?$, область значений которой является множеством, состоящим из всех множеств A_i $(i \in \mathbf{N})$. По *(1)* в этом множестве $Im(A)$ существует элемент $B = A_n$, не содержащий никаких множеств A_i $(i \in \mathbf{N})$ в качестве элементов. Однако, $A_{n+1} \in A_n$ – противоречие.

(2) $\Rightarrow$ *(1).* Докажем, что из аксиом $\mathbf{1^0\text{-}9^0}$ без $\mathbf{7^0}$ и *(2)* следует аксиома регулярности. Снова рассуждаем от противного. Неформальное рассуждение очень простое: пусть A – непустое множество, не удовлетворяющее аксиоме регулярности. Тогда можно выбрать некоторый элемент $A_1 \in A$, который не может удовлетворять свойству $\forall a \in A \ a \notin A_1$. Значит, можно найти элемент $A_2 \in A_1 \in A$. Если уже построены элементы $A \ni A_1 \ni A_2 \ni \ldots \ni A_i$ для некоторого $i \in \mathbf{N}$, то $A_i \in A$ не может удовлетворять свойству $\forall a \in A \ a \notin A_i$. Поэтому, можно найти некоторый элемент $A_{i+1} \in A_i$, получив таким образом более длинную цепочку $A_1 \ni A_2 \ni A_3 \ni \ldots \ni A_i \ni A_{i+1}$. Итак, вопреки предположению *(2)*, построена бесконечная последовательность $A_1 \ni A_2 \ni \ldots \ni A_i \ni \ldots$.

Теорема доказана.

Упражнения: 1. Формализуйте доказательство импликации $(2) \Rightarrow (1)$. Нужна ли аксиома выбора или эквивалентные ей утверждения для строгого доказательства ?

2. Вспомните, опираясь на свой математический опыт, не менее трёх случаев, когда при доказательстве теорем (?!) проводились без комментариев подобные рассуждения.

3. Проанализируйте доказательство последней теоремы и укажите, какие именно аксиомы использованы при доказательстве каждой импликации.

Последняя теорема вместе с упражнением **5** предыдущей серии упражнений показывает, что любое линейно упорядоченное отношением принадлежности $\in$ множество множеств является на самом деле вполне упорядоченным. В частности, вполне упорядоченными относительно $\in$ являются все ординалы, в частности, построенное множество натуральных чисел $\boldsymbol{N}$. В любом вполне упорядоченном множестве справедлив следующий

Принцип (трансфинитной) индукции: *Пусть M – вполне упорядоченное отношением строгого линейного порядка $\prec$ множество с наименьшим элементом m_0. Тогда для любой формулы $A(x)$ теории множеств (с единственной свободной переменной x), удовлетворяющей условию*

$$A(m_0) \wedge (\forall\, m \in M\ (\forall\, u \in M\ (u \prec m) \to A(u)) \to A(m)),$$

верно утверждение $\forall\, m \in M\ A(m)$.

Доказательство. От противного: если $\exists\, n \in M\ \overline{A(n)}$, то $\{n \in M \mid \overline{A(n)}\} \neq \varnothing$ и, ввиду полной упорядоченности, можно рассмотреть наименьший элемент n_0 этого множества. Значит, $\forall\, u \in M\ (u \prec n_0) \to A(u))$, причём $n_0 \neq m_0$ по условию $A(m_0)$ теоремы. Это противоречит условию $\forall\, m \in M\ (\forall\, u \in M\ (u \prec m) \to A(u)) \to A(m))$.

Принцип трансфинитной индукции доказан.

Легко видеть, что для вполне упорядоченного множества натуральных чисел $(\boldsymbol{N}, <)$ принцип трансфинитной индукции превращается в принцип математической индукции, точнее в аксиому индукции для формальной арифметики. Таким образом, в рамках теории множеств получено обоснование формальной арифметики. Восстановите все необходимые детали рассуждений самостоятельно.

Упражнение: Можно ли принцип трансфинитной индукции "упростить" следующим образом: $A(m_0) \wedge (\forall\, m \in M\ A(m) \to A(m_+)) \to (\forall\, m \in M\ A(m))$? Здесь для каждого $m \in M$ через m_+ обозначен элемент $min\{n \in M \mid n \succ m\}$ – непосредственно следующий за m элемент вполне упорядоченного множества $(M, \prec)$.

§ 3. Формальная теория множеств: райские кущи или адские дебри ?

Попытаемся неформально проанализировать общематематические достижения в задаче обоснования теории множеств. Сразу нужно отметить, что замкнутого изложения основ формальная теория множеств не даёт. Во-первых, при доказательстве теорем ис-

пользовались законы математической логики, которые, в свою очередь как отмечалось ранее, требовали (хоть и минимального) знакомства с понятием множества. Во-вторых, неявно предполагалось использование арифметики. Кто с этим не согласен, пусть возьмёт на себя труд пересчитать использованные в пояснениях и доказательствах числительные и попробует обойтись без них… Наконец, для того, чтобы иметь возможность писать любые формулы теории множеств, необходим бесконечный (или по крайней мере, сверхбольшой) алфавит, которым мы молчаливо пользовались. Поэтому всякие претензии на основополагающую роль аксиоматической теории множеств в качестве фундамента для всех математических дисциплин, мягко говоря, не состоятельны. Это относится в равной степени и к другим известным аксиоматикам теории множеств (например, к теории классов Гёделя-Бернсайда, которая эквивалентна теории Цермело-Френкеля).

За краткую (почти столетнюю) историю использования приведённой системы аксиом не было выявлено ни одного противоречия. Это, конечно, не доказывает непротиворечивости построенной теории множеств, ибо противоречия могут обнаружиться в любой момент, но всё же, вселяют некоторую уверенность при использовании множеств. Как уже говорилось, теорема Гёделя не оставляет надежд на доказательство непротиворечивости теории множеств средствами самой теории. Теория множеств неполна, так что существуют утверждения, истинные в некоторых моделях теории множеств, ложные в других и не доказуемые (т.е. не выводимые формально-логическим путём из аксиом теории множеств). Одно дело, когда неполна некоторая частная ветвь математики, но совсем другое дело, когда неполным является основание, т.к. любые различные между собой варианты теории множеств, могут быть надстроены до различных между собой математик.

Долгое время не было известно достаточно простых примеров недоказуемых, и неопровержимых утверждений теории множеств, так что можно было надеяться, что такие монстры слишком экзотичны, искусственны и потому не могут приводить к осязаемым простыми смертными разветвлениям математической науки. Однако, в *60*-е годы XX в. П. Коэном (за подробностями обратитесь к книге [12]) была решена одна из проблем Гильберта – о континуум-гипотезе, и выяснилось, что монстры находятся ближе, чем мы предполагаем: можно сказать, что некоторые из них живут среди нас… Континуум-гипотеза формулируется очень просто: существует ли подмножество X множества действительных чисел $\boldsymbol{R}$, которое содержит все натуральные числа и не равномощно ни $\boldsymbol{R}$, ни $\boldsymbol{N}$? Оказывается, что утверждение о существовании такого множества X недоказуемо и неопровержимо в теории множеств. Поэтому можно с равным основанием принять в качестве аксиомы как наличие такого подмножества $\boldsymbol{N} \subset X \subset \boldsymbol{R}$, так и его отсутствие. Согласитесь, что при реализации любого из этих подходов получаются разные теории вещественных чисел. И дело здесь не в одном утверждении – из принятых аксиом будут выводиться всё новые и новые теоремы, в корне отличные от своих антиподов в другой теории вещественных чисел, что может в конечном итоге изменить привычный мир чисел до неузнаваемости. Так иная, неизведанная и во многом чуждая математика просачивается даже в зазор между натуральными и вещественными числами. Теперь математики могут с полным основанием, перефразируя М.А. Булгакова, спрашивать друг

друга при встрече: “Какую именно разновидность из множества теорий множеств Вы предпочитаете в данное время суток ?”

Быть может, подобные простые недоказуемые утверждения будут скоро открыты и в арифметике. Само их существование в корне меняет психологический климат и настрой математика: если раньше он мог быть уверен, что рано или поздно любая математическая теорема будет либо доказана, либо опровергнута, то теперь такой уверенности нет. Нужно постоянно держать в уме возможность “ничейного” исхода, когда данное утверждение может оказаться независимым от принятой аксиоматики, причём не только от аксиоматики той области, в которой математик ощущает себя профессионалом, но и от неведомых аксиом тёмных, скрытых от постороннего взгляда дилетанта, закоулков зыбких оснований математической науки в целом. Так на смену наивному оптимизму человекобога-творца-преобразователя приходит трезвое понимание ограниченности возможностей бренного человека в неограниченно расширяемом им самим мире потенциально-виртуально-мнимых реальностей. Вспоминается афоризм незабвенного Ежи Леца: “Ну, пробил ты головой стену… И что будешь делать в соседней камере ?..”

Попытаемся теперь ещё раз проанализировать аксиомы теории множеств, кратко останавливаясь лишь на самых неочевидных. Это представляется необходимым, поскольку изложение наше, как это ни печально, было не достаточно формальным, хотя даже в таком виде воспринималось, наверное, с большим трудом. Неформальность эта, прежде всего, выражалась в том, что мы не всегда строго следовали букве формального теоретико-множественного закона. Так, например, для некоторых множеств и теоретико-множественных конструкций были введены удобные и выразительные обозначения ($\varnothing$, $A \cap B$, $A \times B$, $f: A \to B$ и т.д.), которые тем не менее не входят в исходный алфавит. Поэтому, действуя формально, нужно было всякий раз, когда использовалась такая конструкция, писать вместо неё соответствующую её определению формулу, что, конечно же, неудобно, хотя иногда и полезно попробовать. Кроме того, изредка совершались сознательные отступления от аксиоматического канона, на которые, как и на некоторые другие детали приведённых в прошлом параграфе рассуждений, пришло время указать, чтобы прояснить ситуацию. Наконец, неформальными были и доказательства, записанные не в виде формальных логических выводов, а на языке, который можно с полным основанием назвать смесью французского с нижегородским, поскольку в нём причудливо сплетались конструкции русского языка с обрывками математических формул. Попробуйте хотя бы раз хотя бы начать записывать хотя бы только начало доказательства хотя бы одной хотя бы не очень содержательной теоремы, чтобы понять раз и навсегда, какой ад скрывается за ажурной, почти невидимой решёткой райского сада формально-аксиоматического построения любой математической теории… Надеюсь, что большинство читателей обратили внимание на эти умышленные вкрапления неточностей, и буду особенно благодарен, если кто-то укажет и на другие вкравшиеся в текст (не по злой воле автора) несуразности.

3^0. аксиома выделения : $\forall\, A\ \exists\, B\ \forall\, x\ (x \in B \leftrightarrow x \in A \wedge P(x))$, *где* $P(x)$ *– произвольная формула теории множеств со свободной переменной* x, *в которую не входят предметные переменные* A *и* B.

Внимательный читатель уже заметил, что эта аксиома неоднократно нарушалась (постарайтесь выявить, где именно, сколько раз, и сверьте ответы с товарищами !!). В тексте есть ряд мест, где встречаются и пропускаются без комментариев неформальные применения этой аксиомы (пройдитесь ещё раз по тексту, чтобы эти случайные встречи оставили неизгладимое впечатление в памяти).

Таким образом, главная трудность использования аксиомы выделения заключается в том, чтобы не допустить случайного вхождения переменных A и B в формулу $P(x)$. Тем не менее, иногда это приходится делать для краткости записи. Например, при доказательстве импликации $(2) \Rightarrow (4)$ теоремы о равносильных формулировках аксиомы выбора изучалось множество

$$K_a = \{X \in L \mid (\{a\} - н.с.\ X) \wedge (\forall\ Y\ (Y - н.с.\ X) \wedge (Y \neq X) \rightarrow (f(Y) = inf_X(X \setminus Y)))\},$$

о происхождении которого ничего не было сказано. Конечно, оно образовано по аксиоме выделения, но с явными нарушениями этой аксиомы, ибо выделяющее условие не является формулой теории множеств (в нём участвует неформальные записи $\{a\}$, $(Y - н.с.\ X)$), $f(Y) = inf_X(X \setminus Y)$. Для устранения этой неточности нужно заменить эти неформальные записи их формальными определениями в виде форммул. Наконец, для торжества формализма нужно всюду избавиться от обозначений $\subseteq$ и $\subset$, $\varnothing$, $\cup\{S \in K\}$ и $\cup\{T \in K \mid T \subset S\}$, $f(\cup\{T \in K \mid T \subset S\})$, также подставив вместо них определяющие формулы. Проделайте это весьма поучительное упражнение самостоятельно. Если после всех этих манипуляций определение множества K_a займёт у Вас менее полстраницы и Вы ещё будете способны что либо в нём понимать, я готов пожать Вашу мужественную руку ! Подобного сорта нарушения формального аксиоматического канона, обусловленные стремлением к краткости, выразительности и утилитарной экономии чернил и бумаги, встречаются и в других местах. Их можно исправить с помощью аналогичных расшифровок и подстановок.

В чём смысл ограничений на использованную в аксиоме выделения формулу ? Понятно, что недопустимость вхождения в $P(x)$ переменной B (обозначающей определяемое множество) обусловлена стремлением избежать замкнутого круга при таком определении и возникающих противоречий: например, без этого ограничения существовало бы следующее противоречивое “множество” $B = \{x \in A \mid B \neq \varnothing \wedge x \notin B\}$. Хотя противоречия возникают не всегда, и с ними, видимо, можно было бы бороться менее кардинальными мерами, но сложившаяся с обоснованием теории множеств ситуация такова, что будучи не в силах совладать даже с имеющейся теорией, вряд ли имеет смысл стремиться к ещё большему её расширению.

Теперь самое время раскрыть страшную тайну: если в формуле $P(x)$ присутствует переменная A, то при наличии достаточно большого алфавита условие аксиомы выделения можно удовлетворить, записывая в нужном месте доказательства вместо стандартного $\exists\ B\ (\forall\ x\ (x \in B \leftrightarrow x \in A \wedge P(x)))$ более длинное $(\exists\ A_1\ (\forall\ x\ \ (x \in A_1 \leftrightarrow x \in A)) \wedge \wedge (\exists\ B\ \ (\forall\ x\ \ (x \in B \leftrightarrow x \in A_1 \wedge P_1(x))))$, где формула $P_1(x)$ получена из $P(x)$ заменой всех вхождений переменной A на переменную A_1, не использованную ранее. Так что, условие неиспользования переменной A в этой аксиоме чисто экономическое, хотя сле-

дуя негласному математическому преданию, умение обходиться без нарушения условий аксиомы выделения считается хорошим стилем, т.к. уменьшает вероятность впасть в порочный круг при конструировании множеств.

Замечание. Попытка избавиться от вхождения переменной B в формулу $P(x)$ не увенчается успехом, ибо написать $\exists\ B_1\ (\forall\ x\ (x \in B_1 \leftrightarrow x \in B))$, можно лишь в том случае, если известно, что B – множество.

Самый лучший вариант использования аксиомы выделения, к которому следует стремиться, – это отсутствие других свободных переменных, кроме x, в формуле $P(x)$. Тогда эта формула задаёт предикат, областью истинности которого и является выделяемое множество B. В общем случае этот "предикат" зависит от некоторых других переменных, участвующих в $P(x)$, и это требует внимательного контроля – что скрывается за их значениями. Например, если $A = \{x \in B \mid x \in C\}$, $C = \{x \in A \mid x \notin B\}$, то оба множества A и C корректно определены по аксиоме выделения (если переменные A и C различны), но оба они обязаны быть пустыми (?!). Более сложный пример: неформальная (но формализуемая) формула

$$(\exists\ B = \{x \in \mathbf{N} \mid x > \max C - 4\}) \wedge B \neq \varnothing \wedge \mathbf{N} \setminus B \neq \varnothing \wedge$$
$$\wedge\ (\exists\ C = \{y \in B \mid \min(\mathbf{N} \setminus B) + 1 \le y < \min B + 4\})$$

задаёт множества B и C неоднозначно: например, можно взять $B = \{n \in \mathbf{N} \mid n > 2\}$, $C = \{3, 4, 5, 6\}$, или $B = \{n \in \mathbf{N} \mid n > 8\}$, $C = \{9, 10, 11, 12\}$ (докажите, что общий вид множеств B и C таков: $B = \{n \in \mathbf{N} \mid n > k\}$, $C = \{k+1, k+2, k+3, k+4\}$ для некоторого $k \in \mathbf{N}$!!).

Упражнение. Для любого ли $n \in \mathbf{N}$ существует n-элементное множество A, если

$$(A \subseteq \mathbf{N}) \wedge (A - \text{конечно}) \wedge (\max A + \min A < 2 \cdot \min(\mathbf{N} \setminus A)) \wedge$$
$$\wedge\ (\forall a \in A\ \exists\ c \in A\ \ a + c \notin A\ \wedge\ a \cdot c \in A)\ ?$$

Какие значения может принимать величина $\min(\mathbf{N} \setminus A)$?

Трудности ещё более усугубляются в следующем примере: $A = \{x \in \mathbf{N} \mid x - 1 \notin B\}$, $B = \{y \in A \mid y^2 \notin A\}$. Ясно, что $1 \in A$ и потому $1 \notin B$. Далее, $2 \in A$, но для того, чтобы определить, принадлежит ли 2 множеству B, необходимо знать верно ли, что $4 \in A$. Таким образом, проследить последовательно за элементами множеств A и B не представляется возможным, ибо задание этих множеств предполагает изрядную долю произвола. Тем не менее, множества, удовлетворяющие условиям для A и B, существуют: например, $A = \mathbf{N}$, $B = \varnothing$ (приведите пример непустого множества B !!).

Итак, даже приведённые простые примеры показывают, что совместное задание бесконечных множеств (когда одно определяется через другое, которое, в свою очередь, задаётся с использованием элементов первого), приводит к непростым взаимовлияниям, что делает неочевидным не только решение вопроса о принадлежности какого-либо конкретного элемента этим множествам, но и вызывает небезпочвенные сомнения по поводу самого факта существования заданных множеств. Что уж говорить о бесконечных совокупностях множеств, определяемых с помощью перекрёстных ссылок на опре-

деления друг друга ! Не случайно поэтому, что многие математики не признают аксиому выделения в сформулированном широком виде, требуя ограничений на структуру выделяющей формулы $P(x)$. Тем не менее, ***доказано, что использование только аксиомы выделения даже для бесконечных совокупностей множеств не приводит к противоречиям*** [см. 12].

7^0. аксиома регулярности : $\forall A \neq \varnothing \; \exists B \in A \;\; \forall a \in A \;\; a \notin B$

Если сравнивать теорию множеств с игрой в детский конструктор, то другие аксиомы дают средства построения новых множеств из уже известных, и лишь аксиома регулярности запрещает существование некоторых множеств. Поэтому на аксиоме регулярности лежит важная и ответственная миссия контролёра, которая требует отсеять из и без того неочевидной теории как можно больше подозрительных объектов. Как уже отмечалось, эта аксиома лишила статуса множества, например, такой объект как совокупность всех множеств. Этим и обусловлена её достаточно жёсткая форма, запрещающая, как мы видели существование множеств с бесконечными убывающими цепями $a_1 \ni a_2 \ni \ldots \ni a_n \ni \ldots$ Конечно, избавиться от "множества всех множеств" можно было множеством иных способов, требующих значительно более малой крови, однако аксиома отсекла сразу всё, что не соответствовало математической практике. Дело в том, что за всю историю существования математики ни разу не возникла необходимость рассматривать множество, имеющее такие запрещённые бесконечные цепи элементов. С другой стороны, существуют множества, со сколь угодно длинными убывающими по отношению принадлежности цепями элементов: например, построенное нами в прошлом множество $\boldsymbol{N}$ (выделенное в бесконечном множестве N) содержит такие цепи любой заданной длины. Поэтому вводить дальнейшие ограничения в том же направлении – это значит уже резать по живому.

8^0. аксиома существования области значений : *для любой формулы $\Phi(x, y)$ со свободными переменными x, y справедливо свойство*

$$\forall A \, (\forall x \in A \;\; \forall y, z \;\; (\Phi(x, y) \wedge \Phi(x, z) \to y = z)) \to \exists B \;\; \forall y \, (y \in B \leftrightarrow \exists x \in A \; \Phi(x, y))$$

Как уже говорилось, эта аксиома даёт лексический способ задания функции – с помощью формулы, удовлетворяющей условию функциональности – сразу на любом множестве. После сделанных замечаний об аксиоме выделения становится ясно, что при наличии достаточно большого алфавита предметных переменных для любой формулы $\Phi(x, y)$ (возможно после незначительной её модификации) можно рассматривать множество $f = \{x \in A \times Im_A(\Phi) \mid \exists \; a \in A \;\; (\exists \; b \in Im_A(\Phi) \;\; x = (a; b) \wedge \Phi(a, b))\}$, которое будет функцией из множества A в множество $Im_A(\Phi)$.

С помощью этой аксиомы вводились ординалы. Конечно, их можно было определить и без "предиката" Ord (как множество со свойствами транзитивности относительно $\in$, линейной упорядоченности относительно $\in$ и существования наименьшего элемента относительно $\in$ в каждом непустом подмножестве), но аксиома существования области значений позволяет доказать, что множество ординалов, содержащихся в

данном множестве, будет множеством. Можно доказать, что "множество" всех ординалов на самом деле множеством не является (?!).

Это становится понятным, если учесть следующую эквивалентную форму аксиомы регулярности, смысл которой заключается в том, что все множества можно построить с помощью некоторого регулярного процесса из ординалов (поэтому и "регулярность" в названии аксиомы). Вот точная формулировка: *для любого множества A существует некоторый ординал α, для которого $A \in V_\alpha$, где V_α строится с помощью следующих операций (трансфинитной индукции по ординалам): а) $V_0 = \varnothing$; б) $V_\alpha = \mathcal{B}(V_\beta)$, если $\alpha = \beta + 1$; в) $V_\alpha = \bigcup_{\beta < \alpha} V_\beta$, если α – предельный ординал.* Здесь использованы следующие понятия и отношения для ординалов: символ 0 обозначает ординал $\varnothing$, $\alpha = \beta + 1$ означает, что $\alpha = \beta \cup \{\beta\}$, $\beta < \alpha$ – значит $\beta \in \alpha$, ординал α называется *предельным*, если он не имеет вида $\alpha = \beta + 1$.

Ординалы играют важную роль в математике, а процесс трансфинитной индукции, в котором в качестве вполне упорядоченного множества часто берётся множество всех ординалов некоторого множества, обобщает принцип математической индукции для натуральных чисел.

9^0. аксиома бесконечности : $\exists\, N\ ((\varnothing \in N) \wedge (\forall X \in N\ \ X \cup \{X\} \in N))$

С помощью этой аксиомы было построено множество натуральных чисел

$$\boldsymbol{N} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots\},$$

элементы которого – конечные ординалы – были обозначены символами $1, 2, 3, 4, 5, \ldots$ Можно доказать, что это множество в самом деле удовлетворяет аксиомам Пеано для натуральных чисел. Для этого, прежде всего, определим отображение $s: \boldsymbol{N} \to \boldsymbol{N}$, дающее для элемента $n \in \boldsymbol{N}$ значение $s(n)$ *непосредственно следующего за ним элемента*. Это можно сделать, задав s с помощью формулы $\Phi(x, y) = (y = x \cup \{x\})$ по аксиоме существования области значений. После этого легко убедиться в выполнении следующих свойств (аксиом Пеано):

(N1): $\forall\, n \in \boldsymbol{N}\ \ s(n) \neq 1$,

(N2): $\forall\, n \in \boldsymbol{N}\ \ (n \neq 1 \to (\exists m \in \boldsymbol{N}\ \ n = s(m)))$,

(N3): $\forall\, n, m \in \boldsymbol{N}\ \ (s(n) = s(m) \to n = m)$,

(N4): $\forall\, M \subseteq \boldsymbol{N}\ \ ((1 \in M \wedge (\forall n \in \boldsymbol{N}\ \ n \in M \to s(n) \in M)) \to M = \boldsymbol{N})$.

В самом деле, ***(N1)*** и ***(N2)*** очевидны (?!). Если $s(n) = s(m)$, то $n \cup \{n\} = m \cup \{m\}$. В случае $n \neq m$ получим $n \in m$ и $m \in n$ вопреки аксиоме регулярности. Таким образом, ***(N3)*** доказано. Свойство ***(N4)*** докажем от противного: пусть $\exists\, n \in \boldsymbol{N}\ \ n \notin M$. Тогда $A = \boldsymbol{N} \setminus M \neq \varnothing$ и по аксиоме регулярности содержит такой элемент $b \in A$, что $\forall c \in A\ \ c \notin b$. Поскольку $1 \in M$, то $b \neq 1$ и (по ***(N2)***) $b = s(c)$ для некоторого $c \in \boldsymbol{N}$. Если $c \in A$, то $c \in c \cup \{c\} = s(c) = b$, что невозможно. Таким образом, $c \in M$ и значит, $b = s(c) \in M$ – противоречие.

Упражнения: 1. Докажите ***(N2)***, не используя аксиому регулярности.

2. Докажите, что отношение $n \le m \leftrightarrow n \in m \vee n = m$ задаёт полный порядок на $\boldsymbol{N}$. (Указание: если $M \subset \boldsymbol{N}$ не имеет наименьшего элемента, то рассмотреть множество $K = \{k \in \boldsymbol{N} \mid \forall m \in M \;\; k < m\}$)

Чтобы не возникало ощущения, что таким образом обоснована арифметика натуральных чисел, внимательно перечитайте начало этого параграфа, чтобы отчётливо осознать: идея числа незримо витала над нами на всём протяжении построения теории множеств. Поэтому максимум, чем можно гордиться – лишь включением арифметики в качестве частного случая в более общую теорию множеств, которая, тем не менее, сама нуждается в обосновании и при построении которой неявно использовались арифметические конструкции. Так что серьёзного повода для эйфории здесь не обнаруживается !

10^0. аксиома выбора : $\forall X (\forall Y \in X \;\; Y \neq \varnothing \rightarrow \exists M \; \forall Y \in X \;\; \exists! \;\; m \in M \cap Y)$

Аксиома выбора была впервые сформулирована Э. Цермело, который с её помощью построил полный порядок на множестве действительных чисел. Его рассуждения были приняты в штыки большинством математиков, т.к. не давали конструктивного полного упорядочения множества $\boldsymbol{R}$, хотя и решали соответствующую проблему Гильберта о существовании такого порядка. Вскоре, однако, выяснилось, что утверждения, эквивалентные аксиоме выбора, использовались неявно и ранее при доказательстве многих фундаментальных теорем алгебры и анализа, так что всем стало ясно: насколько легко было не замечать аксиому выбора – эту золушку в блистательном дворце математики, – настолько же трудно, а практически невозможно, оказалось жить без её незаменимых услуг.

В настоящее время лишь последовательные конструктивисты отрицают использование аксиомы выбора в любой форме, большинство же математических сект принимает её, хотя и с некоторыми ограничениями, например, требуя счётность (т.е. равномощность множеству $\boldsymbol{N}$) от множества X, в элементах которого совершается выбор. На самом деле ясности это не прибавляет, поскольку теорема Левенгейма-Сколема гарантирует реализацию всей теории множеств в некоторой модели, состоящей только из счётных множеств. Здесь нужно объяснить кажущееся противоречие: все знают, что множество $\boldsymbol{R}$ несчётно – как же оно реализуется в такой модели ? Дело в том, что счётность – это (по определению) равномощность множеству $\boldsymbol{N}$. Таким образом, в рассматриваемой нестандартной модели теории множеств просто нет биективных функций из двойника множества $\boldsymbol{R}$ в двойника множества $\boldsymbol{N}$.

Слишком велики потери, которые понесёт математика при отказе от аксиомы выбора. Она используется, например, при доказательстве теоремы о том, что из всякой бесконечной ограниченной последовательности действительных чисел можно выбрать бесконечную сходящуюся подпоследовательность. Без неё не докажешь теорему о существовании максимума непрерывной функции на замкнутом интервале, не убедишься в компактности такого интервала, не обоснуешь теорему о промежуточных значениях непрерывной функции, и т.д. Без этой аксиомы невозможно работать с фактормножествами, ибо выбор представителей в классах эквивалентных элементов, как пра-

вило, осуществляется с её помощью. Отказ от аксиомы выбора приведёт к исчезновению теоремы о существовании базиса в бесконечномерных векторных пространствах, не говоря уж о более общих утверждениях из теорий групп и колец, связанных с процедурами недетерминированного выбора. Дело даже не в конкретных теоремах – дело в том, что рушатся целые математические миры, которые доселе скрепляет незримая сила, скрытая в этой загадочной аксиоме. Нужно отметить, что само по себе использование аксиомы выбора в том или ином рассуждении вовсе не означает ещё, что это утверждение невозможно доказать без её использования. Вопрос о роли этой аксиомы в доказательстве конкретной теоремы чрезвычайно труден, он требует кропотливого анализа места доказываемой теоремы в здании математики и её взаимосвязей с другими аксиомами. Перечисленные выше утверждения – это лишь наиболее простые примеры, для которых фатальный исход в случае отказа от аксиомы выбора предрешён и доказан. Во многих других случаях положение ещё не столь определённо. Тем не менее, опасность потерять многое частично утишает страсти и охлаждает головы не в меру ретивых математических революционеров-реакционеров.

С другой стороны, из аксиомы выбора следуют довольно странные выводы. Например, представьте себе футбольный мяч и земной шар. Что бы Вы сказали, если бы Вас пытались убедить в том, что можно разрезать мяч на несколько частей (более точно: разбить на несколько подмножеств) и, переместив их в пространстве, покрыть ими земной шар ? Боюсь, что мало кто из нормальных людей подпишется под эти утверждением… Тем не менее, это – теорема Банаха-Тарского, лишь поданная в неформальной парадоксальной упаковке. С математической точки зрения, никакого противоречия это утверждение не содержит, хотя и выглядит странно. Дело в том, что подмножества, на которые разбивается мяч, не являются геометрическими фигурами ! Поэтому при движениях в пространстве не обязаны сохраняться такие их характеристики как площадь, объём и др. Здесь ещё раз предельно выпукло проявляется отличие пространства математического от пространства реального, сферы – как математического объекта, от её реальных бренных прототипов. Чисто внешние, поверхностные сходства не следует автоматически переносить на глубинные, более тонкие и бесконечно более богатые внутренние содержания: математические структуры и реальные объекты – вещи несовместные.

Другая, не менее парадоксальная форма теоремы Банаха-Тарского состоит в том, что *круг можно разбить на пять таких непересекающихся между собой частей (одна из которых – точка), что, будучи передвинутыми на плоскости, эти части образуют два круга, каждый из которых равен исходному (А. Робинсон).* Кажущаяся парадоксальность подобных утверждений зиждется на нашей интуиции площади и объёма. Между тем, аксиома выбора позволяет построить множества, неизмеримые относительно любой нетривиальной меры, инвариантной относительно сдвигов. Пример такого множества на прямой (одномерном пространстве $\boldsymbol{R}^1$) будет приведён ниже. Так что те части сфер и кругов, которые участвуют в описанных разбиениях (по крайней мере, некоторые из них) будут неизмеримыми, и наша интуиция может спать спокойно – эти “парадоксы” не предмет её заботы.

Чтобы лучше понять суть применений аксиомы выбора, приведём строгое обоснование импликации $(2) \Rightarrow (1)$ в теореме об эквивалентных формулировках аксиомы ре-

гулярности, ибо в нём, как в капле воды, отражаются все те проблемы, с которыми сталкивается математик во многих математических рассуждениях, связанных с недетерминированным выбором.

Теорема (эквивалентные формулировки аксиомы регулярности). *Следующие утверждения эквивалентны в системе аксиом* $\mathbf{1^0\text{-}6^0}$, $\mathbf{8^0\text{-}9^0}$:

(1) аксиома регулярности : $\forall A \neq \varnothing \; \exists B \in A \;\; \forall a \in A \;\; a \notin B$,

(2) принцип отсутствия бесконечных убывающих (по отношению $\in$*) цепей множеств: не существует бесконечной последовательности* $\{A_i\}_{i \in N}$ *множеств, удовлетворяющей условию* $\forall i \in \mathbf{N} \;\; A_{i+1} \in A_i$ *(т.е.* $A_1 \ni A_2 \ni A_3 \ni \ldots \ni A_i \ni \ldots$*).*

Доказательство. *(2)* $\Rightarrow$ *(1).* Докажем, что из аксиом $\mathbf{1^0\text{-}9^0}$ без $\mathbf{7^0}$ и *(2)* следует аксиома регулярности. Снова рассуждаем от противного. Неформальное рассуждение очень простое: пусть A – непустое множество, не удовлетворяющее аксиоме регулярности. Тогда можно выбрать некоторый элемент $A_1 \in A$, который не может удовлетворять свойству $\forall a \in A \;\; a \notin A_1$. Значит, можно найти элемент $A_2 \in A_1 \in A$. Если уже построены элементы $A \ni A_1 \ni A_2 \ni \ldots \ni A_i$ для некоторого $i \in \mathbf{N}$, то $A_i \in A$ не может удовлетворять свойству $\forall a \in A \;\; a \notin A_i$. Поэтому, можно найти некоторый элемент $A_{i+1} \in A_i$, получив таким образом более длинную цепочку $A_1 \ni A_2 \ni A_3 \ni \ldots \ni A_i \ni A_{i+1}$. Итак, вопреки предположению *(2)*, построена бесконечная последовательность $A_1 \ni A_2 \ni A_3 \ni \ldots \ni A_i \ni \ldots$.

Импликация “доказана”.

На самом деле, нужно построить функцию $f: \mathbf{N} \to \mathcal{B}(A)$ со свойством $\forall \; i \in \mathbf{N}$ $f(i+1) = A_{i+1} \in A_i = f(i)$. То, что сделано в предыдущем “доказательстве”, эту задачу не решает: например, не ясно даже, почему построенные элементы A_1, A_2, … образуют множество. Думаю, что каждый может привести ещё по крайней мере несколько примеров, когда, не задумываясь, проводил подобные правдоподобные рассуждения, в которых скрыто неявное использование аксиомы выбора, на что первым обратил внимание Э. Цермело.

Итак, проведём рассуждения более формально. Рассмотрим следующее множество функций (не обязательно всюду определённых):

$$F = \{f: \mathbf{N} \to A \;\mid\; \forall i, j \in D(f) \;\; i < j \to f(j) \in f(i)\}$$

Формализуйте задание множества F самостоятельно. Множество F непусто, т.к. содержит, например, функции, определённые на множестве $\{1\}$: $f = \{(1, A_1)\} \in F$. Более того, наше неформальное построение можно использовать, чтобы обосновать существование таких функций с любой конечной областью определения $D(f) = \{1, \ldots, n\}$. Однако, доказать без аксиомы выбора существование всюду определённой функции во множестве F, тем не менее, не удастся. Проще всего это сделать, используя лемму Цорна, предварительно убедившись, что любая цепь в частично упорядоченном множестве $(F, \subseteq)$ имеет верхнюю грань. Если C – цепь функций из F, то функция $\cup \{f \in C\} \in F$ и является верхней гранью множества C. Значит, по лемме Цорна, во

множестве F существует максимальный элемент $m: \mathbf{N} \to A$. Если область определения $D(m)$ функции m равномощна $\mathbf{N}$, то существует биективное отображение $i: \mathbf{N} \to D(m)$, и $f = m \circ i : \mathbf{N} \to A$ будет искомым отображением. Если же $D(m)$ конечно, то это противоречит максимальности m: если $k = max\, D(m)$, то $\exists\, B \in m(k)$, и m можно расширить, вопреки максимальности: $m \subset m \cup \{(k+1, B)\} \in F$.

Теорема доказана.

Упражнение. Постарайтесь видоизменить приведённое рассуждение, чтобы сразу получить всюду определённую функцию (без привлечения явно посторонних идей о равномощности).

Приглядевшись к этим рассуждениям, можно увидеть, что аналогичные проблемы выбора возникают даже при решении, например, следующей простой задачи: *построить в произвольном неограниченном снизу частично упорядоченном множестве* $(A, \leq)$ *бесконечно убывающую цепочку* $a_1 > a_2 > \ldots > a_n > \ldots$ Следует подчеркнуть, что проблемы появляются только тогда, когда порядок на A произволен, т.е. не обладает какими-либо дополнительными свойствами, облегчающими задачу. Например, в $(\mathbf{R}, \leq)$ это делается без аксиомы выбора, т.к. последовательность $a_n = -n$ $(n \in \mathbf{N})$ будет искомой. Решение получилось простым, из-за возможности заменить процедуру недетерминированного выбора явным заданием последовательности по аксиоме выделения. Если никаких аналогичных упрощений применить не удаётся, то без аксиомы выбора в подобной ситуации не обойтись.

Наконец, приведём обещанный пример неизмеримых множеств.

Теорема (о существовании неизмеримых по Лебегу множеств). *Существуют множества в* $\mathbf{R}$, *неизмеримые относительно любой нетривиальной (не равной тождественно нулю) меры (функции длины), инвариантной относительно сдвигов (т.е. оставляющей меру множества неизменной при параллельных переносах в* $\mathbf{R}$*).*

Доказательство. Рассмотрим отрезок $[0; 1]$ и введём на нём отношение эквивалентности ρ по правилу $x \rho y \leftrightarrow x - y \in \mathbf{Q}$. Очевидно, что это бинарное отношение будет в самом деле отношением эквивалентности (т.е. оно рефлексивно, симметрично и транзитивно). Множество $[0; 1]$ разбивается, таким образом, на непересекающиеся между собой классы эквивалентных элементов. По аксиоме выбора для разбиений, в каждом из них можно выбрать по представителю, которые в совокупности образуют некоторое множество-выборку M. Докажем, что M – искомое неизмеримое множество.

В самом деле, $\forall x \in [0; 1]\ \exists!\, m \in M\ x - m \in \mathbf{Q} \cap [0, 1]$. Поэтому имеем: $[0; 1] \subseteq \cup\{M+q \mid q \in \mathbf{Q} \cap [0; 1]\}$, и $\forall\, p, q \in \mathbf{Q} \cap [0; 1]\ p \neq q \to (M+q) \cap (M+p) = \varnothing$. Действительно, если $x \in (M+q) \cap (M+p)$, то $x = m + q = n + p$, где $n, m \in M$, $p, q \in \mathbf{Q}$, $p \neq q$, т.е. $m = n + (p - q) \neq n$: m и n – два различных элемента из одного класса эквивалентности, что противоречит построению выборки M.

Таким образом, отрезок $[0; 1]$ оказался покрыт счётным числом непересекающихся между собой множеств вида $M + q$, полученных из M сдвигом на рациональные числа q. Если M измеримо инвариантной относительно сдвигов мерой $\mu: \mathbf{R} \to \mathbf{R}$, то

$\mu(M+q) = \mu(M)$ и $\mu([0; 1]) \le \mu(\cup\{M + q \mid q \in \mathbf{Q} \cap [0, 1]\}) = \sum_{q \in \mathbf{Q}} \mu(M + q)$ (свойство счётной аддитивности меры). Последняя сумма представляет собой бесконечную сумму одинаковых слагаемых, равных $\mu(M)$, так что для суммируемости этого ряда необходимо и достаточно условие $\mu(M) = 0$. Однако тогда получим $\mu([0; 1]) = 0$ и $\mu(\mathbf{R}) = \mu\left(\bigcup_{n \in \mathbf{Z}} [n; n+1]\right) = \sum_{n \in \mathbf{Z}} \mu([n; n+1]) = \sum_{n \in \mathbf{Z}} \mu([0; 1]) = 0$, вопреки условию нетривиальности меры.

Теорема доказана.

Следует отметить, что как бы то ни было, "корень зла" для теории множеств скрыт не в аксиоме выбора. Ещё К. Гёдель доказал, что аксиома выбора независима от остальных аксиом теории множеств. Значительно большее доказал П. Коэн: континуум-гипотеза независима от аксиом теории множеств независимо от того, включается ли в список аксиом аксиома выбора, или нет, а аксиома выбора независима от остальных аксиом теории множеств независимо от того, включается ли в список аксиом континуум-гипотеза, или нет. Основная трудность в исследованиях этих проблем состоит в выяснении взаимоотношений перечисленных утверждений с аксиомой регулярности, которая накладывает жёсткие ограничения на потенциально-возможные мыслимые миры множеств, удовлетворяющих всем остальным аксиомам.

В заключение остановимся на ещё одном "теоретико-множественном парадоксе", преграждающем и без того тернистый путь по извилистой тропе познания в поисках утраченной математической строгости. Он был приведён в письме Берри к Расселу и является упрощением "парадокса Тарского".

Рассмотрим множество M всех тех натуральных чисел, которые могут быть однозначно определены высказываниями, состоящими не более чем из тысячи букв русского алфавита. Это множество не пусто, поскольку число 1 можно определить, например, так: 1 – это "наименьшее натуральное число". Ясно, что множество M конечно (т.к. конечно число различных осмысленных слов русского языка). Следовательно, множество $\mathbf{N} \setminus M$ бесконечно и, в частности, не пусто. Известно, что каждое непустое подмножество в $\mathbf{N}$ имеет наименьший элемент. В частности, такой наименьший элемент x существует в $\mathbf{N} \setminus M$. По определению множества M, он не может быть определён высказыванием, состоящим не более чем из тысячи букв русского алфавита. С другой стороны, следующее определение: x – это "наименьший из элементов множества всех тех натуральных чисел, которые не могут быть определены высказываниями, состоящими не более чем из тысячи букв русского языка", показывает, вопреки всем доводам рассудка, что $x \in M$. Где ошибка ?

Конечно, можно сразу отмахнуться от этого парадокса, как от назойливой мухи – ведь сразу видно, что к той теории множеств, азы которой мы изучили, приведённое рассуждение не имеет никакого отношения, ибо задание множества M не формализова-

но. Тем не менее, полезно обсудить возникающие здесь проблемы, чтобы лучше понять отличие формальной теории от неформальных рассуждений.

Первый из возникающих вопросов: что значит "могут быть однозначно определены высказываниями …" Видимо, нужно понимать это следующим образом: для каждого $m \in M$ существует высказывание о натуральных числах $A(x)$, состоящее не более чем из тысячи букв русского алфавита, которое истинно тогда и только тогда, когда $x = m$. Однако это ещё не полностью проясняет смысл, ибо непонятным остаётся главное – что такое высказывание. В неформальном языке, это понятие не имеет чёткого определения (см. § 1 главы I), что и создаёт возможность для спекуляций, подобных той, что мы рассматриваем. Далее, в качестве примера, доказывающего, что множество M непусто приведено высказывание, определяющее натуральное число 1: "1 – это наименьшее натуральное число". Можно ли считать это определением ? Чёткого ответа дать невозможно, ясно только одно – это высказывание не является полным определением, ибо не даёт понятия о том, что такое натуральные числа, об отношении порядка на них и о наименьшем элементе. Кто возьмётся определить всё это одной фразой ?

Другой вопрос: можно ли в высказывании говорить о самом "множестве" M ? Если это допускается, то может возникнуть порочный круг, аналогичный тому, что был приведён при обсуждении аксиомы выделения. Запретить же такие высказывания нет возможности, ибо можно не ссылаясь непосредственно на M, включить в высказывание само свойство, определяющее M. Итак, мы видим, что чёткого понимания того, что требуется от элементов множества M, не возникает. Поэтому нет уверенности, что совокупность элементов, удовлетворяющих данному неформальному свойству, образует множество, ибо в списке аксиом Цермело-Френкеля нет аксиом, на основании которых построен объект M.

Тем не менее, попробуем построить совокупность натуральных чисел, входящих в M. Для этого необходимо выписать все фразы русского языка, состоящие не более чем из тысячи букв (их число конечно: оно не больше 33^{1000}), затем – отбросить все бессмысленные фразы и фразы, не являющиеся высказываниями (хотели бы Вы заняться такой работой ?!), и наконец, отсеять все высказывания, говорящие не о натуральных числах. После этого можно последовательно брать натуральные числа (начиная с 1) и просматривая весь список оставшихся высказываний, находить те, которым удовлетворяет только исследуемое число, откладывая их вместе с соответствующим числом в сторону. Кажется, что этот процесс приведёт в конечном итоге к построению всех элементов "множества" M… Так ли это ? В списке оставленных высказываний будет, например, следующее: "число x – наибольший из элементов множества всех тех натуральных чисел, которые могут быть определены высказываниями, состоящими не более чем из тысячи букв русского языка". Какое число мы сопоставим этому высказыванию ? Можно было бы надеяться, что до поры до времени удастся отложить в сторону это высказывание, а в самом конце выяснится, какое число ему сопоставить. Эти надежды также не состоятельны, ибо дело здесь не в том, что речь идёт о максимальном элементе, а в том, что существуют высказывания, говорящие о самом объекте M. Например, высказывание "половина числа x меньше на пять меньше наибольшего из элементов множества всех тех натуральных чисел, которые могут быть определены высказывания-

ми, состоящими не более чем из тысячи букв русского языка” тоже поставит нас в тупик. Таким образом, в конечном итоге перед нами останется список высказываний, ни одному из которых невозможно сопоставить ни одного натурального числа.

Таким образом, “множество” M образовано некорректно. Хотя никакой опасности для теории множеств этот парадокс не представляет, он позволяет высветить некоторые проблемы образования множеств, которые лишь подчёркивают совершенство аксиоматической теории множеств Цермело-Френкеля, вот уже около ста лет хранящего математический мир от подобных потрясений...

Упражнение. Может создаться впечатление, что в сложившейся патологической ситуации виновата свобода образования высказываний, обусловленная слишком либеральным ограничением (в тысячу букв) на длину высказывания. Убедитесь, что те же проблемы будут иметь место, если определить “множество” M следующим образом: M – множество всех тех натуральных чисел, которые могут быть однозначно определены высказываниями, состоящими не более чем из двадцати слов русского языка.

Л И Т Е Р А Т У Р А

А) ОСНОВНАЯ ЛИТЕРАТУРА:

1. Глухов М.М., Козлитин О.А., Шапошников В.А., Шишков А.Б. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов. – С.-Пб.: Издательство “Лань”, 2008.

2. Ершов Ю.Л., Палютин Е.А. Математическая логика. – СПб.: Издательство “Лань”, 2004.

3. Игошин В.И. Математическая логика и теория алгоритмов. – М.: Издательский центр “Академия”, 2004.

4. Игошин В.И. Задачник-практикум по математической логике. – М.: Издательский центр “Академия”, 2005.

5. Лавров И.А. Математическая логика. – М.: Издательский центр “Академия”, 2008.

6. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. – М.: Издательский центр “Академия”, 2007.

7. Лихтарников Л.М., Сукачева Т.Г. Математическая логика. – С.-Пб.: Издательство “Лань”, 2008.

Б) ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

8. Клини С. Введение в метаматематику / Пер. с англ. – М.: ИЛ, 1961.

9. Клини С. Математическая логика / Пер. с англ. – М.: Мир, 1973.

10. Колмогоров А.Н., Драгалин А.Г. Введение в математическую логику. – М.: Изд-во МГУ, 1984.

11. Кондаков Н.И. Логический словарь-справочник. – М.: , 1975.

12. Коэн П. Дж. Теория множеств и континуум-гипотеза. – М.: Мир, 1969.

13. Мальцев А.И. Алгоритмы и рекурсивные функции. – М.: Наука, 1965.

14. Математическая логика (Под общей редакцией А.А. Столяра и др.) – Минск: Вышейшая школа, 1991.

15. Мендельсон Э. Введение в математическую логику. – М.: Наука, 1976.

16. Новиков П.С. Элементы математической логики. – М.: Наука, 1973.

17. Смаллиан Р.М. Как же называется эта книга ? – М.: Мир, 1981.

18. Смаллиан Р.М. Принцесса или тигр ? – М.: Мир, 1985.

19. Чёрч А. Введение в математическую логику. – М: Мир, 1960.

20. Эдельман С.Л. Математическая логика. – М., 1975.

СПИСОК ОСНОВНЫХ ОБОЗНАЧЕНИЙ

$\boldsymbol{N}$ – *множество всех натуральных чисел,*

$\boldsymbol{Q}$ – *множество всех рациональных чисел,*

$\boldsymbol{R}$ – *множество всех действительных чисел,*

$\boldsymbol{B}$ – *множество* $\{0, 1\}$,

$\boldsymbol{f : X \to Y}$ – *функция из множества* X *со значениями во множестве* Y,

$\boldsymbol{f : ? \to ?}$ – *функция с неопределёнными областями определения и значений,*

$\boldsymbol{\{a_i\}_{i \in I}}$ – *последовательность элементов, индексированных элементами множества* I,

$\boldsymbol{D(f)}$ – *область определения функции* f,

$\boldsymbol{D_A(f)}$ – *область определения функции* f *с неопределёнными областями определения и значений на множестве* A,

$\boldsymbol{Im(f)}$ – *область значений функции* f,

$\boldsymbol{Im_A(f)}$ – *область значений функции* f *с неопределёнными областями определения и значений на множестве* A,

$\boldsymbol{P : A^n \to B}$ – *предикат на множестве* A,

$\boldsymbol{D_1(P)}$, $\boldsymbol{D_0(P)}$ – *области истинности и ложности предиката* P,

$\boldsymbol{f : X_1 \times \ldots \times X_n \to Y}$ – *функция от* n *аргументов* $x_1 \in X_1, \ldots, x_n \in X_n$ *со значениями во множестве* Y,

$>$, $\succ$ – *знаки "больше",* $a > b$, $a \succ b$ – a *больше* b,

$<$, $\prec$ – *знаки "меньше",* $a < b$, $a \prec b$ – a *меньше* b,

$\overline{\bullet}$ – *логическая связка отрицание,* $\overline{A}$ – *отрицание формулы* A,

$\wedge$ – *логическая связка конъюнкция,* $(A \wedge B)$ – *конъюнкция двух формул,*

$\vee$ – *логическая связка дизъюнкция,* $(A \vee B)$ – *конъюнкция двух формул,*

$\to$ – *логическая связка импликация,* $(A \to B)$ – *импликация двух формул,*

$\leftrightarrow$ – *логическая связка эквивалентность,* $(A \leftrightarrow B)$ – *эквивалентность двух формул,*

$\equiv$ – *знак равносильности формул,* $A \equiv B$ – *формулы* A *и* B *равносильны, т.е. имеют одинаковые значения при любых интерпретациях,*

$\sim$ – *знак равносильности формул в формальных теориях,* $A \sim B$ – *формулы* A *и* B *равносильны, т.е. доказуемы теоремы* $A \to B$ *и* $B \to A$,

$\oplus$ – *сложение по модулю 2 (исключающее или)* $\boldsymbol{a \oplus b} = a + b \pmod 2$,

$|$ – *штрих Шеффера,* $\boldsymbol{x \,|\, y} = (\overline{x} \vee \overline{y})$,

$\downarrow$ – *стрелка Пирса,* $\boldsymbol{x \downarrow y} = (\overline{x} \wedge \overline{y})$,

$\vdots$ – *делимость нацело целых чисел,* $\boldsymbol{x \vdots y}$ – x *делится нацело на* y,

$\boldsymbol{\Gamma \models A}$, $\boldsymbol{A_1, \ldots, A_n \models A}$, $\boldsymbol{\models A}$ – *обозначение логического следования формулы* A *из множества формул* Γ, *формул* $A_1, \ldots, A_n$, *из пустого множества формул,*

$\dfrac{\mathcal{A}_1, \ldots, \mathcal{A}_n}{\mathcal{A}}$ – *схема правил логического следования,*

$\boldsymbol{A(x_1, \ldots, x_n) \equiv 1}$, $\boldsymbol{A(x_1, \ldots, x_n) \equiv 0}$ – *формула* A *тождественно истинна (закон логики), соответственно тождественно ложная (противоречие),*

$\boldsymbol{P(x_1, \ldots, x_n) \equiv_A 1}$, $\boldsymbol{P(x_1, \ldots, x_n) \equiv_A 0}$ – *тождественно истинный и тождественно ложный предикаты на множестве* A,

$\boldsymbol{P(x_1, \ldots, x_n) \equiv 1}$, $\boldsymbol{P(x_1, \ldots, x_n) \equiv 0}$ – *тождественно истинный и тождественно ложный предикаты на множестве* $D(P)$,

$\boldsymbol{P(x_1, \ldots, x_n) \equiv_A Q(x_1, \ldots, x_n)}$ – *равносильные на множестве* A *предикаты,*

$\boldsymbol{P(x_1, \ldots, x_n) \equiv Q(x_1, \ldots, x_n)}$ – *равносильные на множестве* $D(P) = D(Q)$ *предикаты,*

$\Rightarrow$ – *знак логического следования для предикатов,* $\boldsymbol{P(x) \Rightarrow Q(x)}$ – *предикат* $Q(x)$ *является логическим следствием предиката* $P(x)$ *(т.е.* $\forall x \; P(x) \to Q(x)$*),*

$\Leftrightarrow$ – *знак логической равносильности предикатов,* $\boldsymbol{P(x) \Leftrightarrow Q(x)}$ – *предикаты* $P(x)$ *и* $Q(x)$ *с одинаковыми областями определения равносильны (т.е.* $\forall x \in D(P)\ P(x) \leftrightarrow Q(x)$*),*

$\boldsymbol{P^{(s)}(\_\ , \dots , \_\ )}$ – *предикатный символ от* s *переменных,*

$\mathcal{J} = (M, a_1 = \alpha_1 , \dots , a_m = \alpha_m , \ x_1 = o_1 , \dots , \ x_n = o_n , \ \mathcal{P}_1^{(k_1)}(\_ ,..., \_), \dots , \mathcal{P}_s^{(k_s)}(\_ ,..., \_))$ – интерпретация множества формул исчисления предикатов,

$\bigvee\limits_{i_1 < \dots < i_s} (y_{i_1} \wedge \dots \wedge y_{i_s})$, $\bigvee\limits_{i_1 < \dots < i_s} (x_{i_1}^{\varepsilon_{i_1}} \wedge \dots \wedge x_{i_s}^{\varepsilon_{i_s}})$ – *дизъюнктивная форма,*

$\bigwedge\limits_{i_1 < \dots < i_s} (y_{i_1} \vee \dots \vee y_{i_s})$, $\bigwedge\limits_{i_1 < \dots < i_s} (x_{i_1}^{\varepsilon_{i_1}} \vee \dots \vee x_{i_s}^{\varepsilon_{i_s}})$ – *конъюнктивная форма,*

$\sum\limits_{k=0}^{n} \oplus \sum\limits_{1 \le i_1 < \dots < i_k \le n} x_{i_1} \otimes \dots \otimes x_{i_k} \oplus \varepsilon$ – *полином (многочлен) Жегалкина,*

$\left(\overline{\varepsilon_1 \dots \varepsilon_n}\right)_2$ – *двоичное число с двоичными цифрами* $\varepsilon_1 , \dots , \varepsilon_n$,

$\boldsymbol{\{a_1 ; \dots a_n\}}$ – *конечное множество из* n *элементов,*

$\boldsymbol{\{ x \in A \mid P(x) = 1\}}$ – *множество всех элементов множества* A*, удовлетворяющих характеристическому свойству* P*,*

$\in$ – *знак принадлежности элемента множеству,* $\boldsymbol{a \in A}$, $\boldsymbol{a \notin A}$ – *элемент* a *принадлежит (не принадлежит) множеству* A*,*

$\cap$ – *знак пересечения множеств,* $\boldsymbol{A_1 \cap \dots \cap A_n}$ – *пересечение множеств* $A_1 , \dots , A_n$,

$\cup$ – *знак объединения,* $\boldsymbol{A_1 \cup \dots \cup A_n}$ – *объединение множеств* $A_1 , \dots , A_n$,

$\boldsymbol{\cap\{C \mid C \in A\}}$, $\bigcap\limits_{C \in A} C$ – *пересеченение по множеству* A*,*

$\boldsymbol{\cup\{C \mid C \in A\}}$, $\bigcup\limits_{C \in A} C$ – *объединение по множеству* A*,*

$\setminus$ – *знак разности множеств,* $\boldsymbol{A \setminus B}$ – *разность множеств* A *и* B*,*

$\subseteq$ – *знак включения,* $\boldsymbol{A \subseteq B}$ – A *является подмножеством в* B *(*A *содержится в* B*),*

$\varnothing$ – *пустое множество,*

$\mathcal{B}(A)$ – *булеан множества* A *(множество всех подмножеств множества* A*),*

$\boldsymbol{(a ; b)}$ – *упорядоченная пара,* $\boldsymbol{(a_1 ; \dots ; a_n)}$ – *упорядоченная* n*-ка,*

$\times$ – *знак прямого произведения множеств,* $\boldsymbol{A_1 \times \dots \times A_n}$ – *прямое (декартово) произведение мжеств* $A_1 , \dots , A_n$,

$\forall$, $\exists$ – *кванторы всеобщности и существования,*

$\exists!$ – *знак существования и единственности,*

$\vdash \boldsymbol{A}$ – *формула* A *доказуема в ИВ или ИП,*

ИВ *– исчисление высказываний,*

ИП – *исчисление предикатов,*

ДФ – *дизъюнктивная форма,*

КФ – *конъюнктивная форма,*

РКС – *релейно контактная схема,*

СБИС – *сверхбольшая интегральная схема,*

ПФ – *приведённая форма формулы ИП,*

ПНФ – *предварённая нормальная форма формулы ИП,*

ППНФ – *предварённая приведённая нормальная форма формулы ИП,*

МР – *правило вывода* modus ponens*,*

ч. у. м. – *частично упорядоченное множество,*

в. у. м. – *вполне упорядоченное множество.*

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Т

У

Ф

Ц

Ч

Ш

Э

Я

Алексей Игоревич Валицкас

КОНСПЕКТ ЛЕКЦИЙ ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ

Учебно-методическое пособие

Лицензия на издательскую деятельность
ЛР № 040287 от 25 июля 1997 г.

Подписано в печать ___. ___. 2010 г.
Формат 60×84 1/16. Усл. печ. л. 9 Тираж 300 экз. Заказ № _____

Отпечатано в типографии редакционно-издательского отдела ГОУ ВПО
“Тобольская государственная социально-педагогическая академия им. Д.И. Менделеева”
626150, Тобольск, ул. Знаменского, 58