Министерство образования и науки Российской федерации
Южно-Российский государственный университет сервиса

С. Ю. Кулабухов

Дискретная математика

(конспект лекций)

Для студентов механико-радиотехнического факультета всех форм обучения

Шахты
2006

Содержание

От автора

Главы конспекта разбиты на параграфы, соответствующие, как правило, одной лекции. Структура каждого параграфа такова: ключевые моменты параграфа, краткая теория, новые термины, контрольные вопросы, упражнения. Контрольные вопросы содержат задания, рассчитанные, как правило, на устное их решение в случае усвоения основ краткой теории. Упражнения носят более глубокий характер и рассчитаны как на закрепление прочитанного материала, так и на приобретение определенных вычислительных навыков.

Кроме того автор заранее благодарит читателей за найденные в тексте и доведенные до его сведения неточности, а также за различные замечания и пожелания, связанные с данным изданием.

Глава I

Введение в теорию множеств

§ 1. Основные понятия теории множеств

Множество, элемент, принадлежит. Равенство множеств. Пустое множество. Конечные и бесконечные множества. Способы задания множеств. Включение множеств. Операции над множествами и их свойства. Нахождение числа элементов объединения множеств. Алгебры подмножеств.

1.1. Первичные понятия. Такие понятия, как "множество", "элемент", "принадлежит" являются первичными, неопределяемыми понятиями теории множеств. Смысл их разъясняется при помощи различного рода метаматематических (внематематических) описаний. Г. Кантор (1845–1918), основатель интуитивной теории множеств, предложил следующее очень меткое описание этого понятия: "Множество есть многое, мыслимое нами как единое целое". Множества принято обозначать большими латинскими буквами, элементы множеств — малыми латинскими буквами. $\in$ — символ для обозначения принадлежности того или иного элемента данному множеству.

1.2. Равенство множеств. Пустое множество.

Определение 1 (равенства множеств). *Два множества считаются равными в том и только в том случае, когда они состоят из одних и тех же элементов.*

Определение 2 (пустого множества). *Всякое множество, не содержащее ни одного элемента, называется пустым.*

Теорема 1 (единственность пустого множества). *Существует единственное пустое множество. Оно обозначается символом* $\varnothing$.

Доказательство. 1. Существование. Множество всех вещественных корней уравнения $x^2 = -1$ являются, очевидно, пустым.

2. Единственность. Пусть A и B пустые множества. Если бы они не совпадали, то состояли бы не из одних и тех же элементов. То есть, в одном из этих множеств нашелся бы элемент, которого нет в другом. Однако, наличие элемента в каком-либо из множеств A или B противоречит определению пустого множества. Таким образом, из $A = B$ следует существование не более одного пустого множества. ■

1.3. Способы задания множеств. Множество, которое содержит конечное (бесконечное) число элементов, называется *конечным (бесконечным)*. $\varnothing$ считается конечным множеством.

Определение 1. *Будем считать множество заданным, если для любого предмета (элемента) есть принципиальная возможность установить, является он элементом этого множества или нет.*

Задание множеств перечислением. Для некоторых конечных множеств употребляется способ задания перечислением всех элементов этих множеств. При этом перечисляемые элементы

заключаются в фигурные скобки. Например, $\{27, 3, \Phi, \Delta\}$; $\{\Phi\}$; $\{\{\Phi\}\}$; $\{\Phi, \{\Phi\}\}$ и т. д. Понятно, что не все множества реально можно задать перечислением и, даже, не все конечные.

Задание множеств указанием характеристического свойства. Пусть некоторое множество U уже задано и P — некоторое свойство, которым какие-то элементы U обладают, а какие-то не обладают. Таким образом, задано множество M всех тех и только тех элементов из U, которые обладают свойством P. Свойство P называется *характеристическим* для множества M, а такой способ задания множеств — *при помощи* (или *указанием*) характеристического свойства. В общем виде приняты такие обозначения:

$$M = \{x \mid x \in U \text{ и } P(x)\} \text{ или } M = \{x \in U \mid P(x)\},$$

где запись $P(x)$ означает, что элемент x обладает свойством P. Читается "множество всех x из U, обладающих свойством P" или более кратко "множество всех x из U таких, что $P(x)$". Если из контекста ясно о каком множестве U идет речь, то пишут:

$$M = \{x \mid P(x)\}.$$

Пример 1. Пусть N — множество всех натуральных чисел и множество

$$M = \{x \in N \mid x^3 - 5x^2 + 6x = 0\}.$$

Понятно, что M в данном случае можно задать и перечислением: $M = \{2, 3\}$.

Словесный способ задания множеств — это, в действительности, есть либо перечисление, либо словесное описание характеристического свойства.

1.4. Отношение включения множеств.

Определение 1. *Говорят, что множество A включается во множество B (содержится во множестве B): $A \subseteq B$, если все элементы множества A являются элементами и множества B.*

Если же $A \subseteq B$ и $A \neq B$, то говорят, что множество A строго включается в B: $A \subset B$.

Если $A \subseteq B$, то говорят также, что A — *подмножество* множества B, а если $A \subset B$, то говорят, что A *собственное* подмножество множества B.

Теорема 1. *Пустое множество является подмножеством любого множества и собственным подмножеством любого непустого множества.*

Докажите самостоятельно.

1.5. Свойства отношения включения.

1. **Рефлексивность.** Для любого множества A:

   $A \subseteq A$.

2. **Транзитивность.** Для любых множеств A, B, C:

   если $A \subseteq B$ и $B \subseteq C$, то $A \subseteq C$.

3. **Антисимметричность.** Для любых множеств A, B:

   если $A \subseteq B$ и $B \subseteq A$, то $A = B$.

На антисимметричном свойстве отношения включения основано доказательство равенства множеств. Для доказательства того, что $A = B$ доказывают два включения $A \subseteq B$ и $B \subseteq A$.

Доказательство свойств 1–3 проводится на основании определения отношения включения. Сделайте это самостоятельно.

1.6. Операции над множествами.

Определение 1. *Пусть A, B, C — некоторые множества, причем $A \subseteq C$. При помощи характеристического свойства определим еще четыре множества:*

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\},$$
$$A \cup B = \{x \mid x \in A \text{ или } x \in B\},$$
$$A \setminus B = \{x \mid x \in A \text{ и } x \notin B\},$$
$$\overline{A}_C = C \setminus A.$$

Можно сказать, что определение этих четырех множеств определяет в действительности операции над множествами A, B, C, которые мы обозначили символами $\cap$, $\cup$, $\setminus$, $\overline{\ }$. Операции эти называются соответственно пересечение, объединение, разность (вычитание) и дополнение.

С целью наглядности принято иногда изображать множества частями плоскости. Пользуясь этим, проиллюстрируем введенные выше операции (рис. 1).

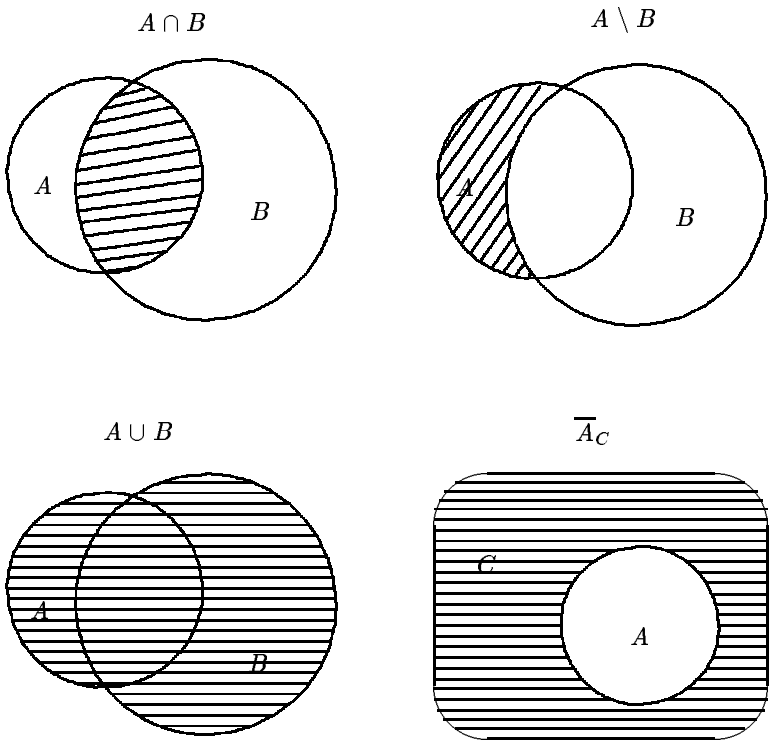

Рис. 1: Операции над множествами $\cap$, $\cup$, $\setminus$ и $\overline{\ }$.

1.7. Свойства операций над множествами.

Теорема 1. *Пусть A, B, C — произвольные подмножества некоторого фиксированного множества U, которое назовем универсальным.*

Справедливы следующие соотношения:

1. *Закон двойного дополнения:*
   $\overline{\overline{A}} = A$.
2. *Идемпотентность операций $\cap$ и $\cup$:*
   $A \cap A = A$,
   $A \cup A = A$.

3. *Коммутативность операций* $\cap$ *и* $\cup$*:*
$A \cap B = B \cap A,$
$A \cup B = B \cup A.$

4. *Ассоциативность операций* $\cap$ *и* $\cup$*:*
$A \cap (B \cap C) = (A \cap B) \cap C,$
$A \cup (B \cup C) = (A \cup B) \cup C.$

5. *Дистрибутивные законы каждой из операций* $\cap$ *и* $\cup$ *относительно другой:*
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

6. *Законы поглощения:*
$A \cap (A \cup B) = A,$
$A \cup (A \cap B) = A.$

7. *Законы де-Моргана:*
$\overline{A \cap B} = \overline{A} \cup \overline{B},$
$\overline{A \cup B} = \overline{A} \cap \overline{B}.$

8. $A \cap \overline{A} = \varnothing,$
$A \cup \overline{A} = U.$

9. $A \cap U = A, \quad A \cap \varnothing = \varnothing,$
$A \cup U = U, \quad A \cup \varnothing = A,$
$\overline{U} = \varnothing, \qquad \overline{\varnothing} = U.$

Свойства 2–4, 8, 9 следуют непосредственно из соответствующих определений. Свойства 1, 5–7 доказываются стандартным методом на основе антисимметричного свойства отношения включения. Проведите самостоятельно эти рассуждения.

1.8. Количество элементов объединения множеств. Будем обозначать через $|A|$ количество элементов конечного множества A. Число $|A|$ называют также *мощностью* множества A, а множества содержащие одинаковое количество элементов — *равномощными*. Основная формула, которой пользуются при нахождении числа элементов объединения двух конечных множеств такова:

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{1}$$

Действительно, $|A|+|B|$ есть число, которое мы получим, перечислив все элементы множества A, а затем — все элементы множества B. Но в этом случае общие элементы (их число $|A \cap B|$) будут перечислены дважды, то есть

$$|A| + |B| = |A \cup B| + |A \cap B|.$$

Отсюда и получается равенство (1).

Установим теперь общую формулу для нахождения числа элементов объединения нескольких множеств.

Теорема 1. *Если* $A_1, A_2, \ldots, A_n$ *— некоторые конечные множества, то*

$$\begin{aligned} &|A_1 \cup A_2 \cup \ldots \cup A_n| = (|A_1| + |A_2| + \ldots + |A_n|) - \\ &-(|A_1 \cap A_2| + |A_1 \cap A_3| + \ldots + |A_{n-1} \cap A_n|) + \\ &+(|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \ldots \\ &\ldots + |A_{n-2} \cap A_{n-1} \cap A_n|) - \ldots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|. \end{aligned} \tag{2}$$

Доказательство. Правая часть равенства (2) является суммой n слагаемых, k-е по порядку слагаемое имеет вид

$$(-1)^{k-1}S_k(A_1, A_2, \ldots, A_n),$$

где $S_k(A_1, A_2, \ldots, A_n)$ есть сумма чисел $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|$ по всем возможным пересечениям ровно k разных множеств из множеств $A_1, A_2, \ldots, A_n$.

Из формулы (1) следует, что формула (2) справедлива для двух множеств. Предположим, что она справедлива для $n-1$ множества, и покажем, что она выполняется и для n множеств, то есть проведем доказательство методом математической индукции.

По предположению

$$\begin{aligned}
&|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2 \cup A_3 \cup \ldots \cup A_n| - \\
&-|(A_1 \cap A_2) \cup (A_1 \cap A_3) \cup \ldots \cup (A_1 \cap A_n)| = \\
&= |A_1| + \big(S_1(A_2, A_3, \ldots, A_n) - S_2(A_2, A_3, \ldots, A_n) + \ldots \\
&\ldots + (-1)^{n-2}S_{n-1}(A_2, A_3, \ldots, A_n)\big) - \\
&-\big(S_1(A_1 \cap A_2, A_1 \cap A_3, \ldots, A_1 \cup A_n) - \\
&-S_2(A_1 \cap A_2, A_1 \cap A_3, \ldots, A_1 \cap A_n) + \ldots \\
&\ldots + (-1)^{n-2}S_{n-1}(A_1 \cap A_2, A_1 \cap A_3, \ldots, A_1 \cap A_n)\big)
\end{aligned}$$

Для того, чтобы отсюда получить формулу (2), остается принять во внимание, что

$$\begin{aligned}
&|A_1| + S_1(A_2, A_3, \ldots, A_n) = S_1(A_1, A_2, \ldots, A_n), \\
&S_2(A_2, A_3, \ldots, A_n) + S_1(A_1 \cap A_2, A_1 \cap A_3, \ldots, A_1 \cap A_n) = \\
&\qquad = S_2(A_1, A_2, \ldots, A_n), \\
&S_k(A_2, A_3, \ldots, A_n) + S_{k-1}(A_1 \cap A_2, A_1 \cap A_3, \ldots, A_1 \cap A_n) = \\
&\qquad = S_k(A_1, A_2, \ldots, A_n), \\
&S_{n-1}(A_1 \cap A_2, A_1 \cap A_3, \ldots, A_1 \cap A_n) = S_n(A_1, A_2, \ldots, A_n).
\end{aligned}$$

Теорема доказана. ■

Задача 1. Каждый ученик класса — либо девочка, либо блондин, либо любит математику. В классе 20 девочек, из них 12 блондинок, и одна блондинка любит математику. Всего в классе 24 ученика-блондина, математику из них любят 12, а всего учеников (мальчиков и девочек), которые любят математику, 17, из них 6 девочек. Сколько учеников в данном классе?

Решение. Если A — множество девочек, B — блондинов, C — учеников, которые любят математику, то $|A \cup B \cup C|$ — искомое число. $A \cap B$ — множество блондинок, $A \cap C$ — множество девочек, которые любят математику, $A \cap B \cap C$ — множество блондинок, которые любят математику. Тогда

$$\begin{aligned}
|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + \\
+|A \cap B \cap C| = 20 + 24 + 17 - (12 + 6 + 12) + 1 = 32.
\end{aligned}$$

Таким образом, в классе 32 ученика. ■

1.9. Алгебры множеств. Пусть U — некоторое фиксированное множество. Обозначим через $\mathcal{B}(U)$ множество всех подмножеств множества U. Отметим, что результат применения операций над множествами к множествам из $\mathcal{B}(U)$ дает множества, принадлежащие также $\mathcal{B}(U)$. В этом случае говорят, что $\mathcal{B}(U)$ замкнуто относительно указанных выше операций, то есть $\mathcal{B}(U)$ образует алгебру относительно определенных ранее операций. Эта алгебра называется *булевой алгеброй подмножеств множества* U. Это название в честь английского математика и логика Джорджа Буля (1815–1864).

1.10. Новые термины. Множество, элемент, принадлежит, метаматематика, конечное множество, бесконечное множество, характеристическое свойство, отношение включения, подмножество, собственное подмножество, рефлексивность, транзитивность, антисимметричность. Пересечение, объединение, вычитание множеств, дополнение множества. Законы: двойного дополнения, идемпотентности, коммутативности, ассоциативности, дистрибутивности, поглощения, де-Моргана. Мощность множества. Равномощные множества. Замкнутость относительно операции, булева алгебра множеств (подмножеств).

1.11. Контрольные вопросы.

1. Совпадают ли множества:
   (a) $\{1,2,3\}$ и $\{3,1,2\}$;
   (b) $\{1,2,3\}$ и $\{1,2,2,3,1\}$;
   (c) $\{1,2,3\}$ и $\{\{1\},2,3\}$;
   (d) $\varnothing$ и $\{\varnothing\}$.
2. Истинны ли следующие утверждения:
   (a) $\varnothing \in \{1,2,3\}$; $\varnothing \subseteq \{1,2,3\}$; $\varnothing \subset \{1,2,3\}$;
   (b) $\varnothing \in \{\varnothing,1,2\}$; $\varnothing \subseteq \{\varnothing,1,2\}$; $\varnothing \subset \{\varnothing,1,2\}$;
   (c) $\varnothing \in \{\{\varnothing\},1,2\}$; $\varnothing \subseteq \varnothing$; $\varnothing \subset \varnothing$.
3. Рефлексивно ли отношение $\in$?
4. Транзитивно ли отношение $\in$?
5. Пусть Z — универсальное множество всех целых чисел, Z_2 — множество всех четных целых чисел, $A = \{x \mid x < 10\}$. Опишите словесно множества: $\overline{Z_2}$, $\overline{A}$, $Z_2 \cap A$, $Z_2 \cup A$, $Z_2 \setminus A$, $A \setminus Z_2$, $\overline{Z_2 \cap A}$, $\overline{Z_2 \cup A}$, $\overline{Z_2 \setminus A}$, $\overline{A \setminus Z_2}$.
6. Обладают ли операции сложения, умножения и вычитания целых чисел свойствами идемпотентности, коммутативности и ассоциативности?
7. Дистрибутивна ли операция умножения целых чисел относительно сложения? Сложения целых чисел относительно умножения?
8. Запишите все элементы алгебры $\mathcal{B}(A)$ для множества
$$A = \{\{\varnothing\},\{1,2\},3\}.$$
9. В одном множестве 5 элементов, в другом — 6. Можно ли утверждать, что в объединении этих множеств 11 элементов? Приведите соответствующий пример.
10. В одном множестве 4 элемента, а в другом — 11. Можно ли утверждать, что в пересечении может оказаться 5?
11. Из десяти девочек 5^a класса 8 посещает музыкальную школу, а трое — Дом творчества. Как это может быть?
12. Из 35 учащихся в период летних каникул 17 съездили на экскурсию в Москву, а 19 — во Владивосток. Можно ли утверждать что экскурсии проходили в одно и то же время?

1.12. Упражнения.

1. Доказать, что для любых предметов a и b
$$\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\} \Longleftrightarrow a = c \text{ и } b = d.$$
2. Доказать истинность следующих утверждений для произвольных множеств A, B, C:

(a) $A \subseteq B$ и $B \subset C \Longrightarrow A \subset C$;

(b) $A \subset B$ и $B \subseteq C \Longrightarrow A \subset C$;

(c) $A \subset B$ и $B \subset C \Longrightarrow A \subset C$.

3. Выполните действия:

$$\varnothing \cap \{\varnothing\}, \quad \{\varnothing\} \cap \{\varnothing\}, \quad \{\varnothing, \{\varnothing\}\} \setminus \varnothing, \quad \{\varnothing, \{\varnothing\}\} \setminus \{\varnothing\}, \quad \{\varnothing, \{\varnothing\}\} \setminus \{\{\varnothing\}\}.$$

4. Изобразите на плоскости внутри некоторого ограниченного контуром множества U точек плоскости два пересекающихся, не совпадающих множества. Контуры, ограничивающие эти множества назовем *границами*. Всякую часть плоскости, ограниченную некоторой границей и такую, что внутри нее нет границ, назовем *государством*, а всю получившуюся картинку — *картой*. Охарактеризуйте каждое государство при помощи исходных множеств.

5. Та же задача при условии, что внутри U изображено 3 пересекающихся и попарно пересекающихся, но несовпадающих множества.

6. Пусть A и B — подмножества некоторого универсального множества U. Докажите, что следующие ниже условия (a)–(d) эквивалентны.

(a) $A \subseteq B$, (b) $\overline{B} \subseteq \overline{A}$, (c) $A \cup B = B$, (d) $A \cap B = A$.

7. Докажите соотношение $(A \cup B) \setminus B = A \setminus B$.

8. Докажите соотношение $A \cap (B \cup C) = A \setminus \big((A \setminus B) \cap (A \setminus C)\big)$.

9. Докажите, что $A \setminus B = \varnothing$ тогда и только тогда, когда $A \cap B = A$

10. — Сколько в вашем классе детей, — спросила мама свою дочь.

— А вот подсчитай, — сказала Лена.

— 17 ребят нашего класса спортсмены, 22 увлекаются математикой. Коля, Вася, Надя, Люда и Лариса любят спорт и математику. А один мальчик, Валера, ничем не интересуется.

Подсчитайте и вы количество ребят в классе Лены.

11. Из 27 учащихся 5^a класса 8 учащихся участвовали в танцевальных номерах на концерте, а 11 пели в хоре. 4 человека и пели и танцевали. Сколько учащихся 5^a класса не приняли участия в художественной самодеятельности?

12. Среди чисел от 1 до 100 — 50 делящихся на 2, 33 делящихся на 3, 17 нечетных делится на 3. Сколько чисел делится на 6? Сколько чисел не делится на 3? Сколько чисел не делится ни на 2, ни на 3?

13. Из 20 спортсменов 5 класса — 10 лыжников, 9 гимнастов и 11 легкоатлетов. 6 занимаются легкой атлетикой и гимнастикой, 7 — лыжами и легкой атлетикой, 6 — лыжами и гимнастикой. Всеми тремя видами спорта занимаются 5 спортсменов. Сколько учащихся занимаются только лыжами, только легкой атлетикой и только гимнастикой? Сколько учащихся занимаются другими видами спорта?

14. Из 29 учащихся 8 класса 18 учащихся не пожелали принять участие ни в математической, ни в химической, ни в физической олимпиаде. В математической олимпиаде приняли участие 8 учащихся, в физической — 4, в химической — 4, только в математической — 3, только в физической — 1, только в химической — 2. Во всех трех олимпиадах не принял участие никто. Могли ли проходить в одно и то же время математическая и химическая олимпиады? Химическая и физическая?

15. Из 100 студентов английский язык знают 28 студентов, немецкий — 30, французский — 42, английский и немецкий — 8, английский и французский — 10, немецкий и французский — 5, а все три языка знают 3 студента. Сколько студентов не знают ни одного из трех языков?

16. В кровопролитном бою не менее 70% воинов потеряли глаз, не менее 75% — ухо, не менее 80% — руку и не менее 85% — ногу. Оценить снизу число воинов, потерявших одновременно глаз, ухо, руку и ногу. (Льюис Кэрролл).

17. В классе учится n учеников, которые посещают 2^{n-1} кружков. Известно, что любые два разных кружка имеют различный состав и любые три кружка имеют хотя бы одного общего участника. Докажите, что существует в точности один ученик, который посещает все кружки.

§ 2. Соответствия, функции, отображения

Последовательности. Декартовы произведения. Соответствия. Графы соответствий. Обратное соответствие. Частичные функции и функции (отображения). Обратимые частичные функции и обратимые функции. Критерий обратимости функции (частичной функции). Классификация функций (= отображений).

2.1. Декартовы произведения.

Определение 1. *Пусть $a_1, a_2, \ldots, a_n$ — элементы некоторых множеств, $n \in N$. Определим индуктивно последовательность $(a_1, a_2, \ldots, a_n)$:*

при $n = 1$ $(a_1) = a_1$;

при $n = 2$ $(a_1, a_2) = \{a_1, \{a_1, a_2\}\}$;

при $n > 2$ $(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$.

Последовательность (a_1, a_2) называется парой или упорядоченной парой элементов a_1, a_2.

Теорема 1. *Две последовательности $\alpha = (a_1, a_2, \ldots, a_n)$ и $\beta = (b_1, b_2, \ldots, b_n)$ равны $\alpha = \beta$ тогда и только тогда, когда $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$.*

Доказательство проводится индукцией по n. Проведите его самостоятельно.

Определение 2. *Пусть $A_1, A_2, \ldots, A_n$, $n \in N$, — какие-то непустые множества. Их декартовым произведением $A_1 \times A_2 \times \ldots \times A_n$ называется множество:*

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

2.2. Соответствия.

Определение 1. *Всякое подмножество ϱ декартова произведения $A \times B$ непустого множества A на непустое множество B называется соответствием из множества A во множество B или отношением между множествами A и B*

По определению, соответствиями из A в B являются подмножества декартова произведения, поэтому $\varnothing$ и $A \times B$ также являются соответствиями, которые называются соответственно *пустым соответствием* (отношением) и *полным соответствием* (отношением).

Условимся элементы из множеств A и B изображать точками плоскости (*вершинами*), а пары (a, b) принадлежащие соответствию ϱ, стрелочками (*дугами*), начинающимися в a и оканчивающимися в b. Тогда всякое соответствие будет изображаться картинкой (*графом*), состоящей из вершин и соединяющих вершины дуг.

Пример 1. Зададим соответствия ϱ_1–ϱ_6 из множества $A = \{0, 1, 2, 3, 4\}$ в $B = \{5, 6, 7, 8, 9\}$.

$\varrho_1 = \{(1,5), (1,6), (2,6), (3,9), (4,9)\}$;

$\varrho_2 = \{(0,6), (2,6), (3,8), (4,9)\}$;

$\varrho_3 = \{(0,6), (1,7), (3,9), (4,8)\}$;

$\varrho_4 = \{(0,6), (1,6), (2,7), (3,7), (4,9)\}$;

$\varrho_5 = \{(0,5), (1,6), (2,7), (3,8), (4,9)\}$;

$\varrho_6 = \{(0,6), (1,7), (2,5), (3,8), (4,9)\}$;

На рис. 2–4 изображены графы этих соответствий.

Пусть ϱ — соответствие из A в B. Если $(a, b) \in \varrho$, то будем писать $b \in \varrho(a)$ или $a \in \varrho^{-1}(b)$. Элемент b будем называть при этом *образом* элемента a при соответствии ϱ а a — *прообразом* элемента b при соответствии ϱ. Положим для $a \in A$ и $b \in B$:

$$\varrho(a) = \{y \mid y \in B \text{ и } (a, y) \in \varrho\};$$
$$\varrho^{-1}(b) = \{x \mid x \in A \text{ и } b \in \varrho(x)\}.$$

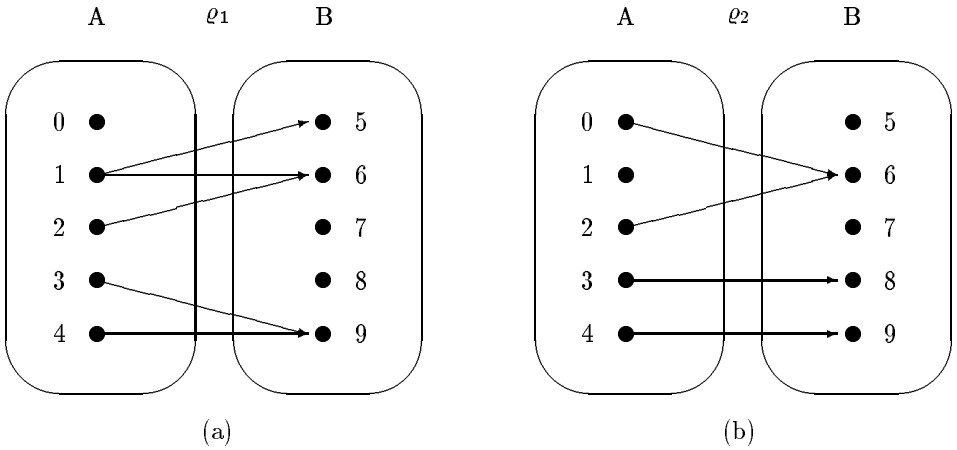

Рис. 2: Соответствия из A в B.

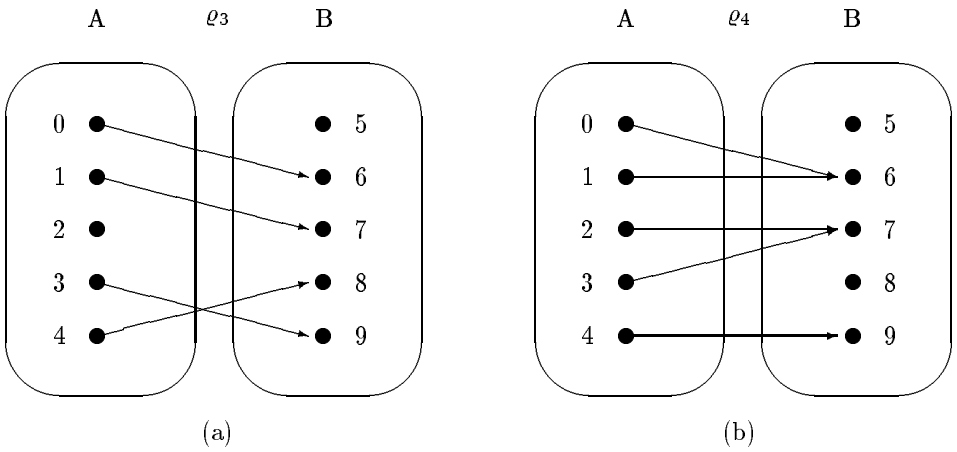

Рис. 3: Соответствия из A в B.

Множество $\varrho(a)$ называется *полным образом* элемента a, а $\varrho^{-1}(b)$ — *полным прообразом* элемента b при соответствии ϱ. Положим также:

$$\mathfrak{X}_\varrho = \{x \mid x \in A \text{ и } \varrho(x) \neq \varnothing\},$$
$$\mathfrak{Y}_\varrho = \{y \mid y \in B \text{ и } \varrho^{-1}(y) \neq \varnothing\}.$$

$\mathfrak{X}_\varrho$ называется *областью определения* соответствия ϱ, а $\mathfrak{Y}_\varrho$ — *областью значений* соответствия ϱ.

Пример 2. $\varrho_1(0) = \varnothing$; $\varrho_1(1) = \{5, 6\}$; $\varrho_1(2) = \{6\}$; $\varrho_1(3) = \{9\}$; $\varrho_1(4) = \{9\}$.
$\varrho_1^{-1}(5) = \{1\}$; $\varrho_1^{-1}(6) = \{1, 2\}$; $\varrho_1^{-1}(7) = \varnothing$; $\varrho_1^{-1}(8) = \varnothing$; $\varrho_1^{-1}(9) = \{3, 4\}$.
$\mathfrak{X}_{\varrho_1} = \{1, 2, 3, 4\}$; $\mathfrak{Y}_{\varrho_1} = \{5, 6, 9\}$.

2.3. Обратное соответствие.

Определение 1. *Пусть ϱ — соответствие из A в B. Положим:*

$$\varrho^{-1} = \{(b, a) \mid (a, b) \in \varrho\}.$$

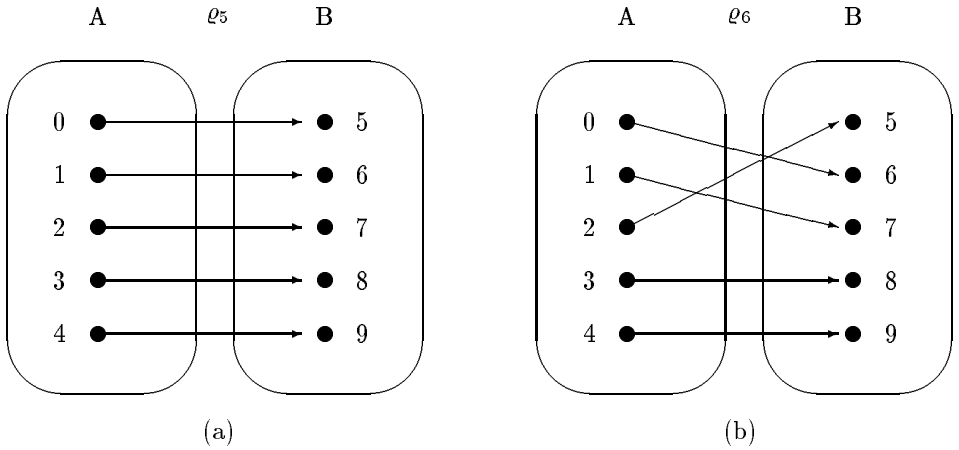

Рис. 4: Соответствия из A в B.

ϱ^{-1} называется обратным для соответствия ϱ. Понятно, что ϱ^{-1} — соответствие из B в A.

Пример 1. $\varrho_1^{-1} = \{(5,1),(6,1),(6,2),(9,3),(9,4)\}$ (см. рис. 5).

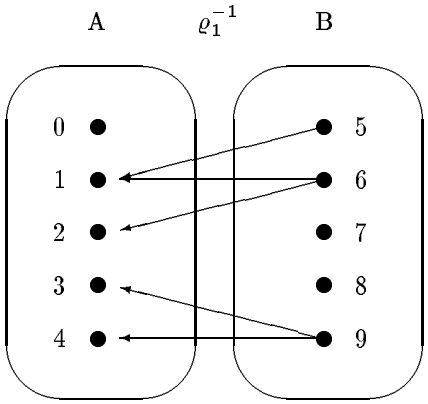

Рис. 5: Пример обратного соответствия.

Отметим, что для любого соответствия ϱ верны формулы

$$\mathfrak{X}_{\varrho^{-1}} = \mathfrak{Y}_{\varrho}, \quad \mathfrak{Y}_{\varrho^{-1}} = \mathfrak{X}_{\varrho}.$$

2.4. Частичные функции.

Определение 1. *Частичной функцией или однозначным соответствием из множества A во множество B называется такое соответствие из A в B, при котором каждому элементу множества A соответствует не более одного элемента множества B.*

Иными словами, отличительным признаком частичной функции f является тот факт, что для любого элемента $x \in A$ полный образ его $f(x)$ должен быть не более чем одноэлементное множество.

Пример 1. Легко убедиться, что из соответствий ϱ_1–ϱ_6 лишь ϱ_1 не является частичной функцией. Отметим, что пустое соответствие $\varnothing$ также является частичной функцией.

2.5. Обратная частичная функция.

Определение 1. *Пусть f — частичная функция из A в B. Если соответствие f^{-1} также является частичной функцией, то f^{-1} называется частичной функцией, обратной для f.*

Понятно, что обратная частичная функция для данной существует не всегда. Например, для ϱ_2, ϱ_4 обратных частичных функций не существует, а для $\varrho_3, \varrho_5, \varrho_6$ существуют. Легко понять, что для пустой частичной функции обратной частичной функцией будет она сама и, таким образом, пустая частичная функция обратима.

Определение 2. *Частичная функция f из A в B называется инъективной, если для произвольных $x, y \in A$ из того, что $f(x) = f(y)$ следует $x = y$.*

Пустая частичная функция, очевидно, инъективна.

Теорема 1. *Частичная функция f из A в B имеет обратную частичную функцию тогда и только тогда, когда f инъективна.*

Доказательство. 1. Пусть f имеет обратную частичную функцию. Если $f = \varnothing$, то f инъективна. Пусть f отлична от $\varnothing$ и соответствие f^{-1} является частичной функцией.

Пусть $x, y \in A$ и $f(x) = f(y)$. Для определенности пусть $f(x) = f(y) = z$. Это значит, что $(x, z), (y, z) \in f$. Тогда $(z, x), (z, y) \in f^{-1} \Longrightarrow x, y \in f^{-1}(z)$. Но f^{-1} — частичная функция, следовательно, образ элемента z не должен содержать более одного элемента и потому $x = y$.

2. Пусть теперь частичная функция f является инъективной. Если $f = \varnothing$, то f имеет обратную частичную функцию — $\varnothing$. Пусть f отлична от $\varnothing$, b — произвольный элемент множества B и $x, y \in f^{-1}(b)$. Если докажем, что $x = y$, то это будет означать, что каждому элементу из B соответствует при f^{-1} не более одного элемента множества A. Так как $x, y \in f^{-1}(b)$, то $(b, x), (b, y) \in f^{-1} \Longrightarrow (x, b), (y, b) \in f \Longrightarrow f(x) = b$ и $f(y) = b$, то есть $f(x) = f(y)$. Но тогда $x = y$. Теорема доказана. ■

2.6. Функции (отображения).

Определение 1. *Частичная функция f из A в B называется отображением множества A во множество B или функцией, заданной на A, со значениями в B, если область определения f совпадает с множеством A: $\mathfrak{X}_f = A$.*

Примерами отображений являются частичные функции ϱ_4–ϱ_6, см. рис. 2–4. Частичные функции ϱ_2, ϱ_3 отображениями множества A в B не являются.

Отметим, что всякая частичная функция является отображением своей области определения. Если отображение f есть инъективная частичная функция, то f называют *инъективным отображением.*

Если каждый элемент множества B имеет хотя бы один прообраз при отображении (функции) f, то есть если $\mathfrak{Y}_f = B$ то f называется *сюръективным* отображением (функцией) или отображением множества A *на* множество B.

Если же отображение f является и инъективным и сюръективным одновременно, то f называется *биективным* отображением множества A на множество B или *биекцией* A на B.

Отметим, что отображения ϱ_5, ϱ_6 (рис. 4) являются биекциями, а частичная функция ϱ_4 (рис. 3) не является ни инъективной, ни сюръективной.

Пример 1. Отображение $f\colon N \to N$ по правилу $f(n) = n + 1$ является инъективным, но не сюръективным.

Пример 2. Отображение $h\colon N \to N$ по правилу

$$h(n) = \begin{cases} 1, & \text{если } n = 1, \\ n - 1, & \text{если } n > 1, \end{cases}$$

является сюръективным, но не инъективным.

На конечных множествах инъективность отображения множества в себя влечет его сюръективность и обратно, сюръективность отображения множества на себя влечет его инъективность, см. упр. 7.

2.7. Обратимые отображения.

Определение 1. *Если соответствие f^{-1}, обратное для некоторого отображения $f\colon A \to B$ является отображением $f^{-1}\colon B \to A$, то f называется обратимым отображением, а f^{-1} — отображением, обратным для f.*

Отметим, что отображение f может быть обратимым как частичная функция и не быть обратимым как отображение. Примером служит отображение $f\colon N \to N$ по правилу $f(n) = n+1$. Пояснить!

Теорема 1. *Отображение $f\colon A \to B$ обратимо $\Longleftrightarrow$ f — биекция.*

Доказательство. 1. Пусть f — обратимо как отображение. Тогда f обратима как частичная функция и по теореме 2.5.1 f — инъективна. Пусть $b \in B$. Так как f^{-1} — отображение B в A, то для b есть некоторый образ $a \in A\colon f^{-1}(b) = a \Longrightarrow f(a) = b \Longrightarrow$ все элементы из B имеют непустые прообразы при отображении f множества A в $B \Longrightarrow f$ — биекция.

2. Пусть f — биекция. Необходимо доказать обратимость f, то есть что f^{-1} — отображение. Докажите самостоятельно. ■

2.8. Новые термины. Последовательность. Упорядоченная пара. Декартово произведение множеств. Соответствие из множества A во множество B. Пустое соответствие. Полное соответствие. Граф соответствия. Вершины и дуги графа. Образы и прообразы элементов при данном соответствии. Полный образ и полный прообраз. Область определения и область значений соответствия. Обратное соответствие. Частичная функция. Обратимая частичная функция. Функция (= отображение). Инъективные, сюръективные и биективные функции (отображения). Обратимые функции.

2.9. Контрольные вопросы.

1. Пусть A и B — конечные, соответственно m и n-элементные множества. Укажите количество элементов во множестве $A \times B$. Сколько существует соответствий из A в B? Из B в A?
2. Можно ли утверждать, что $A \times B = B \times A$?
3. Если известно, что $A \times B = B \times A$, то что можно сказать о множествах A и B?
4. Для каждого из соответствий ϱ_1–ϱ_6 из п. I.2.2. найти полный образ каждого элемента из A; полный прообраз каждого элемента из B; область определения и область значений.
5. Какие из соответствий ϱ_1–ϱ_6 являются функциями (частичными функциями)? Инъективными функциями (частичными функциями)? сюръективными функциями (частичными функциями)? Обратимыми функциями (частичными функциями)?
6. Пусть A и B произвольные конечные, соответственно m и n-элементные множества. Каково должно быть соотношения между числами m и n, чтобы существовало сюръективное отображение A на B (B на A).
7. Для каждого из соответствий ϱ_1–ϱ_6 укажите обратное соответствие и его граф.
8. Какие из соответствий ϱ_1–ϱ_6 являются отображениями множества A в B? Отображениями множества A на B? Биекциями A на B?
9. Что вы можете сказать по поводу утверждения: “Всякая частичная функция из множества A во множество B является отображением своей области определения на свою область значений”?
10. Ответить на вопросы заданий 4–7 для пустого и полного соответствий из A в B.

2.10. Упражнения.

1. Пусть $A = \{1, 2\}$, $B = \{3, 4, 5\}$. Изобразите графами все отображения A в B и B в A. Подсчитайте количество всех инъективных отображений A в B (B в A). Всех сюръективных отображений A в B (B в A).

2. Пусть A и B те же, что и в 1. Изобразите графами все частичные функции A в B и B в A. Подсчитайте количество всех частичных функций, всех инъективных частичных функций A в B (B в A). Всех сюръективных частичных функций A в B (B в A).

3. Пусть A и B произвольные конечные, соответственно m и n-элементные множества. Подсчитайте количество всех отображений A в B и B в A. Всех инъективных отображений A в B (B в A). Подсчитайте количество всех частичных функций, всех инъективных частичных функций из A в B (B в A).

4. Докажите, что для произвольного соответствия f выполняется равенство: $(f^{-1})^{-1} = f$.

5. Если функция (частичная функция) обратима, то и обратная ей функция (частичная функция) обратима. Доказать.

6. Приведите пример, показывающий, что частичная функция в качестве обратного соответствия может иметь функцию (отображение).

7. Доказать, что инъективное отображение конечного множества в себя является сюръективным и обратно, сюръективное отображение конечного множества на себя является инъективным.

§ 3. Суперпозиция соответствий. Преобразования

Полные образы и полные прообразы множеств при данном соответствии. Суперпозиция (произведение) соответствий. Ассоциативность суперпозиции соответствий. Суперпозиция функций. Свойства тождественной и обратной функций. Преобразования. Преобразования конечных множеств. Подстановки.

3.1. Полные образы и прообразы множеств. Пусть $f \subseteq A \times B$, $A_1 \subseteq A$ и $B_1 \subseteq B$. Обозначим:

$$f(A_1) = \bigcup_{a \in A_1} f(a),$$
$$f^{-1}(B_1) = \bigcup_{b \in B_1} f^{-1}(b).$$

$f(A_1)$ называется *полным образом* множества A_1 при соответствии f, а $f^{-1}(B_1)$ — *полным прообразом* множества B_1 при соответствии f.

Пример 1. Пусть $f \subseteq R \times R$ определяется формулой $f(x) = x^2$. Тогда

$$f([0,1]) = [0,1], \quad f^{-1}([0,1]) = [-1,1], \quad f^{-1}([-1,0]) = \{0\},$$
$$f([-1,0]) = [0,1], \quad f^{-1}([-1,1]) = [-1,1], \quad f^{-1}([-2,-1]) = \varnothing.$$

Убедитесь в этом.

Теорема 1. *Два соответствия f и g из A в B равны тогда и только тогда, когда для произвольного элемента $a \in A$ $f(a) = g(a)$.*

Доказательство. Если $f = g$, то совершенно очевидно, что для любого $a \in A$ $f(a) = g(a)$. Пусть теперь для любого $a \in A$ $f(a) = g(a)$ и $(x, y) \in f$. Имеем:

$$y \in f(x) \text{ и } f(x) = g(x) \Longrightarrow y \in g(x) \Longrightarrow (x, y) \in g \Longrightarrow f \subseteq g.$$

Аналогично доказывается, что и $g \subseteq f$. Докажите это. ■

3.2. Суперпозиция соответствий.

Определение 1. *Пусть $f \subseteq A \times B$ и $g \subseteq C \times D$ — пара соответствий. Определим их суперпозицию или произведение gf условиями 1–2.*

1. *$gf \subseteq A \times D$.*
2. *для любого $a \in A$ $gf(a) = g(f(a))$.*

Пусть $\varnothing_{A,B}$ — пустое соответствие из A в B и $f \subseteq C \times D$. Тогда:

$$\varnothing_{A,B} \cdot f = \varnothing_{C,B},$$
$$f \cdot \varnothing_{A,B} = \varnothing_{A,D}.$$

Пример 1. Пусть $f(x) = e^x$, $g(x) = \cos x$, $f, g \in R \times R$, где R — множество всех действительных чисел. Тогда:

$$(fg)(x) = f(g(x)) = f(\cos x) = e^{\cos x},$$
$$(gf)(x) = g(f(x)) = g(e^x) = \cos e^x.$$

Приведенный пример показывает, что для функций из R в R (от одной переменной) суперпозиция функций — это сложная функция (функция от функции).

Теорема 1. *Произведение gf двух непустых соответствий $f \subseteq A \times B$ и $g \subseteq C \times D$ является непустым соответствием тогда и только тогда, когда $\mathcal{Y}_f \cap \mathcal{X}_g \neq \varnothing$.*

Доказательство. 1. Пусть $gf \neq \varnothing$. Тогда найдется $a \in A$ такой, что $(gf)(a) = g(f(a)) \neq \varnothing$.

Пусть $d \in g(f(a))$, где $d \in D$. Следовательно, существует $b \in f(a)$ такой, что $d \in g(b)$. Это означает, что $b \in \mathfrak{X}_g$ и $b \in \mathfrak{Y}_f$, то есть $b \in \mathfrak{Y}_f \cap \mathfrak{X}_g \Longrightarrow \mathfrak{Y}_f \cap \mathfrak{X}_g \neq \varnothing$.

2. Пусть $\mathfrak{Y}_f \cap \mathfrak{X}_g \neq \varnothing$ и пусть $c \in \mathfrak{Y}_f \cap \mathfrak{X}_g$. Тогда: $c \in \mathfrak{Y}_f$ и $c \in \mathfrak{X}_g \Longrightarrow c \in f(a)$ для некоторого $a \in A$ и $d \in g(c)$ для некоторого $d \in D$. Но так как $c \in f(a)$, то $g(c) \subseteq g(f(a))$ и потому из того, что $d \in g(c)$ следует $d \in g(f(a)) = (gf)(a)$. Так что: $(gf)(a) \neq \varnothing \Longrightarrow gf$ — непустое соответствие. ■

3.3. Ассоциативность суперпозиции соответствий.

Теорема 1. *Произведение соответствий ассоциативно.*

Доказательство. Пусть $f \subseteq A \times B$, $g \subseteq C \times D$, $h \subseteq E \times F$. Тогда:

$$(h(gf))(a) = h((gf)(a)) = h(g(f(a))) = (hg)(f(a)) = ((hg)f)(a) \Longrightarrow h(gf) = (hg)f.$$

Приведите более подробные пояснения к этому доказательству. ■

3.4. Суперпозиция функций.

Теорема 1. *Пусть $f\colon A \to B$ и $g\colon B \to C$ — пара функций. Тогда:*

1. *gf — функция из A в C.*
2. *Если f и g инъективны, то и gf инъективна.*
3. *Если f и g сюръективны, то и gf сюръективна.*
4. *Если f и g — биекции, то и gf — биекция.*

Доказательство. 1. Пусть a — произвольный элемент из A. Так как f — функция на A, то $f(a)$ — одноэлементное множество и потому можно считать, что $f(a) \in B$. g — функция на B и потому $g(f(a))$ — одноэлементное множество. Но $g(f(a)) = (gf)(a)$ и, таким образом, $(gf)(a)$ — одноэлементное множество. В силу произвольности a можно сделать заключение о том, что полный образ всякого элемента из A при соответствии (gf) есть в точности одноэлементное множество. Таким образом gf — функция из A в C.

2. Пусть $(gf)(x) = (gf)(y) \in C$. Тогда: $g(f(x)) = g(f(y)) \neq \varnothing \Longrightarrow f(x) = f(y) \neq \varnothing \Longrightarrow x = y \Longrightarrow gf$ — инъективна. Поясните это доказательство.

3. Пусть $c \in C$. Тогда существует $b \in B$ такой, что $g(b) = c$. В свою очередь для b существует $a \in A$ такой, что $f(a) = b$. Таким образом: $c = g(b) = g(f(a)) = (gf)(a) \Longrightarrow gf$ — сюръективная функция.

4. Следует из двух предыдущих пунктов. ■

3.5. Свойства тождественной и обратной функции. Пусть M — некоторое множество. Обозначим:

$$e_M = \{(a, a) \mid a \in M\}.$$

Очевидно, $e_M \subseteq M \times M$.

Теорема 1 (Свойства тождественной функции).

1. *e_M — биективная функция из M на M.*
2. *$(\forall a \in M)(e_M(a) = a)$.*
3. *Если $f \subseteq M \times K$, то $fe_M = f$.*
4. *Если $g \subseteq P \times M$, то $e_M g = g$.*

Доказательство. 1, 2 докажите самостоятельно.

3. Пусть x — произвольный элемент из M. Тогда:

$$(fe_M)(x) = f(e_M(x)) = f(x) \Longrightarrow fe_M = f.$$

4. Пусть y — произвольный элемент из P. Тогда:

$$(e_M g)(y) = e_M(g(y)) = g(y) \Longrightarrow e_M g = g. \blacksquare$$

Теорема 2 (Свойства обратной функции). *Если $f\colon A \to B$ — обратимая функция, то:*

1. $ff^{-1} = e_B$,
2. $f^{-1}f = e_A$.

Доказательство. По определению f^{-1} имеем:

$$f(x) = y \Longleftrightarrow f^{-1}(y) = x.$$

1. Пусть y — произвольный элемент из B.

$$(ff^{-1})(y) = f(f^{-1}(y)) = f(x) = y = e_B(y) \Longrightarrow ff^{-1} = e_B.$$

2. Пусть x — произвольный элемент из A.

$$(f^{-1}f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = e_A(x) \Longrightarrow f^{-1}f = e_A. \blacksquare$$

3.6. Преобразования.

Определение 1. *Всякое отображение f множества A в себя называется преобразованием множества A.*

Преобразование f называется инъективным (сюръективным, биективным, обратимым), если f является инъективным (сюръективным, биективным, обратимым) как отображение.

Теорема 1.

1. *Произведение двух преобразований множества A является преобразованием множества A.*
2. *Произведение двух инъективных (сюръективных, биективных) преобразований множества A есть инъективное (сюръективное, биективное) преобразование множества A.*
3. *Если f — обратимое преобразование A, то $ff^{-1} = f^{-1}f = e_A$.*
4. *Если f и g — обратимые преобразования множества A, то gf обратимое преобразование множества A, причем, $(gf)^{-1} = f^{-1}g^{-1}$.*

Доказательство. Утверждения 1, 2 являются частным случаем теоремы 3.4.1 при $A = B = C$. Утверждение 3 является частным случаем теоремы 3.5.2 о свойствах обратной функции при $A = B$.

4. Пусть z — произвольный элемент из A. Так как g — обратимое преобразование, то g — обратимая функция. По теореме 2.7.1, g — биекция. Следовательно, $g(y) = z$ для некоторого $y \in A$. f — тоже обратимая функция $\Longrightarrow$ f — биекция $\Longrightarrow$ $f(x) = y$ для некоторого $x \in A$. Тогда $f^{-1}(y) = x$ и $g^{-1}(z) = y$ и $(gf)(x) = g(f(x)) = g(y) = z \Longrightarrow (gf)^{-1}(z) = x$. С другой стороны

$$(f^{-1}g^{-1})(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x \Longrightarrow$$
$$(f^{-1}g^{-1})(z) = (gf)^{-1}(z) \Longrightarrow f^{-1}g^{-1} = (gf)^{-1}.$$

3.7. Преобразования конечных множеств. Пусть A — конечное множество, а f — преобразование множества A. Пусть $A = \{a_1, a_2, \ldots, a_n\}$. Условимся f записывать в виде:

$$f = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{bmatrix}$$

Запись преобразования f в таком виде будем называть *паростроч ной записью* f.

Пример 1. Приведем паростроч ные записи всех преобразований трехэлементного множества $\{1, 2, 3\}$.

$$e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad g_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad g_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix},$$

$$g_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad g_4 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \quad g_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix},$$

$$f_{11} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{bmatrix}, \quad f_{12} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \end{bmatrix}, \quad f_{13} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 2 \end{bmatrix},$$

$$f_{14} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 2 \end{bmatrix}, \quad f_{15} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{bmatrix}, \quad f_{16} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 3 \end{bmatrix},$$

$$f_{21} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 3 \end{bmatrix}, \quad f_{22} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \end{bmatrix}, \quad f_{23} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 1 \end{bmatrix},$$

$$f_{24} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{bmatrix}, \quad f_{25} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 3 \end{bmatrix}, \quad f_{26} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \end{bmatrix},$$

$$f_{31} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \end{bmatrix}, \quad f_{32} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{bmatrix}, \quad f_{33} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \end{bmatrix},$$

$$f_{34} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{bmatrix}, \quad f_{35} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{bmatrix}, \quad f_{36} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 2 \end{bmatrix},$$

$$h_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{bmatrix}, \quad h_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \end{bmatrix}, \quad h_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{bmatrix}.$$

3.8. Подстановки.

Определение 1. *Биективное преобразование конечного множества называется подстановкой этого множества.*

Пример 1. 1. На двухэлементном множестве можно задать лишь две подстановки:

$$\begin{bmatrix} a_1 & a_2 \\ a_1 & a_2 \end{bmatrix}, \quad \begin{bmatrix} a_1 & a_2 \\ a_2 & a_1 \end{bmatrix}.$$

2. На трехэлементном множестве можно задать 6 подстановок. Это подстановки e, g_1–g_5 примера 3.7.1.

Теорема 1. *Обратимые преобразования конечного множества A и только они являются подстановками множества A.*

Доказательство следует из теоремы 2.7.1.

3.9. Новые термины. Полные образы и полные прообразы множеств при соответствии, суперпозиция (произведение) соответствий. Преобразование множества. Инъективное (сюръективное, биективное, обратимое) преобразование множества. Парострочная запись. Подстановка.

3.10. Контрольные вопросы.

1. Что является полным образом при соответствии f области определения этого соответствия $\mathfrak{X}_f$?
2. Что является полным прообразом при соответствии f области значений этого соответствия $\mathfrak{Y}_f$?
3. Пусть $f\colon A \to B$, $A_1 \subseteq A$ и $|A_1| = n$, $|B| = m$. Что можно сказать о количестве элементов в $f(A_1)$? Тот же вопрос при условии, что f — инъективная функция?
4. Пусть $\varnothing_{A,B}$, $\varnothing_{C,D}$ — пустые соответствия из A в B и из C в D соответственно. Найдите их произведения.
5. Пусть $f \subseteq A \times B$. Верно ли, что $f^{-1}f(a) = a$? Каким должно быть f, чтобы для любого $a \in A$ $f^{-1}f(a) = a$?
6. Пусть $f \subseteq A \times B$. Подберите A, B и f так, чтобы выполнялись условия:
   1) для каждого $a \in A$ $ff^{-1}f(a) \neq B$;
   2) для каждого $a \in A$ $ff^{-1}f(a) = B$.
7. Запишите все преобразования двухэлементного множества в парострочном виде.

3.11. Упражнения.

1. Пусть $f = \sin x \subseteq R \times R$, где R — множество всех вещественных чисел. Найдите: $f(\frac{\pi}{6})$, $f^{-1}f(\frac{\pi}{6})$, $f^{-1}([0, \frac{1}{2}])$.
2. Пусть $f = \ln x$, $g = \sin x$, $h = x^3$. Найти: fg, gf, fh, hf, gh, hg, fgh, ghf, gfh.
3. “Научитесь” перемножать преобразования в парострочной записи.
4. Из преобразований трехэлементного множества выберите все *идемпотентные* преобразования, то есть такие преобразования f, что $ff = f$.
5. Приведите примеры преобразований f 4-элементного множества такие, что: $ff = f$ и $\mathfrak{Y}_f$ — двухэлементное множество. $\mathfrak{Y}_f$ — трехэлементное множество.
6. Выпишите все подстановки трехэлементного множества. Коммутативно ли умножение подстановок?
7. Пусть дана парострочная запись подстановки f n-элементного множества. Научитесь находить парострочную запись подстановки f^{-1}.
8. Найдите обратные подстановки для всех подстановок трехэлементного множества.
9. Подсчитайте количество подстановок 4-элементного множества, 5-элементного множества, n-элементного множества.
10. Суперпозиция частичных функций является частичной функцией. Доказать
11. Пусть $f \subseteq A \times B$ и $g \subseteq B \times C$. Покажите на примерах, что:
    (a) если f не является частичной функцией или g не является частичной функцией, то, вообще говоря, и gf не является частичной функцией.
    (b) если f не является функцией или g не является функцией, то, вообще говоря, и gf не является функцией.

12. Пусть $f\colon A \to B$ и $g\colon B \to C$ — пара функций. Покажите на примерах, что:

    (a) если f не инъективна или g не инъективна, то gf, вообще говоря, не инъективна.

    (b) если f не сюръективна или g не сюръективна, то gf, вообще говоря, не сюръективна.

    (c) если f не биективна или g не биективна, то gf, вообще говоря, не биективна.

§ 4. Отношения эквивалентности и разбиения на классы

Бинарные отношения. Эквивалентности. Классы эквивалентности. Фактормножество. Связь разбиений и фактормножеств. Кардинальные числа.

4.1. Бинарные отношения.

Определение 1 (бинарного отношения). *Всякое соответствие из множества A в себя называется бинарным отношением на множестве A.*

Таким образом бинарное отношение на множестве A — это всякое подмножество декартова произведения $A \times A$.

Определение 2. *Бинарное отношение ϱ на множестве A называется:*

1) рефлексивным, если для любого $a \in A$ пара $(a, a) \in \varrho$;

2) симметричным, если из того, что $(a, b) \in \varrho$ следует $(b, a) \in \varrho$;

3) транзитивным, если из того, что $(a, b) \in \varrho$ и $(b, c) \in \varrho$ следует $(a, c) \in \varrho$.

Определение 3 (эквивалентности). *Бинарное отношение на множестве A называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.*

Пример 1. $A = \{1, 2, 3\}$.

а) $\varrho_1 = \{(1,1), (3,3), (1,2)\}$ — транзитивно, но не рефлексивно и не симметрично.

б) $\varrho_2 = \{(1,1), (3,3), (2,2)\}$ — эквивалентность.

в) $\varrho_3 = \{(1,2), (2,1)\}$ — симметрично, но не рефлексивно и не транзитивно.

г) $\varrho_4 = \{(1,1), (3,3), (1,2), (2,1)\}$ — симметрично, но не рефлексивно и не транзитивно.

д) $\varrho_5 = \{(1,1)\}$ — транзитивно и симметрично, но не рефлексивно.

е) $\varrho_6 = \{(1,2)\}$ — транзитивно, но не симметрично и не рефлексивно.

4.2. Разбиения на классы.

Определение 1. *Пусть A — некоторое множество. Совокупность подмножеств*

$$\mathfrak{A} = \{A_1, A_2, \ldots\}$$

множества A называется разбиением множества A, если:

1) любые два различных подмножества не пересекаются;

2) объединение всех подмножеств совпадает с A.

Пример 1. $A = \{1, 2, 3\}$.

а) $\mathfrak{A}_1 = \{\{1\}, \{2\}, \{3\}\}$ — разбиение A.

б) $\mathfrak{A}_2 = \{\{1\}, \{2\}, \{1, 3\}\}$ — не разбиение.

в) $\mathfrak{A}_3 = \{\{1\}, \{2\}\}$ — не разбиение.

г) $\mathfrak{A}_4 = \{\{1, 2\}, \{3\}\}$ — разбиение.

д) $\mathfrak{A}_5 = \{1, \{2, 3\}\}$ — не разбиение.

е) $\mathfrak{A}_6 = \{1, 2, 3\}$ — не разбиение.

ж) $\mathfrak{A}_7 = \{\{1, 2, 3\}\}$ — разбиение.

4.3. Классы эквивалентности.

Определение 1. *Пусть A — некоторое множество, а ϱ — отношение эквивалентности на множестве A. Для каждого элемента $a \in A$ определим подмножество $\overline{a}$ множества A следующим образом:*

$$\overline{a} = \{x \mid x \in A \text{ и } (a, x) \in \varrho\}.$$

Подмножество $\overline{a}$ назовем классом эквивалентности множества A по ϱ, определяемое элементом a. Элемент a назовем представителем этого класса.

Иногда $\overline{a}$ будем обозначать $\overline{a}_\varrho$, чтобы явно указывать, что $\overline{a}$ является классом по ϱ.

Пример 1. Пусть $A = \{1, 2, 3\}$, $\varrho = \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$. Тогда $\overline{1} = \overline{3} = \{1, 3\}$, $\overline{2} = \{2\}$.

Теорема 1. *Пусть A — некоторое множество, ϱ — эквивалентность на A, а предметы a, b — элементы множества A.*

1. *Для любого $a \in A$, $a \in \overline{a}$. Таким образом представитель класса $\overline{a}$ ему принадлежит.*
2. *Если $b \in \overline{a}$, то $\overline{b} = \overline{a}$. Это означает, в частности, что каждый элемент класса $\overline{a}$ является его представителем.*
3. *$\overline{a} = \overline{b} \iff (a, b) \in \varrho$.*
4. *Два произвольных класса $\overline{a}$ и $\overline{b}$ либо не пересекаются либо совпадают.*

Доказательство. 1. Так как ϱ рефлексивно, то для произвольного элемента $a \in A$, $(a, a) \in \varrho$ и, поэтому, из определения класса $\overline{a}$ следует, что $a \in \overline{a}$.

2. Пусть $b \in \overline{a}$. Если $x \in \overline{b}$, то, по определению $\overline{b}$, $(b, x) \in \varrho$. С другой стороны, так как $b \in \overline{a}$, то $(a, b) \in \varrho$. Из транзитивности ϱ следует, что $(a, x) \in \varrho$ и, следовательно, $x \in \overline{a}$. Таким образом, $\overline{b} \subseteq \overline{a}$.

Если $y \in \overline{a}$, то $(a, y) \in \varrho$. Так как $(a, b) \in \varrho$, то из симметричности ϱ следует, что $(b, a) \in \varrho$. Тогда $(b, y) \in \varrho$, то есть $y \in \overline{b}$. Таким образом, $\overline{a} \subseteq \overline{b}$. Итак, $\overline{a} = \overline{b}$.

3. Из п. 1 теоремы следует, что $b \in \overline{b}$. Из $\overline{a} = \overline{b}$ и $b \in \overline{b}$, следует, что $(a, b) \in \varrho$, по определению класса $\overline{a}$.

Пусть $(a, b) \in \varrho$. Тогда, если $x \in \overline{a}$, то $(a, x) \in \varrho$. Из симметричности ϱ следует, что $(b, a) \in \varrho$. Значит $(b, x) \in \varrho$ и, следовательно, $x \in \overline{b}$, то есть $\overline{a} \subseteq \overline{b}$. Аналогично доказывается, что $\overline{b} \subseteq \overline{a}$.

4. Пусть $\overline{a} \cap \overline{b} \neq \varnothing$ и $x \in \overline{a} \cap \overline{b}$. Тогда $x \in \overline{a}$ и $x \in \overline{b}$, следовательно, по определению классов $\overline{a}$ и $\overline{b}$, $(a, x) \in \varrho$ и $(b, x) \in \varrho$. Тогда $(a, b) \in \varrho$ и по п. 3 этой теоремы $\overline{a} = \overline{b}$. ■

Заметим, что из п. 1 только что доказанной теоремы следует, что каждый класс эквивалентности непуст.

4.4. Фактормножество.

Определение 1. *Пусть A — некоторое множество, а ϱ — эквивалентность на A. Множество всевозможных классов эквивалентности множества A по отношению ϱ называется фактормножеством множества A по отношению ϱ и обозначается $A/_\varrho$ (не путать с $A \setminus \varrho$).*

Теорема 1. *Пусть A — множество, а ϱ, ϱ_1 и ϱ_2 — эквивалентности на A. Тогда:*

1. *$A/_\varrho$ является разбиением множества A;*
2. *Если эквивалентности ϱ_1 и ϱ_2 на множестве A различны, то различны и фактормножества $A/_{\varrho_1}$ и $A/_{\varrho_2}$.*

Доказательство. 1. Так как ϱ — эквивалентность на A, то из п. 4 теоремы 4.3.1 следует, что два различных класса по ϱ не пересекаются. Далее, из п. 1 теоремы 4.3.1 следует, что объединение всех классов по ϱ совпадает со всем множеством A. Таким образом, согласно определению 4.2.1, фактормножество A/ϱ является разбиением A.

2. Пусть $\varrho_1 \neq \varrho_2$. Значит ϱ_1 и ϱ_2 состоят из различных пар. Пусть, для определенности, $(a,b) \in \varrho_1$ и $(a,b) \notin \varrho_2$, где $a, b \in A$. Предположим, что $\overline{a}_{\varrho_1} \in A/\varrho_2$. Значит найдется $x \in A$ такой, что $\overline{x}_{\varrho_2} = \overline{a}_{\varrho_1}$. Так как $a \in \overline{a}_{\varrho_1}$, то $a \in \overline{x}_{\varrho_2}$. Это означает, что для любого $y \in A$ $(a,y) \in \varrho_1$ тогда и только тогда, когда $(a,y) \in \varrho_2$. Однако, для $y = b$ это не так. Значит наше предположение неверно, то есть $\overline{a}_{\varrho_1} \notin A/\varrho_2$. Но, так как $\overline{a}_{\varrho_1} \in A/\varrho_1$, то $A/\varrho_1 \neq A/\varrho_2$. ■

4.5. Разбиения и фактормножества.

Теорема 1. *Для всякого разбиения $\mathfrak{A}$ множества A существует единственная эквивалентность ϱ на A такая, что $\mathfrak{A} = A/\varrho$.*

Доказательство. Построим бинарное отношение ϱ следующим образом: для любых элементов $a, b \in A$, пара $(a,b) \in \varrho$ тогда и только тогда, когда a и b принадлежат одному и тому же подмножеству из $\mathfrak{A}$. Легко понять, что ϱ является отношением эквивалентности и $\mathfrak{A} = A/\varrho$.

Предположим, что существует еще одна эквивалентность σ на A такая, что $\sigma \neq \varrho$ и $\mathfrak{A} = A/\sigma$. Однако, по условию теоремы, $\mathfrak{A} = A/\varrho$. Тогда $A/\varrho = A/\sigma$, что невозможно в силу п. 2 теоремы 4.4.1. Следовательно, ϱ — единственная эквивалентность на A такая, что $\mathfrak{A} = A/\varrho$. ■

Пример 1. Указать все эквивалентности на множестве $A = \{1,2,3\}$.

Разбиение множества A	Соответствующая ему эквивалентность
$\mathfrak{A}_1 = \{\{1\},\{2\},\{3\}\}$	$\varrho_1 = E_A$
$\mathfrak{A}_2 = \{\{1,2\},\{3\}\}$	$\varrho_2 = \{(1,1),(2,2),(1,2),(2,1),(3,3)\}$
$\mathfrak{A}_3 = \{\{1,3\},\{2\}\}$	$\varrho_3 = \{(1,1),(3,3),(1,3),(3,1),(2,2)\}$
$\mathfrak{A}_4 = \{\{1\},\{2,3\}\}$	$\varrho_4 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$
$\mathfrak{A}_5 = \{\{1,2,3\}\}$	$\varrho_5 = A \times A$

4.6. Новые термины. Бинарное отношение. Отношение эквивалентности. Классы эквивалентности. Фактормножество. Разбиение. Кардинальные числа.

4.7. Контрольные вопросы.

1. Пустое соответствие из A в A для любого A, очевидно, является бинарным отношением на A. Какими свойствами из указанных в определении 4.1.2 оно обладает? Является ли оно отношением эквивалентности?

2. Укажите примеры бинарных отношений на множестве $A = \{1,2\}$, которые были бы:

   (a) не рефлексивными, не симметричными и не транзитивными;

   (b) рефлексивными, но не симметричными и не транзитивными;

   (c) симметричными, но не рефлексивными и не транзитивными;

   (d) транзитивными, но не рефлексивными и не симметричными;

   (e) рефлексивными, симметричными, но не транзитивными;

   (f) рефлексивными, транзитивными, но не симметричными;

   (g) симметричными и транзитивными, но не рефлексивными;

   (h) рефлексивными, симметричными и транзитивными.

3. Сделайте задание 2 для множества $A = \{1,2,3\}$.

4. Укажите все разбиения множества A, если:

(a) $A = \{1, 2\}$;

(b) $A = \{1, 2, 3, 4\}$.

5. Всякое ли разбиение множества A является фактормножеством множества A по некоторой эквивалентности?

6. Всякое ли фактормножество множества A является разбиением этого множества?

7. Является ли отношение

$$\varrho = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,5), (5,1), (2,5), (5,2), (1,2), (2,1)\}$$

эквивалентностью на $A = \{1, 2, 3, 4, 5\}$? Если да, то укажите соответствующее ему фактормножество.

4.8. Упражнения.

1. Укажите все эквивалентности на $A = \{1, 2, 3, 4\}$.

2. Докажите, что произведение бинарных отношений на A не коммутативно.

3. Докажите, что произведение рефлексивных бинарных отношений на A есть рефлексивное бинарное отношение на A.

4. Докажите, что произведение симметричных бинарных отношений на A не всегда является симметричным бинарным отношением на A.

5. Докажите, что произведение транзитивных бинарных отношений на A не всегда является транзитивным бинарным отношением на A.

6. Укажите все такие бинарные отношения ϱ на $A = \{1, 2, 3\}$, которые обладают свойством:

$$\varrho \circ \varrho = \varrho.$$

§ 5. Отношение порядка

Отношение порядка. Частично упорядоченные множества. Минимальные (максимальные) и наименьшие (наибольшие) элементы упорядоченного множества. Покрывающие элементы. Линейно и вполне упорядоченные множества. Решетки.

5.1. Основное определение.

Определение 1. *Пусть ϱ — бинарное отношение на A.*

1. *ϱ называется антисимметричным, если из того, что $(a,b) \in \varrho$ и $(b,a) \in \varrho$ следует $a = b$.*
2. *ϱ называется отношением порядка, если ϱ рефлексивно, антисимметрично и транзитивно.*
3. *Множество A с зафиксированным на нем отношением порядка ϱ называется упорядоченным: $\langle A, \varrho \rangle$.*

Пример 1. Пусть $A = \{1,2,3\}$.

1. $\varrho_1 = E_A = \{(1,1),(2,2),(3,3)\}$ — отношение порядка;
2. $\varrho_2 = E_A \cup \{(1,2),(1,3)\}$ — отношение порядка (отношение делимости $\vdots$);
3. $\varrho_3 = \{(1,1),(1,2),(1,3)\}$ не является отношением порядка;
4. $\varrho_4 = E_A \cup \{(1,2),(2,1),(3,3)\}$ не является отношением порядка;
5. $\varrho_5 = E_A \cup \{(1,2),(2,3)\}$ не является отношением порядка;
6. $\varrho_6 = E_A \cup \{(1,2),(2,3),(1,3)\}$ — отношение порядка (отношение сравнения по величине — $\leq$).

Отношения порядка будем обозначать символами $\leq$, $\subseteq$ и т. д. Вместо $(a,b) \in \leq$ будем писать $a \leq b$.

5.2. Упорядоченные множества.

Определение 1. *Пусть $\langle A, \leq \rangle$ — упорядоченное множество.*

1. *Если $(a,b) \in \leq$, то этот факт будем записывать в виде:*

$$a \leq b, \quad b \geq a,$$

и говорить "a меньше либо равно b", "b больше либо равно a" (в смысле отношения порядка $\leq$). Если $a \leq b$ или $a \geq b$ и $a \neq b$, то будем писать $a < b$ или $b > a$ и говорить "a меньше b", "b больше a".

2. *Элемент $a \in A$ называется минимальным (максимальным), если в A нет элементов, меньших (больших) элемента a.*
3. *Элемент $a \in A$ называется наименьшим (наибольшим) элементом множества A, если этот элемент меньше (больше) любого другого элемента из A.*

Пример 1. Пусть $A = \{1,2,3\}$.

1. $2^A = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, A\}$, $\langle 2^A, \subseteq \rangle$ — упорядоченное множество, наименьший элемент (он же минимальный) — $\varnothing$, наибольший (он же максимальный) — само множество $A = \{1,2,3\}$.
2. $2_0^A = 2^A \setminus \{\varnothing\}$, $\langle 2_0^A, \subseteq \rangle$ — упорядоченное множество, наименьшего элемента нет, минимальные — $\{1\}$, $\{2\}$, $\{3\}$, наибольший (он же максимальный) — $A = \{1,2,3\}$.

3. $2_1^A = 2^A \setminus \{A\}$, $\langle 2_1^A, \subseteq \rangle$ — упорядоченное множество, наибольшего элемента нет, максимальные — $\{1,2\}$, $\{2,3\}$, $\{1,3\}$, наименьший (он же минимальный) — $\varnothing$.

4. $2_2^A = 2^A \setminus \{\varnothing, A\}$, $\langle 2_2^A, \subseteq \rangle$ — упорядоченное множество, наибольшего и наименьшего элементов нет, максимальные — $\{1,2\}$, $\{2,3\}$, $\{1,3\}$, минимальные — $\{1\}$, $\{2\}$, $\{3\}$.

5. $\langle N, \leq \rangle$ — упорядоченное множество, наибольшего и максимальных элементов нет, наименьший (он же минимальный) — 1.

6. $\langle N, \vdots \rangle$ — упорядоченное множество, наибольшего и максимальных элементов нет, наименьший (он же минимальный) — 1.

7. $\langle N \setminus \{1\}, \vdots \rangle$ — упорядоченное множество, наибольшего, наименьшего и максимальных элементов нет, минимальные — все простые числа.

Определение 2 (покрывающего элемента). *Пусть $\langle A, \leq \rangle$ — некоторое упорядоченное множество, $a, b \in A$.*

Элемент b называется покрывающим для элемента a или покрытием элемента a, если выполнены следующие условия.

1. *$a < b$.*
2. *В A нет элементов x таких, что $a < x < b$.*

Замечание. Условимся изображать конкретные упорядоченные множества рисунками так, что:

1. Каждый элемент изображаем точкой на ориентированном листе бумаги так, что различным элементам множества соответствуют различные точки.
2. Если b — покрытие для a, то точка b расположена выше точки a и эти точки соединены отрезками. Такие рисунки называются графами упорядоченного множества.

Пример 2. На рис. 6 (стр. 34) изображены графы упорядоченных множеств из предыдущего примера.

Теорема 1.

1. *Упорядоченное множество имеет не более одного наименьшего и не более одного наибольшего элемента.*
2. *Наименьший элемент упорядоченного множества является единственным минимальным элементом этого множества.*

   Наибольший элемент упорядоченного множества является единственным максимальным элементом этого множества.

Доказательство проведите самостоятельно.

5.3. Линейные и вполне упорядоченные множества.

Определение 1. *Пусть $\langle A, \leq \rangle$ — упорядоченное множество.*

1. *Элементы $a, b \in A$ называются сравнимыми, если $a \leq b$ или $b \leq a$. В противном случае элементы a и b называются несравнимыми.*
2. *A называется линейно упорядоченным множеством (цепью), если любые два элемента этого множества сравнимы.*
3. *A называется вполне упорядоченным множеством, если каждое непустое подмножество множества A имеет наименьший элемент.*

Пример 1. Рассмотрим некоторые упорядоченные множества.

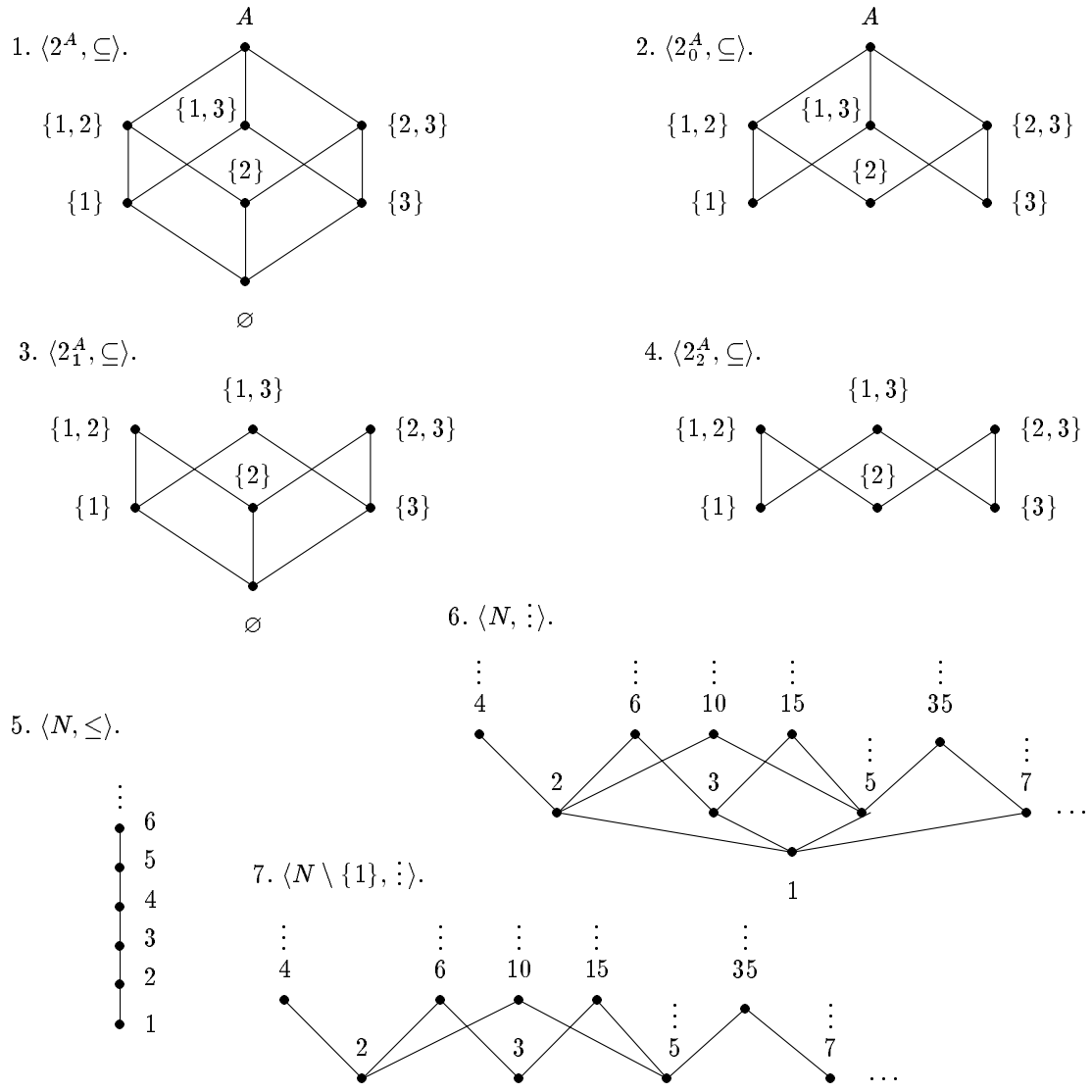

Рис. 6: Примеры упорядоченных множеств.

1. $\langle N, \leq\rangle$ — линейно упорядоченное множество.
2. $\langle Z, \leq\rangle$ также является линейно упорядоченным множеством.
3. Рассмотрим множество $A = \{1, 2, 3\}$. Множество всех его подмножеств $\langle 2^A, \subseteq\rangle$ не является вполне упорядоченным.

Теорема 1.

1. *Если упорядоченное множество является вполне упорядоченным, то оно является и линейно упорядоченным.*
2. *Если конечное упорядоченное множество является линейно упорядоченным, то оно является вполне упорядоченным.*

Доказательство. 1. Пусть $\langle A, \leq\rangle$ — вполне упорядоченное множество. Тогда, по определению, каждое его непустое подмножество имеет наименьший элемент. Следовательно, и каждое его двухэлементное подмножество имеет наименьший элемент, но это означает, что любые два элемента A сравнимы, то есть A линейно упорядочено.

2. Пусть $\langle A, \leq \rangle$ — конечная цепь и $B \subseteq A$, $B \neq \varnothing$.

Если $|B| = 1$, то $b \in B$ является наименьшим для подмножества B.

Если $|B| > 1$, то пусть $a, b \in B$, $a \neq b$. Так как A линейно упорядочено, то $a < b$ или $b < a$, значит $\{a, b\} \subseteq B$ имеет наименьший элемент. Далее, выбираем произвольный $c \in B \setminus \{a, b\}$ и сравниваем его с наименьшим элементом множества $\{a, b\}$ (это возможно, так как A — цепь). Таким образом, получаем наименьший элемент множества $\{a, b, c\}$. Этот процесс закончится нахождением наименьшего элемента подмножества B, так как A и, следовательно, B являются конечными множествами. В силу произвольности выбора B заключаем, что A вполне упорядочено. ■

Заметим, что требование конечности линейно упорядоченного множества во втором пункте только что доказанной теоремы является существенным.

Пример 2. Пусть $A = \{a_1, a_2, a_3, \ldots\} \cup \{b\}$. Введем на A бинарное отношение $\leq$ следующим образом: $a_i \leq a_j$, если число j не превосходит i; $b < a_i$ для любого i. Очевидно, что A линейно упорядочено. Однако, A не является вполне упорядоченным, так как подмножество $\{a_1, a_2, a_3, \ldots\}$ не имеет наименьшего элемента.

5.4. Решетки.

Определение 1. *Пусть $\langle A, \leq \rangle$ — упорядоченное множество. $B \subseteq A$, $a \in A$.*

1. *a называется нижней границей (верхней границей) множества B, если a меньше (больше) любого элемента из B, отличного от a.*

2. *a называется точной нижней границей (точной верхней границей) множества B, если a есть нижняя граница (верхняя граница) и a больше (меньше) любой другой нижней (верхней) границы множества B.*

3. *A называется решеткой, если любая пара элементов из A имеет точную верхнюю границу и точную нижнюю границу.*

Пример 1.

1. Пусть $A = \{1, 2, 3, 4, 5\}$.
   (a) $\langle A, E_A \rangle$ не является решеткой.
   (b) Пусть $\varrho = E_A \cup \{(1,3), (2,3), (1,4), (2,4), (3,5), (4,5), (1,5), (2,5)\}$, тогда $\langle A, \varrho \rangle$ не является решеткой.

2. $A = \{1, 2, 3\}$. $\langle 2^A, \subseteq \rangle$ — решетка.

3. $\langle N, \vdots \rangle$ — решетка.

Теорема 1. *Всякое линейно упорядоченное множество является решеткой.*

Доказательство проведите самостоятельно.

Следствие 1. *Всякое вполне упорядоченное множество является решеткой.*

Следует из теоремы 5.3.1 и предыдущей теоремы.

Теорема 2. *Всякая конечная решетка имеет наименьший и наибольший элемент.*

Доказательство проведите самостоятельно.

5.5. Новые термины. Антисимметричность. Частично упорядоченное множество. Минимальные (максимальные) и наименьшие (наибольшие) элементы. Покрытие. Графы упорядоченных множеств. Линейно упорядоченные и вполне упорядоченные множества. Нижняя (верхняя) граница. Точная нижняя (верхняя) граница. Решетка.

5.6. Контрольные вопросы.

1. Укажите все не антисимметричные бинарные отношения на множестве $A = \{1, 2\}$.
2. Известно, что бинарное отношение ϱ на A не является симметричным. Означает ли это, что ϱ антисимметрично?
3. Известно, что бинарное отношение ϱ на A не является антисимметричным. Означает ли это, что ϱ симметрично?
4. Приведите пример бинарного отношения ϱ на некотором множестве A, которое не является симметричным и не является антисимметричным.
5. Существует ли бинарное отношение, являющееся одновременно и симметричным и антисимметричным?
6. Существует ли такое бинарное отношение, которое является одновременно и отношением эквивалентности и отношением порядка?
7. Приведите пример упорядоченного множества:
   (a) не имеющего минимальных элементов;
   (b) не имеющего максимальных элементов;
   (c) не имеющего ни минимальных, ни максимальных элементов;
   (d) имеющего минимальные элементы, но не имеющего наименьших;
   (e) имеющего максимальные элементы, но не имеющего наибольших.
8. Может ли упорядоченное множество иметь два различных наименьших элемента? Два различных наибольших элемента?
9. Может ли упорядоченное множество иметь наименьший элемент, но не иметь минимальных? Иметь наибольший элемент, но не иметь максимальных?
10. Может ли упорядоченное множество иметь элементы:
    (a) с двумя покрывающими;
    (b) покрывающие два различных элемента?
11. Обладает ли отношение “быть покрывающим” свойством транзитивности?
12. Существуют ли упорядоченные множества, содержащие элементы, которые не имеют ни одного покрывающего?
13. Упорядоченное множество A вполне упорядочено. Является ли оно линейно упорядоченным?
14. Упорядоченное множество A линейно упорядочено. Является ли оно вполне упорядоченным?
15. Пусть $\langle N, \vdots \rangle$. Укажите все нижние границы для элементов 3 и 5, 16 и 18, 36 и 48. Укажите все верхние границы для указанных пар чисел. Укажите для этих пар чисел все точные нижние и точные верхние границы.
16. Пусть $\langle A, \leq \rangle$, $a, b \in A$ и $a < b$. Укажите точную верхнюю и точную нижнюю границы для пары элементов a и b. Для пары элементов a и a.

5.7. Упражнения.

1. Бинарное отношение ϱ на множестве A, является антисимметричным и симметричным одновременно тогда и только тогда, когда $\varrho \subseteq E_A$.
2. Докажите, что единственное бинарное отношение на множестве A, являющееся эквивалентностью и упорядоченным множеством — это E_A.

§ 6. Кардинальные числа

Равномощные множества. Кардинальные числа. Сравнение кардинальных чисел. Теорема Кантора-Бернштейна. Операции над кардинальными числами и их свойства.

6.1. Учение о мощности. Ранее мы определили понятие мощности для конечных множеств. Теперь расширим это понятие на случай произвольных множеств.

Определение 1. *Два множества A и B называются равномощными, если существует биекция из A на B,*

Рассмотрим класс всех множеств $\mathfrak{K}$. Будем считать, что множества A и B находятся в отношении ϱ, если существует биекция из A на B. Легко понять, что ϱ будет отношением эквивалентности на $\mathfrak{K}$. Все множества, находящиеся в одном классе по ϱ будут равномощными. Поставим в соответствие каждому классу ϱ некоторый объект, называемый *кардинальным числом* или *кардиналом*. Например, классу ϱ, содержащему все n-элементные множества (n фиксировано), поставим в соответствие число n. Классу ϱ, состоящему из одного пустого множества, ставится в соответствие кардинальное число 0. Классу ϱ, содержащему множество натуральных чисел ставится в соответствие кардинальное число $\aleph_0$ ($\aleph$ ("алеф") — первая буква иврита). Любое множество из этого класса называется *счетным*. Классу ϱ, содержащему множество всех действительных чисел, ставится в соответствие кардинальное число $\aleph_1$, которое называется также *мощностью континуума*.

Таким образом, кардинальные числа являются символами, выражающими мощность множеств. Будем в дальнейшем обозначать произвольные кардинальные числа маленькими готическими буквами, а тот факт, что множество A принадлежит классу эквивалентности ϱ, которому поставлено в соответствие кардинальное число $\mathfrak{a}$, будем обозначать так: $|A| = \mathfrak{a}$. Далее, в этом случае, будем говорить, что мощность множества A равна $\mathfrak{a}$.

6.2. Сравнение кардинальных чисел. В этом пункте устанавливается способ сравнения мощностей произвольных множеств.

Определение 1. *Пусть $\mathfrak{a} = |A|$, $\mathfrak{b} = |B|$. Определим на множестве всех кардинальных чисел бинарное отношение $\leq$ следующим образом: $\mathfrak{a} \leq \mathfrak{b}$ тогда и только тогда, когда существует биекция из A на собственное подмножество множества B.*

Очевидно, что это определение не зависит от выбора множеств A и B и поэтому выражает отношение между кардинальными числами.

Теорема 1. *Пусть $\mathfrak{A}$ — произвольное множество кардинальных чисел, тогда $\langle \mathfrak{A}, \leq \rangle$ является линейно упорядоченным множеством.*

Для доказательства этой теоремы нам необходимо показать, что бинарное отношение $\leq$ является отношением порядка. Рефлексивность и транзитивность этого отношения следуют из выше данного определения и свойств суперпозиции функций (отображений), см. § 3. Антисимметричность отношения $\leq$ следует из теоремы Кантора-Бернштейна, доказательство которой приводится в следующем пункте.

Для любых двух множеств A и B существует, очевидно, одна и только одна из следующих возможностей:

1) существует биекция из A на собственное подмножество множества B, но не существует биекции из B на собственное подмножество множества A;

2) существует биекция из B на собственное подмножество множества A, но не существует биекции из A на собственное подмножество множества B;

3) существует биекция из A на собственное подмножество множества B и существует биекции из B на собственное подмножество множества A.

Если $|A| = \mathfrak{a}$, $|B| = \mathfrak{b}$, то в первом случае имеем $\mathfrak{a} < \mathfrak{b}$, во втором — $\mathfrak{b} < \mathfrak{a}$. Теорема Кантора-Бернштейна утверждает, что в третьем случае будет $\mathfrak{a} = \mathfrak{b}$. Таким образом, получаем способ сравнения мощностей произвольных множеств.

Например, если таким образом сравнивать мощности конечных множеств, то такое сравнение фактически будет представлять собой сравнение по числу элементов. Это согласуется с ранее данным определением мощности конечного множества.

6.3. Теорема Кантора-Бернштейна.

Лемма 1. *Пусть $\alpha \subseteq A \times B$ — соответствие из A в B, I — некоторое множество индексов и $A_i \subseteq A$, $i \in I$. Тогда*

$$\alpha\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} \alpha(A_i).$$

Доказательство. 1. Пусть $x \in \alpha\left(\bigcup\limits_{i\in I} A_i\right)$, тогда существует $a \in \bigcup\limits_{i\in I} A_i$ такой, что $x \in \alpha(a)$. Следовательно, существует такой индекс $k \in I$, что $a \in A_k$, то есть $x \in \alpha(A_k)$. Но это значит, что $x \in \bigcup\limits_{i\in I} \alpha(A_i)$. Таким образом, $\alpha\left(\bigcup\limits_{i\in I} A_i\right) \subseteq \bigcup\limits_{i\in I} \alpha(A_i)$.

2. Пусть $x \in \bigcup\limits_{i\in I} \alpha(A_i)$, тогда существует такой индекс $k \in I$, что $x \in \alpha(A_k)$. Это означает, что существует $a \in A_k$ такой, что $x \in \alpha(a)$. Так как $a \in A_k$, то $a \in \bigcup\limits_{i\in I} A_i$. Следовательно, $x \in \alpha(a) \subseteq \alpha\left(\bigcup\limits_{i\in I} A_i\right)$ и, значит, $\bigcup\limits_{i\in I} \alpha(A_i) \subseteq \alpha\left(\bigcup\limits_{i\in I} A_i\right)$.

Из пунктов 1 и 2 следует утверждение леммы. ■

Лемма 2. *Если $\alpha\colon A \to \alpha(A)$ — биекция множества A на свое собственное подмножество $\alpha(A) \subset A$, то для всякого множества $C \subseteq \big(A \setminus \alpha(A)\big)$ существует биекция $\alpha^*\colon A \to \alpha^*(A)$, причем $\alpha^*(A) = C \cup \alpha(A)$.*

Доказательство. Обозначим $\alpha^0(C) = C$, $\alpha^1(C) = \alpha(C)$, $\alpha^{n+1}(C) = \alpha(\alpha^n(C))$ и рассмотрим множество

$$S = C \cup \alpha(C) \cup \alpha^2(C) \cup \alpha^3(C) \cup \ldots = \bigcup_{n=0}^{\infty} \alpha^n(C). \tag{1}$$

1. Покажем, что $S = C \cup \alpha(S)$.

Пусть $x \in S$, тогда, так как $C \subseteq S$, то $x \in C$ или $x \notin C$. В первом случае $x \in C \cup \alpha(S)$. Если же $x \notin C$, то тогда существует такое число $n \in N$, что $x \in \alpha^n(C)$ (см. (1)). Так как из леммы 6.3.1 следует, что

$$\alpha(S) = \alpha(C) \cup \alpha^2(C) \cup \alpha^3(C) \cup \ldots, \tag{2}$$

то $\alpha^n(C) \subseteq \alpha(S)$. Но тогда $x \in \alpha(S)$. Таким образом, $x \in C \cup \alpha(S)$, то есть доказано, что $S \subseteq C \cup \alpha(S)$.

Пусть $x \in C \cup \alpha(S)$, тогда $x \in C$ или $x \notin C$. В первом случае, так как $C \subseteq S$, то $x \in S$. Если $x \notin C$, то $x \in \alpha(S)$. Но, так как $\alpha(S) \subseteq S$ (см. (1) и (2)), то, и в этом случае, $x \in S$. Следовательно $C \cup \alpha(S) \subseteq S$.

Итак, из антисимметричности отношения включения (см. I.1.5.) следует, что $S = C \cup \alpha(S)$.

2. Построим соответствие α^* из A в A, по следующему правилу:

$$\alpha^*(x) = \begin{cases} x, & x \in S, \\ \alpha(x), & x \in (A \setminus S), \end{cases}$$

то есть α^* является отображением, которое на множестве S тождественно и совпадает с α на множестве $A \setminus S$.

Так как $S = C \cup \alpha(S)$, то $S \cap \alpha(A \setminus S) = \big[C \cup \alpha(S)\big] \cap \alpha(A \setminus S) = \big[C \cap \alpha(A \setminus S)\big] \cup \big[\alpha(S) \cap \alpha(A \setminus S)\big]$. Но $C \cap \alpha(A \setminus S) = \varnothing$, так как $C \subseteq A \setminus \alpha(A)$, а $\alpha(S) \cap \alpha(A \setminus S) = \varnothing$, так как $\alpha\colon A \to A$ инъекция.

Таким образом, $S \cap \alpha(A \setminus S) = \varnothing$, а это значит, что $\alpha^*\colon A \to A$ является инъекцией, причем $\alpha^*(A) = S \cup \alpha(A \setminus S) = C \cup \alpha(S) \cup \alpha(A \setminus S) = C \cup \alpha(A)$. ■

Следующая теорема является краеугольным камнем теории множеств. Она показывает, что отношение $\leq$ на множестве всех кардинальных чисел обладает свойством антисимметричности и, следовательно, является отношением линейного порядка (см. теорему 6.2.1). Кроме того она дает метод доказательства равномощности множеств.

Теорема 1 (Кантора-Бернштейна). *Если существуют биекции множества A на собственное подмножество множества B и множества B на собственное подмножество множества A, то существует биекция A на B.*

Доказательство. Пусть $\alpha\colon A \to \alpha(A)$ и $\beta\colon B \to \beta(B)$ — биекции, причем $\alpha(A) \subset B$, $\beta(B) \subset A$. Рассмотрим суперпозицию $\gamma = \beta\alpha$, $\gamma\colon A \to A$, $\gamma(A) = \beta(\alpha(A))$. Так как α и β являются инъекциями, то и их суперпозиция также будет инъекцией по теореме 3.4.1, то есть γ является биекцией множества A на свое собственное подмножество $\gamma(A)$. Тогда, по лемме 6.3.2, для любого подмножества $C \subseteq \big(A \setminus \gamma(A)\big)$ существует биекция $\gamma^*\colon A \to C \cup \gamma(A)$. Выберем $C = \beta(B) \setminus \gamma(A)$. В этом случае $\gamma^*(A) = \big(\beta(B) \setminus \gamma(A)\big) \cup \gamma(A) = \beta(B)$. Тогда $\beta^{-1}\gamma^*(A) = \beta^{-1}\beta(B) = B$. Следовательно, так как β^{-1} — инъективная частичная функция, то $\beta^{-1}\gamma^*\colon A \to B$ является искомой биекцией A на B. ■

Заметим, что иногда теоремой Кантора-Бернштейна (в другой формулировке) называют лемму 6.3.2 в силу ее важности и сложности, а приведенную здесь классическую формулировку теоремы называют следствием этой леммы.

6.4. Операции над кардинальными числами.

Определение 1. *Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — произвольные кардинальные числа, причем $\mathfrak{a} = |A|$, $\mathfrak{b} = |B|$ и $A \cap B = \varnothing$.*

Определим операции над кардинальными числами следующим образом:

$$\mathfrak{a} + \mathfrak{b} = |A \cup B|,$$
$$\mathfrak{a} \cdot \mathfrak{b} = |A \times B|,$$
$$\mathfrak{a}^{\mathfrak{b}} = |A^B|,$$

где A^B — множество всех отображений из B в A.

Как обычно, знак $\cdot$ будем в записи выражений опускать.

Видно, что результаты операций не зависят от природы элементов множеств A и B.

6.5. Свойства операций над кардинальными числами. Основные свойства введенных операций над кардинальными числами выражает

Теорема 1. *Пусть $|A| = \mathfrak{a}$, $|B| = \mathfrak{b}$, $|C| = \mathfrak{c}$ и A, B, C — попарно непересекающиеся множества. Тогда*

1) $\mathfrak{a} + (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c}$
2) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$
3) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$
4) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$
5) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$
6) $\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}}\mathfrak{a}^{\mathfrak{c}}$
7) $(\mathfrak{a}\mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}}\mathfrak{b}^{\mathfrak{c}}$
8) $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}\mathfrak{c}}$

Доказательство этой теоремы проводится на основе определения операций над кардинальными числами. Проведите его самостоятельно.

Теорема 2. *Пусть A — произвольное множество, $\mathcal{B}(A)$ — множество всех подмножеств множества A. Тогда*

$$|\mathcal{B}(A)| = 2^{|A|}.$$

Доказательство. Для произвольного подмножества $B \subseteq A$ рассмотрим характеристическую функцию этого подмножества:

$$\chi_B(a) = \begin{cases} 0, & \text{если } a \in B, \\ 1, & \text{если } a \notin B. \end{cases}$$

Рассмотрим соответствие α из $\mathcal{B}(A)$ в $\mathcal{X} = \{\chi_B \mid B \subseteq A\}$, которое каждому $B \in \mathcal{B}(A)$ ставит в соответствие его характеристическую функцию χ_B. Легко понять, что $\alpha\colon \mathcal{B}(A) \to \mathcal{X}$ является биекцией. Но каждая характеристическая функция фактически является отображением $\chi_B\colon A \to \{0,1\}$. Таким образом, из теоремы 6.3.1 Кантора-Бернштейна и определения операций над кардинальными числами, следует $|\mathcal{B}(A)| = |\mathcal{X}| = |\{0,1\}^A| = 2^{|A|}$. ■

Теорема 3. *Множество $\mathcal{B}(A)$ всех подмножеств любого множества A имеет мощность, строго бóльшую мощности множества A, то есть*

$$|A| < 2^{|A|}.$$

Доказательство. Если поставить в соответствие каждому элементу $a \in A$ одноэлементное подмножество $\{a\}$ множества A, то получим биекцию множества A на собственное подмножество $\mathcal{B}(A)$. Поэтому $|A| \leq |\mathcal{B}(A)|$.

Покажем, что $|A| \neq |\mathcal{B}(A)|$. Предположим, что это не так, тогда существует биекция φ из A на $\mathcal{B}(A)$. Пусть

$$M = \{a \in A \mid a \notin \varphi(a)\}.$$

Так как $M \subseteq A$, то $M \in \mathcal{B}(A)$. Следовательно, должен существовать элемент $m \in A$ такой, что $\varphi(m) = M$. Получаем противоречие: если $m \in M$, то $m \notin \varphi(m) = M$, а если $m \notin M$, то $m \in \varphi(m) = M$. ■

Теорема 4. *Пусть I — некоторое множество индексов и $\mathfrak{a}_i = \mathfrak{a}$, для любого $i \in I$. Тогда*

$$\sum_{i \in I} \mathfrak{a}_i = |I|\mathfrak{a}.$$

Доказательство. Пусть A — произвольное множество такое, что $|A| = \mathfrak{a}$. Тогда, по определению умножения кардинальных чисел 6.4.1, $|I|\mathfrak{a} = |I \times A|$. Обозначим $(i, A) = \{(i, a) \mid a \in A\}$, где $i \in I$. Очевидно, что $\bigcup\limits_{i \in I} (i, A) = I \times A$. Так как $(i, A) \cap (j, A) = \varnothing$, при $i \neq j$ и для любого $i \in I$ $|(i, A)| = \mathfrak{a}$, то $\sum\limits_{i \in I} \mathfrak{a}_i = |\bigcup\limits_{i \in I} (i, A)| = |I \times A| = |I|\mathfrak{a}$. ■

Следствие 1. *Для любого кардинального числа $\mathfrak{a}$*

$$\underbrace{\mathfrak{a} + \mathfrak{a} + \ldots}_{\aleph_0} = \aleph_0 \mathfrak{a}.$$

Приведем следующую важную теорему без доказательства.

Теорема 5. *Для любого бесконечного кардинального числа $\mathfrak{a} \geq \aleph_0$*

$$\aleph_0 \mathfrak{a} = \mathfrak{a}. \tag{3}$$

Следствие 2. *Если хотя бы одно из кардинальных чисел $\mathfrak{a}$, $\mathfrak{b}$ бесконечно, то*

$$\mathfrak{a} + \mathfrak{b} = \max(\mathfrak{a}, \mathfrak{b})$$

Доказательство. Пусть, например, $\mathfrak{a} \geq \mathfrak{b}$. Тогда, по условию, $\mathfrak{a} \geq \aleph_0$. В этом случае, используя равенство (3), получим

$$\mathfrak{a} \leq \mathfrak{a} + \mathfrak{b} \leq \mathfrak{a} + \mathfrak{a} = 2\mathfrak{a} \leq \aleph_0 \mathfrak{a} = \mathfrak{a}.$$

Следовательно, $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$. ■

6.6. Новые термины. Кардинальные числа. Счетное множество. Мощность континуума.

6.7. Контрольные вопросы.

1. Является ли инъекция α из A в B биекцией из A на $\alpha(A) \subset B$?
2. Может ли объединение конечных множеств быть бесконечным?
3. Пусть $\mathfrak{a} = |\{a, b, c, d\}|$, $\mathfrak{b} = |\{a, b, h\}|$. Чему равно $\mathfrak{a} + \mathfrak{b}$?
4. Опишите способ сравнения кардинальных чисел.
5. Пусть N_2 — множество всех четных натуральных чисел. Сравните $|N|$ и $|N_2|$.

6.8. Упражнения.

1. Докажите теорему 6.5.1.
2. Докажите, что для любого $n \in N$, $\aleph_0^n = \aleph_0$.
3. Докажите, что $\aleph_1 = 2^{\aleph_0}$.

   Заметим, что вопрос о существовании промежуточной мощности между $\aleph_0$ и $\aleph_1$ называется *проблемой континуума*. Долгое время она оставалась нерешенной. Оказалось, однако, что как утверждение о существовании кардинального числа $\mathfrak{c}$ такого, что $\aleph_0 < \mathfrak{c} < \aleph_1$ (*гипотеза континуума*), так и его отрицание совместимо с общепринятой аксиоматикой теории множеств.
4. Докажите, что если хотя бы одно из кардинальных чисел $\mathfrak{a}$, $\mathfrak{b}$ бесконечно, то $\mathfrak{ab} = \max(\mathfrak{a}, \mathfrak{b})$.

Глава II

Основы комбинаторики

§ 1. Основной принцип комбинаторики. Перестановки, размещения и сочетания

Основной принцип комбинаторики. Количество подмножеств данного множества. Размещения и перестановки: A_n^k, P_n. Формулы для вычисления A_n^k, P_n. Сочетания C_n^k. Формулы для вычисления C_n^k. Некоторые свойства сочетаний.

1.1. Основной принцип комбинаторики. Установим сначала очень важное правило, которое часто применяется при комбинаторных расчетах. Начнем с такой задачи.

Задача 1. Из Ростова-на-Дону до Москвы можно добраться пароходом, поездом, автобусом и самолетом. Из Москвы до Санкт-Петербурга — поездом, автобусом и самолетом. Сколькими способами можно осуществить путешествие по маршруту Ростов-на-Дону — Москва — Санкт-Петербург?

Решение. Очевидно, что число различных путей из Ростова-на-Дону до Санкт-Петербурга равно $4 \cdot 3 = 12$, так как, выбрав один из четырех возможных способов путешествия от Ростова-на-Дону до Москвы, имеем три возможных способа путешествия от Москвы до Санкт-Петербурга (рис. 1). ■

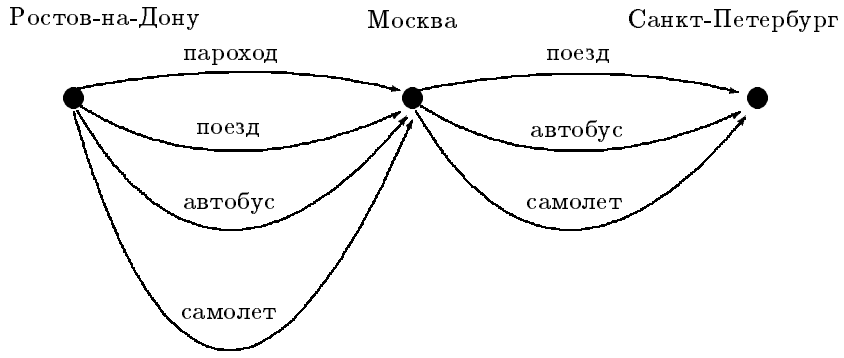

Рис. 1: Способы путешествия по маршруту Ростов-на-Дону — Москва — Санкт-Петербург.

Соображения, которые были приведены при решении задачи 1, позволяют сформулировать следующее простое утверждение, которое будем называть *основным правилом комбинаторики.*

Если некоторый выбор A можно осуществить m различными способами, а для каждого из этих способов некоторый другой выбор B можно осуществить n способами, то выбор A и B (в указанном порядке) можно осуществить $m \cdot n$ способами.

Иначе говоря, если некоторое действие (например, выбор пути из Ростова-на-Дону до Москвы) можно осуществить m различными способами, после чего другое действие (выбор пути от Москвы до Санкт-Петербурга) можно осуществить n способами, то два действия вместе (выбор пути от Ростова-на-Дону до Москвы, затем выбор пути от Москвы до Санкт-Петербурга) можно осуществить $m \cdot n$ способами.

Задача 2. В розыгрыше первенства страны по футболу принимают участие 16 команд. Сколькими способами могут быть распределены золотая и серебряная медали?

Решение. Золотую медаль может получить одна из 16 команд. После того как определен владелец золотой медали, серебряную медаль может получить одна из оставшихся 15 команд. Следовательно, общее число способов, которыми могут быть распределены золотая и серебряная медали равно $16 \cdot 15 = 240$. ■

Сформулируем теперь основное правило комбинаторики (правило умножения) в общем виде.

Пусть требуется выполнить одно за другим k действий. Если первое действие можно выполнить n_1 способами, второе действие — n_2 способами, третье действие — n_3 способами и так далее до k-го действия, которое можно выполнить k способами, то все k действий вместе могут быть выполнены

$$n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$$

способами.

Задача 3. Сколько четырехзначных чисел можно составить пользуясь только цифрами 0, 1, 2, 3, 4, 5, если ни одна из цифр не повторяется более одного раза.

Решение. Первой цифрой числа может быть одна из 5 цифр 1, 2, 3, 4, 5 (0 не может быть первой цифрой, так как в этом случае число не будет четырехзначным); если первая цифра выбрана, то вторая может быть выбрана 5 способами, третья — 4 способами, четвертая — 3 способами. Согласно основному правилу комбинаторики общее число способов равно $5 \cdot 5 \cdot 4 \cdot 3 = 300$. ■

Часто удается разбить все изучаемые комбинации на несколько классов, причем каждая комбинация входит в один и только один класс. Ясно, что в этом случае общее число комбинаций равно сумме чисел комбинаций во всех классах. Это утверждение называют иногда *правилом суммы*. Иногда его формулируют несколько иначе.

Если некоторый объект A можно выбрать m способами, а другой объект B можно выбрать n способами, то выбор "либо A, либо B" можно осуществить $m + n$ способами.

При использовании правила суммы в этой последней формулировке надо следить, чтобы ни один из способов выбора объекта A не совпадал с каким-нибудь способом выбора объекта B (или, как мы говорили раньше, чтобы ни одна комбинация не попала в два разных класса). Если такие совпадения есть, то правило суммы утрачивает силу, и мы получаем лишь $m + n - k$ способов выбора, где k — число совпадений.

Как мы увидим далее, комбинаторные задачи бывают самых разных видов. Но большинство задач решается с помощью двух основных правил — правила суммы и правила умножения.

Задача 4. В Стране Чудес есть четыре города A, B, C, D. Из города A в город B ведет 6 дорог, а из города B в город D — 4 дороги. Из города A в город C ведет 2 дороги, а из города C в город D — 3 дороги (рис. 2). Сколькими способами можно проехать от A до D?

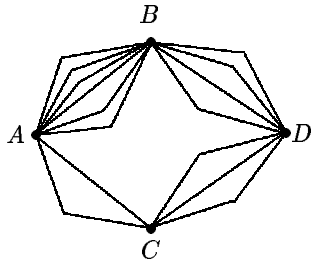

Рис. 2: Карта дорог Страны Чудес.

Решение. Выделим два случая: путь проходит через город B или путь проходит через город C. В каждом из этих случаев легко подсчитать количество возможных маршрутов: в первом — 24, во втором — 6. Складывая, получим общее количество маршрутов — 30. ■

1.2. Количество подмножеств данного множества. Выясним теперь, сколько всего подмножеств имеет множество, состоящее из n элементов (пустое множество также является подмножеством данного множества).

Теорема 1. *Число всех подмножеств множества из n элементов равно 2^n.*

Доказательство. Перенумеруем элементы данного множества. Для каждого подмножества построим последовательность длины n из нулей и единиц по следующему правилу: на k-м месте пишем 1, если элемент с номером k входит в подмножество, и 0, если элемент с номером k не входит в подмножество. Итак, каждому подмножеству соответствует своя последовательность нулей и единиц. Например, пустому множеству соответствует последовательность из одних нулей. Число всех возможных последовательностей длины n, составленных из нулей и единиц, согласно основному правилу комбинаторики, $\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{n} = 2^n$. Следовательно, и число всех подмножеств данного множества равно 2^n. ■

1.3. Размещения. Обозначим $N_0 = \{0, 1, 2, \ldots\}$.

Определение 1. *Пусть $n, k \in N_0$, $k \leq n$ и $B = \{b_1, b_2, \ldots, b_n\}$. Размещением из n элементов множества B по k элементов называется всякая последовательность длины k, составленная из неповторяющихся элементов этого множества.*

Очевидно, что количество всевозможных размещений из элементов множества B по k элементов не зависит от природы элементов множества B. По этой причине через A_n^k обозначим количество всевозможных размещений по k элементов n-элементного множества.

Пример 1. Рассмотрим множество $B = \{1, 2, 3, 4\}$. Ниже приведены все размещения этого множества по 2 элемента:

$$\begin{array}{cccccc} (1,2) & (1,3) & (1,4) & (2,1) & (2,3) & (2,4) \\ (3,1) & (3,2) & (3,4) & (4,1) & (4,2) & (4,3) \end{array}$$

То есть $A_4^2 = 12$.

Теорема 1. *Число размещений из n элементов по k равно*

$$A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1).$$

Доказательство. Подсчитаем количество всех последовательностей длины k, составленных из неповторяющихся элементов n-элементного множества. На первом месте в последовательности может стоять любой из n элементов, на втором месте — любой из оставшихся $n-1$ элементов, и так далее до k-го места на котором можно поместить любой из $n-(k-1)$ элементов. Отсюда, по правилу умножения, следует искомая формула. ■

Задача 1. Сколькими способами можно рассадить 4 учащихся на 25 местах?

Решение. Искомое число способов равно числу размещений из 25 по 4:

$$A_{25}^4 = 25 \cdot 24 \cdot 23 \cdot 22 = 303\,600. \blacksquare$$

Задача 2. Учащемуся необходимо сдать 4 экзамена на протяжении 8 дней. Сколькими способами это можно сделать?

Решение. Искомое число способов равно числу 4-элементных последовательностей (дни сдачи экзаменов) множества из 8 элементов, то есть $A_8^4 = 8{\cdot}7{\cdot}6{\cdot}5 = 1680$ способов. Если известно, что последний экзамен будет сдаваться на восьмой день, то число способов равно $4{\cdot}A_7^3 = 7{\cdot}6{\cdot}5{\cdot}4 = 840$. ■

1.4. Перестановки.

Определение 1. *Пусть $n \in N_0$, $B = \{b_1, b_2, \ldots, b_n\}$. Перестановкой из элементов множества B называется всякое размещение этого множества по n элементов.*

Очевидно, что количество всевозможных перестановок множества B не зависит от природы элементов множества B. Поэтому количество перестановок произвольного n-элементного множества обозначим через P_n.

Пример 1. Рассмотрим трехэлементное множество $B = \{1, 2, 3\}$. Все перестановки этого множества: $(1, 2, 3)$, $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$, $(3, 2, 1)$. Таким образом, $P_3 = 6$.

Будем обозначать символом $n!$ (читается "эн факториал") произведение всех натуральных чисел от 1 до n включительно: $n! = 1 \cdot \ldots \cdot n$. Удобно считать. что $0! = 1$.

Теорема 1. $P_n = n!$.

Доказательство. Согласно определению перестановки

$$P_n = A_n^n = n \cdot (n-1) \cdot \ldots \cdot 1 = n!. \blacksquare$$

Задача 1. Сколькими способами можно разместить 5 книг на полке?

Решение. Число способов расстановки книг равно числу способов упорядочения множества, состоящего из 5 элементов, то есть

$$P_5 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120. \blacksquare$$

Задача 2. Сколькими способами можно упорядочить множество

$$\{1, 2, \ldots, 2n\}$$

так, чтобы каждое четное число имело четный номер?

Решение. Четные числа можно расставить на местах с четными номерами (таких мест n) $n!$ способами; каждому способу размещения четных чисел на местах с четными номерами соответствует $n!$ способов размещения нечетных чисел на местах с нечетными номерами. Поэтому общее число перестановок указанного типа по правилу умножения равно $n! \cdot n! = (n!)^2$. $\blacksquare$

Задача 3. Сколько можно составить перестановок из n элементов, в которых данные два элемента не стоят рядом?

Решение. Определим число перестановок, в которых данные два элемента a и b стоят рядом. Могут быть следующие случаи: a стоит на первом месте, a стоит на втором месте, $\ldots$, a стоит на $(n-1)$-м месте, а b стоит правее a; число таких случаев равно $n-1$. Кроме того, a и b можно поменять местами, и, следовательно, существует $2(n-1)$ способов размещения a и b рядом. Каждому из этих способов соответствует $(n-2)!$ перестановок других элементов. Следовательно, число перестановок, в которых a и b стоят рядом, равно $2 \cdot (n-1) \cdot (n-2)! = 2 \cdot (n-1)!$. Поэтому искомое число перестановок равно $n! - 2 \cdot (n-1)! = (n-1)! \cdot (n-2)$. $\blacksquare$

Задача 4. Сколькими способами можно расположить на шахматной доске 8 ладей так, чтобы они не могли бить друг друга?

Решение. При указанном расположении ладей на каждой вертикали и каждой горизонтали стоит лишь одна ладья. Рассмотрим одно из таких расположений ладей. Пусть a_1 — номер вертикали, в которой стоит ладья из первой горизонтали, a_2 — номер вертикали, в которой стоит ладья из второй горизонтали, $\ldots$, a_8 — номер вертикали, в которой стоит ладья из восьмой горизонтали, Тогда $(a_1, a_2, \ldots, a_8)$ есть некоторая перестановка чисел $1, 2, \ldots, 8$. Среди чисел $a_1, a_2, \ldots, a_8$ нет ни одной пары равных, иначе две ладьи попали бы на одну вертикаль. Следовательно, каждому расположению ладей соответствует определенная перестановка чисел $1, 2, \ldots, 8$. Наоборот, каждой перестановке чисел $1, 2, \ldots, 8$ соответствует такое расположение ладей, при котором они не бьют друг друга. Следовательно, число искомых расположений ладей равно $P_8 = 8! = 40\,320$. $\blacksquare$

1.5. Сочетания.

Определение 1. *Пусть $n, k \in N_0$, $k \le n$ и $B = \{b_1, b_2, \ldots, b_n\}$ — n-элементное множество. Всякое k-элементное подмножество B называется сочетанием из n элементов этого множества по k элементов.*

Совершенно очевидно, что количество всевозможных сочетаний по k элементов множества B *не зависит* от природы элементов множества B. В силу этого, количество всевозможных сочетаний произвольного n-элементного множества по k элементов обозначим через C_n^k.

Пример 1. Рассмотрим множество $B = \{1, 2, 3, 4\}$. Все сочетания этого множества по 2 элемента: $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$. Таким образом, $C_4^2 = 6$.

Теорема 1. *Число всех k-элементных подмножеств множества из n элементов*

$$C_n^k = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} = \frac{n!}{k!(n-k)!}. \tag{1}$$

Доказательство. Формула для числа сочетаний легко получается из выведенных раннее формул для числа размещений и перестановок. В самом деле, составим вначале все сочетания из n элементов по k, а потом переставим входящие в каждое сочетание элементы всеми возможными способами. При этом получатся все размещения из n элементов по k, причем каждое только по одному разу. Но из каждого k-сочетания можно сделать P_k перестановок, а число этих сочетаний равно C_n^k. Значит, справедлива формула

$$A_n^k = P_k \cdot C_n^k.$$

Отсюда находим, что

$$C_n^k = \frac{A_n^k}{P_k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}. \blacksquare$$

Задача 1. Сколькими способами читатель может выбрать 3 книжки из 5?

Решение. Искомое число способов равно числу 3-элементных подмножеств 5-элементного множества:

$$C_5^3 = \frac{5!}{3! \cdot 2!} = 10. \blacksquare$$

Задача 2. Сколькими способами из 7 человек можно выбрать комиссию, состоящую из 3 человек?

Решение. Чтобы рассмотреть все возможные комиссии, нужно рассмотреть все возможные 3-элементные подмножества множества, состоящего из 7 человек. Искомое число способов равно

$$C_7^3 = \frac{7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3} = 35. \blacksquare$$

Задача 3. В турнире принимали участие n шахматистов, и каждые 2 шахматиста встретились 1 раз. Сколько партий было в турнире?

Решение. Партий было сыграно столько, сколько можно выделить 2-элементных подмножеств в множестве из n элементов, то есть

$$C_n^2 = \frac{n(n-1)}{1 \cdot 2}. \blacksquare$$

Задача 4. В скольких точках пересекаются диагонали выпуклого n-угольника, если никакие 3 из них не пересекаются в одной точке?

Решение. Каждой точке пересечения двух диагоналей соответствует 4 вершины n-угольника, а каждым 4 вершинам n-угольника соответствует 1 точка пересечения (точка пересечения диагоналей четырехугольника с вершинами в данных 4 точках). Поэтому число всех точек пересечения равно числу способов, которыми среди n вершин можно выбрать 4 вершины:

$$C_n^4 = \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4} = \frac{n(n-1)(n-2)(n-3)}{24}. \blacksquare$$

1.6. Некоторые свойства сочетаний.

Теорема 1. *Имеет место равенство*

$$C_n^k = C_{n-1}^k + C_{n-1}^{k-1}.$$

В справедливости этого равенства можно убедиться используя формулу

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Советуем читателю провести это самостоятельно. Приведем другое
Доказательство. Рассмотрим некоторый элемент a множества A, состоящего из n элементов, и все k-элементные подмножества множества A (число их равно C_n^k). Все k-элементные подмножества разделим на 2 группы: подмножества, в состав которых входит a, и подмножества, в состав которых a не входит. Число подмножеств в первой группе равно C_{n-1}^{k-1}, так как каждое такое подмножество получается присоединением к a некоторого $(k-1)$-элементного подмножества множества $A\backslash\{a\}$. Число подмножеств во второй группе равно C_{n-1}^k, так как каждое такое подмножество есть k-элементное подмножество множества $A \setminus \{a\}$. Следовательно, $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$. $\blacksquare$

Теорема 2. *Имеет место равенство*

$$C_n^k = C_n^{n-k}.$$

Доказательство. Имеем:

$$C_n^{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = C_n^k. \blacksquare$$

Теорема 3. *Имеет место равенство*

$$C_{n+m}^n = C_{n+m}^m.$$

Доказательство проводится непосредственной проверкой с помощью формулы (1).

Теорема 4. *Имеет место равенство*

$$\sum_{k=0}^{n} C_n^k = 2^n.$$

Доказательство. В самом деле, поскольку C_n^k — число k-элементных подмножеств n-элементного множества, то сумма в левой части равенства есть число всех подмножеств, которое равно 2^n. $\blacksquare$

1.7. Новые термины. Правило умножения (основное правило комбинаторики). Правило сложения. Размещения. Перестановки. Сочетания.

1.8. Упражнения.

1. На вершину горы ведет 7 дорог. Сколькими способами турист может подняться на гору и спуститься с нее? Дайте ответ на тот же самый вопрос, если подъем и спуск осуществляется различными путями.

2. Сколько четырехзначных чисел можно составить из цифр 0, 1, 2, 3, 4, 5, если:

   (a) цифры могут повторяться;

   (b) числа должны быть нечетные (цифры могут повторяться)?

3. Сколько трехзначных чисел можно составить из цифр 1, 2, 3, 4, 5?

4. Сколько трехзначных чисел можно составить из цифр 1, 2, 3, 4, 5, если каждую из этих цифр можно использовать не более одного раза?

5. Сколькими способами 7 человек могут разместиться в очереди в кассу?

6. В классе изучают 10 предметов. В понедельник 6 уроков, причем все уроки разные. Сколькими способами можно составить расписание на понедельник?

7. Сколько имеется пятизначных чисел, которые делятся на 5?

8. Флаг составляется из 13 горизонтальных полос красного, белого и голубого цвета, причем любые две соседние полосы должны быть разных цветов. Сколькими способами это можно осуществить?

9. На одной из боковых сторон треугольника взято n точек, на другой — m точек. Каждая из вершин при основании треугольника соединена прямыми с точками, взятыми на противоположной стороне.

   (a) Сколько точек пересечения этих прямых образуется внутри треугольника?

   (b) На сколько частей делят треугольник эти прямые?

10. Сколько есть двузначных чисел, у которых обе цифры четные?

11. Сколько есть пятизначных чисел, у которых все цифры нечетные?

12. Сколько есть трехзначных чисел, которые записываются с помощью цифр 0, 1, 2, 3, 4, 5, и делятся на 3?

13. Сколько есть пятизначных чисел, которые одинаково читаются слева направо и справа налево (например таких, как 67876, 17071)?

14. 5 мальчиков и 5 девочек садятся в ряд на 10 расположенных подряд стульев, причем мальчики садятся на места с нечетными номерами, а девочки — на места с четными номерами. Сколькими способами это можно сделать?

15. В селении живут 1500 жителей. Доказать, что по крайней мере двое из них имеют одинаковые инициалы.

16. Сколькими способами можно упорядочить множество $\{1, \ldots, n\}$ так, чтобы числа 1, 2, 3 стояли рядом и в порядке возрастания?

17. В комнате студенческого общежития живут трое студентов. У них есть 4 чашки, 5 блюдец, и 6 чайных ложек (все чашки, блюдца и ложки отличаются друг от друга). Сколькими способами они могут накрыть стол для чаепития (каждый получает одну чашку, одно блюдце и одну ложку)?

18. Сколькими способами из 30 учащихся можно выбрать делегацию, состоящую из 3 учащихся?

19. В комнате n лампочек. Сколько всего разных способов освещения комнаты, при которых горит ровно k лампочек? Сколько всего может быть различных способов освещения комнаты?

20. Дано n точек, никакие 3 из которых не лежат на одной прямой. Сколько прямых можно провести, соединяя точки попарно?

21. На плоскости проведено n прямых так, что никакие 2 из них не параллельны и никакие 3 не пересекаются в одной точке.

    (a) Найти количество точек пересечения этих прямых.

    (b) Сколько треугольников образуют эти прямые?

    (c) На сколько частей делят плоскость эти прямые?

    (d) Сколько среди них ограниченных частей и сколько неограниченных?

22. Сколько имеется четырехзначных чисел, у которых каждая следующая цифра больше предыдущей?

23. Сколько имеется четырехзначных чисел, у которых каждая следующая цифра меньше предыдущей?

24. Пять девушек и трое юношей играют в городки. Сколькими способами они могут разбиться на команды по 4 человека в каждой команде. если в каждой команде должно быть хотя бы по одному юноше?

25. У одного человека есть 7 книг по математике, а у другого — 9 книг, Сколькими способами они могут обменять книгу одного на книгу другого?

26. Та же самая задача, но меняются две книги одного на две книги другого.

27. У мамы 2 яблока и 3 груши. Каждый день в течение пяти дней подряд она выдает по одному фрукту. Сколькими способами это может быть сделано?

28. Из группы, состоящей из 7 мужчин и 4 женщин, надо выбрать 6 человек так, чтобы среди них было не менее двух женщин. Сколькими способами это можно сделать?

29. Рота состоит из 3 офицеров, 6 сержантов и 60 рядовых. Сколькими способами можно Образовать из них отряд, состоящий из одного офицера, двух сержантов и 20 рядовых? Та же задача, если в отряд должен войти командир роты и старший из сержантов?

§ 2. Размещения, перестановки и сочетания с повторениями. Бином Ньютона и полиномиальная формула

Размещения с повторениями $\overline{A}_n^k$. Перестановки с повторениями. Полиномиальные коэффициенты. Сочетания с повторениями f_n^k. Формулы для вычисления $\overline{A}_n^k$, полиномиальных коэффициентов и f_n^k. Бином Ньютона. Треугольник Паскаля. Полиномиальная теорема.

2.1. Размещения с повторениями.

Определение 1. *Пусть $n, k \in N_0$ и $B = \{b_1, b_2, \ldots, b_n\}$. Размещением с повторениями из n элементов множества B по k элементов называется всякая последовательность длины k, составленная из элементов этого множества (в последовательности возможны повторяющиеся элементы).*

Очевидно, что количество всевозможных размещений с повторениями из элементов множества B по k элементов не зависит от природы элементов множества B. По этой причине через $\overline{A}_n^k$ обозначим количество всевозможных размещений с повторениями n-элементного множества по k элементов.

Пример 1. Пусть $C = \{a, b, c\}$. Все размещения с повторениями по 2 этого множества: (a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c).

Таким образом, $\overline{A}_3^2 = 9$.

Теорема 1. *Число размещений с повторениями*

$$\overline{A}_n^k = n^k.$$

Доказательство. 1-ым элементом последовательности может быть любой из n элементов множества, 2-ым — также любой из n элементов и т. д., до k-го элемента последовательности. Отсюда, по правилу умножения, $\overline{A}_n^k = \underbrace{n \cdot n \cdot \ldots \cdot n}_{k} = n^k$. ■

Задача 1. Для запирания сейфов и автоматических камер хранения применяют секретные замки, которые открываются лишь тогда, когда набрано некоторое "тайное слово". Это слово набирают с помощью одного или нескольких дисков, на которых нанесены буквы (или цифры). Пусть на диск нанесены 12 букв, а секретное слово состоит из 5 букв. Сколько неудачных попыток может быть сделано человеком не знающим секретного слова?

Решение. Общее число комбинаций равно

$$\overline{A}_{12}^5 = 12^5 = 248832.$$

Значит, неудачных попыток может быть 248831. Впрочем, обычно сейфы делают так, что после первой же неудачной попытки открыть их раздается сигнал тревоги. ■

2.2. Перестановки с повторениями.

Определение 1. *Пусть $n \in N_0$, $B = \{b_1, b_2, \ldots, b_n\}$. Перестановкой с повторениями из элементов множества B называется всякое размещение с повторениями длины n.*

Пусть $k_1, k_2, \ldots, k_m$ — целые неотрицательные числа, причем $k_1 + k_2 + \ldots + k_m = n$. Число перестановок с повторениями, в которых m различных элементов множества B и k_i элементов i-го вида $(i = 1, 2, \ldots, m)$ не зависит от природы элементов множества B. Поэтому число таких перестановок будем обозначать через $C_n(k_1, k_2, \ldots, k_m)$. Числа $C_n(k_1, k_2, \ldots, k_m)$ называются *полиномиальными коэффициентами.*

Пример 1. Пусть $A = \{a, b, c, d\}$. Тогда соответствующие перестановки с повторениями в которых 1 элемент a и 3 элемента b ($m = 2$, $k_1 = 1$, $k_2 = 3$): (a, b, b, b), (b, a, b, b), (b, b, a, b), (b, b, b, a).

То есть $C_4(1, 3) = 4$.

Теорема 1. *Пусть $k_1, k_2, \ldots, k_m$ — целые неотрицательные числа, причем $k_1+k_2+\ldots+k_m = n$. Число различных перестановок, которые можно составить из n элементов, среди которых имеется k_1 элементов первого типа, k_2 элементов второго типа, ..., k_m элементов m-го типа (полиномиальный коэффициент) равно*

$$C_n(k_1, k_2, \ldots, k_m) = \frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_m!}.$$

Доказательство. Рассмотрим одну перестановку и заменим в ней все одинаковые элементы разными. Тогда число различных перестановок, которые можно составить из рассматриваемой перестановки, равно $k_1! \cdot k_2! \cdot \ldots \cdot k_m!$. Проделав это для каждой перестановки, получим $n!$ перестановок. Следовательно,

$$C_n(k_1, k_2, \ldots, k_m) \cdot k_1! \cdot k_2! \cdot \ldots \cdot k_m! = n!,$$

что и доказывает утверждение теоремы. ■

Полиномиальные коэффициенты имеют еще одну очень важную комбинаторную интерпретацию. Пусть имеется n букв: k_1 букв a_1, k_2 букв a_2, ..., k_m букв a_m $(k_1+k_2+\ldots+k_m = n)$. Число различных слов, которые можно составить из этих букв, очевидно, равно

$$C_n(k_1, k_2, \ldots, k_m) = \frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_m!}.$$

Задача 1. Сколько различных слов можно составить, переставляя буквы слова “математика”?

Решение. Число различных слов равно

$$C_{10}(2, 2, 3, 1, 1, 1) = \frac{10!}{2! \cdot 2! \cdot 3!} = 151200. \blacksquare$$

Задача 2. Сколькими способами можно разделить $m+n+s$ предметов на 3 группы так, чтобы в первой группе было m предметов, во второй — n предметов, в третьей — s предметов?

Решение. Искомое число способов равно

$$C_{m+n+s}(m, n, s) = \frac{(m+n+s)!}{m! \cdot n! \cdot s!}. \blacksquare$$

2.3. Сочетания с повторениями.

Определение 1. *Пусть $k \in N_0$, $n \in N$. Сочетанием из n элементов по k элементов с повторениями называется совокупность, содержащая k элементов, причем каждый элемент принадлежит к одному из n типов.*

Число сочетаний из n элементов по k элементов с повторениями обозначается f_n^k.

Пример 1. Из трех букв a, b, c можно составить такие сочетания по два с повторениями: aa, bb, cc, ac, bc, ab. Таким образом, $f_3^2 = 6$.

Теорема 1. *Число различных сочетаний из n элементов по k элементов с повторениями равно*

$$f_n^k = C_{n+k-1}^{n-1} = C_{n+k-1}^k.$$

Доказательство. Каждое сочетание полностью определяется, если указать, сколько элементов каждого из n типов в него входит. Поставим в соответствие каждому сочетанию последовательность нулей и единиц, составленную по такому правилу: напишем подряд столько единиц, сколько элементов первого типа входит в сочетание, далее поставим нуль и после него напишем

столько единиц, сколько элементов второго типа входит в сочетание и т. д. Например, написанным выше сочетаниям из трех букв по две будут соответствовать такие последовательности:

$$1100,\ 0110,\ 0011,\ 1001,\ 0101,\ 1010.$$

Таким образом, каждому сочетанию из n элементов по k элементов с повторениями соответствует последовательность из k единиц и $n-1$ нулей, и наоборот, по каждой такой последовательности однозначно восстанавливается такое сочетание. Поэтому число сочетаний из n по k с повторениями равно числу последовательностей из k единиц и $n-1$ нулей.

Рассмотрим множество A последовательностей $(x_1, x_2, \ldots, x_{k+n-1})$, где числа x_i принимают только значения 0 или 1 и среди них ровно k единиц. Чтобы вычислить число элементов множества A, обратим внимание, что оно равномощно множеству всех k-элементных подмножеств множества $\{1, 2, \ldots, k+n-1\}$: подмножество чисел $\{i_1, \ldots, i_k\}$ соответствует той последовательности $(x_1, \ldots, x_{k+n-1})$, у которой $x_{i_1} = 1, \ldots, x_{i_k} = 1$. Следовательно, $|A| = C^k_{k+n-1}$. ■

Пример 2. Кости домино можно рассматривать как сочетания с повторениями из семи цифр 0, 1, 2, 3, 4, 5, 6 по две. Число всех таких сочетаний равно

$$f_7^2 = C_8^2 = \frac{8 \cdot 7}{2} = 28.$$

Задача 1. Сколько целых неотрицательных решений имеет уравнение

$$x_1 + x_2 + \ldots + x_n = k?$$

Решение. Если имеем целые неотрицательные числа $x_1, \ldots, x_n$ такие, что $x_1 + \ldots + x_n = k$, то можем составить сочетание из n элементов по k с повторениями взяв x_1 элементов первого типа, x_2 — второго типа, $\ldots$, x_n — n-го типа. Наоборот, имея сочетание из n элементов по k, получим решение уравнения $x_1 + \ldots + x_n = k$ (x_1 элементов первого типа, x_2 — второго типа, $\ldots$, x_n — n-го типа) в целых неотрицательных числах. Следовательно, существует биекция между множеством всех сочетаний из n элементов по k с повторениями и множеством всех целых неотрицательных решений уравнения $x_1 + \ldots + x_n = k$. Поэтому число решений равно $f_n^k = C^{n-1}_{n+k-1} = C^k_{n+k-1}$. ■

2.4. Бином Ньютона.

Известно, что

$$(a+b)^2 = a^2 + 2ab + b^2,$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

Как раскрывать скобки при вычислении выражения $(a+b)^n$? Ответ на этот вопрос дает следующая

Теорема 1. *Имеет место равенство*

$$(a+b)^n = C_n^0 a^n b^0 + C_n^1 a^{n-1} b^1 + \ldots + C_n^k a^{n-k} b^k + \ldots + C_n^n a^0 b^n, \tag{1}$$

где $C_n^k = \dfrac{n!}{k!(n-k)!}$.

Формулу (1) можно записать в виде

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$

Доказательство. Перемножим последовательно $(a+b)$ n раз. Тогда получим сумму 2^n слагаемых вида $d_1 \ldots d_n$, где d_i $(i = 1, \ldots, n)$ равно либо a, либо b. Разобьем все слагаемые на $n+1$ группу $B_0, \ldots, B_n$, отнеся к B_k все те произведения, в которых b встречается множителем k раз,

а a — $(n-k)$ раз. Число произведений в B_k равно, очевидно, C_n^k (таким числом способов среди n множителей $d_1, d_2, \ldots, d_n$ можно выбрать k множителей, которые будут равны b), а каждое слагаемое в B_k равно $a^{n-k}b^k$. Поэтому

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$

Теорема доказана. ■

Эту теорему иногда называют *биномиальной теоремой,* а числа C_n^k — *биномиальными коэффициентами.* Равенство (1) часто называют *биномом Ньютона.*

Напомним следующее важное свойство биномиальных коэффициентов:

$$C_{n+1}^k = C_n^k + C_n^{k-1}. \tag{2}$$

Оно было установлено в п. II.1.5.

Равенство (2) показывает, что биномиальные коэффициенты можно последовательно выписывать в виде треугольной таблицы, которая называется *треугольником Паскаля:*

$$\begin{array}{ccccccccccc}
 & & & & 1 & & 1 & & & & n=1 \\
 & & & 1 & & 2 & & 1 & & & n=2 \\
 & & 1 & & 3 & & 3 & & 1 & & n=3 \\
 & 1 & & 4 & & 6 & & 4 & & 1 & n=4 \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \quad n=5 \\
 & & & & \ldots & & & & & &
\end{array}$$

В n-ой строке треугольника Паскаля стоят коэффициенты разложения $(a+b)^n$, причем каждый коэффициент, кроме крайних двух, которые равны 1, равен сумме соответствующих коэффициентов из предыдущей строки.

2.5. Полиномиальная теорема. Рассмотрим вопрос о том, как раскрывать скобки при вычислении выражения вида

$$(a_1 + a_2 + \ldots + a_k)^n.$$

Ответ на этот вопрос дает следующая

Теорема 1. *Выражение*

$$(a_1 + a_2 + \ldots + a_k)^n$$

равно сумме всех возможных слагаемых вида

$$\frac{n!}{r_1! r_2! \ldots r_k!}\, a_1^{r_1} a_2^{r_2} \ldots a_k^{r_k},$$

где $r_1 + r_2 + \ldots + r_k = n$, *то есть*

$$(a_1 + a_2 + \ldots + a_k)^n = \sum_{\substack{r_1 \geq 0, \ldots, r_k \geq 0 \\ r_1 + \ldots + r_k = n}} \frac{n!}{r_1! r_2! \ldots r_k!}\, a_1^{r_1} a_2^{r_2} \ldots a_k^{r_k}. \tag{3}$$

Доказательство. Перемножим последовательно $a_1 + \ldots + a_k$ n раз. Тогда получим k^n слагаемых вида $d_1 \ldots d_n$, где каждый множитель d_i равен или a_1, или a_2, ..., или a_k. Обозначим через $B(r_1, \ldots, r_k)$ совокупность всех тех слагаемых, где a_1 встречается множителем r_1 раз, a_2 — r_2 раз, ..., a_k — r_k раз. Число таких слагаемых равно $C_n(r_1, \ldots, r_k)$ (см. п. II.2.2.). Но

$$C_n(r_1, \ldots, r_k) = \frac{n!}{r_1! r_2! \ldots r_k!}.$$

Следовательно,

$$(a_1 + a_2 + \ldots + a_k)^n = \sum_{\substack{r_1 \geq 0, \ldots, r_k \geq 0 \\ r_1 + \ldots + r_k = n}} \frac{n!}{r_1! r_2! \ldots r_k!} a_1^{r_1} a_2^{r_2} \ldots a_k^{r_k}. \blacksquare$$

Данная теорема называется *полиномиальной.*

При $n = 2$ равенство (3) принимает вид

$$(a_1 + a_2)^n = \sum_{r=0}^{n} \frac{n!}{r!(n-r)!} a_1^{n-r} a_2^r.$$

Таким образом, формула бинома Ньютона является частным случаем полиномиальной формулы.

2.6. Биномиальные тождества. Числа C_n^k имеют ряд важных свойств. Укажем некоторые из них и установим ряд интересных тождеств, которым удовлетворяют биномиальные коэффициенты.

Рассмотрим следующие равенства:

$$C_n^k = C_n^{n-k}, \tag{4}$$
$$C_{n+1}^k = C_n^k + C_n^{k-1}, \tag{5}$$
$$C_n^0 + C_n^1 + \ldots + C_n^n = 2^n, \tag{6}$$
$$C_n^0 - C_n^1 + C_n^2 - \ldots + (-1)^n C_n^n = 0. \tag{7}$$

Равенство (4) легко проверяется вычислением. Равенства (5) и (6) были получены ранее (равенство (6) можно получить также взяв в формуле бинома $a = b = 1$). Если в формуле бинома Ньютона положить $a = 1$, $b = -1$, то получим равенство (7).

2.7. Новые термины. Размещения с повторениями. Перестановки с повторениями. Сочетания с повторениями. Полиномиальные коэффициенты. Бином Ньютона. Треугольник Паскаля. Биномиальные коэффициенты. Полиномиальная теорема. Биномиальные тождества.

2.8. Упражнения.

1. Сколько различных слов можно составить, переставляя буквы слова “мама”? Напишите все эти слова.

2. Сколько пятибуквенных слов можно составить из букв a, b, c, если известно, что буква a встречается в слове не более двух раз, буква b — не более одного раза, буква c — не более трех раз?

3. Напишите все сочетания с повторениями из трех предметов a, b, c по 3.

4. Сколькими способами можно выбрать 6 одинаковых или разных пирожных в кондитерской, где есть 11 разных сортов пирожных?

5. Сколько целых положительных корней имеет уравнение

$$x_1 + \ldots + x_m = n?$$

6. Сколько целых неотрицательных решений имеет неравенство

$$x_1 + \ldots + x_m \leq n?$$

7. Сколькими способами можно раздать 18 различных предметов 5 ученикам так, чтобы четверо из них получили по 4 предмета, а пятый — 2 предмета. Та же задача, но трое получают по 4 предмета, а двое — по 3 предмета.

8. Сколькими способами можно расставить 12 белых и 12 черных шашек на черные поля доски так, чтобы это положение было симметрично относительно центра доски?

9. Сколькими способами два человека могут разделить $2n$ предметов одного вида, $2n$ предметов второго вида и $2n$ предметов третьего вида так, чтобы каждый получил по $3n$ предметов.

10. Найти число всех разбиений n-элементного множества.

11. Указать наибольшее среди чисел C_n^k $(k = 0, 1, \ldots, n)$.

12. Найти n, если известно, что в разложении $(1+x)^n$ коэффициенты при x^5 и x^{12} равны.

13. Сколько рациональных членов содержит разложение

$$(\sqrt{2} + \sqrt[4]{3})^{100}?$$

14. Пользуясь полиномиальной теоремой, вычислить $(x+y+z)^3$.

15. Чему равен коэффициент при $x^2y^3z^2$ в выражении $(x+y+z)^7$?

16. Доказать, что числа $C_p^1, C_p^2, \ldots, C_p^{p-1}$ делятся на p, если p — простое число.

17. Доказать, что разность $a^p - a$ при любом целом a делится на p, если p — простое число (*малая теорема Ферма*).

18. В классе $2n$ предметов. Все ученики учатся на 4 и 5. Никакие 2 из них не учатся одинаково, ни о каких двух из них нельзя сказать, что один из них учится лучше другого. Доказать, что число учеников в классе не превышает C_{2n}^n.

19. Вычислить сумму: $C_n^0 + C_n^4 + C_n^8 + \ldots$

20. Вычислить сумму: $C_n^1 + C_n^3 + C_n^5 + \ldots$

Глава III

Алгебра высказываний

§ 1. Построение алгебры высказываний

Высказывания: простые, составные, конкретные и переменные. Логические операции над высказываниями. Формулы, логические возможности формулы. Тождественно истинные, тождественно ложные и равносильные формулы. Таблицы истинности. Свойства операций над высказываниями. Алгебра высказываний.

1.1. Простые и составные высказывания. Высказывательные переменные. Понятие *высказывания* является одним из первичных неопределяемых понятий в математике. Определенное представление о смысле этого понятия дает следующее его описание. *Высказывание — это предложение, относительно которого имеет смысл утверждать, истинно оно или ложно.* Таким образом, отличительной особенностью высказываний является возможность принимать одно из двух значений: истина — 1, или ложь — 0. Эти значения называются *истинностными значениями.*

Высказывания могут быть *простыми* или *составными.*

Если в высказывании A нельзя выделить некоторую часть, которая сама является высказыванием и не совпадает по смыслу с высказыванием A, то A называется простым высказыванием. В противном случае высказывание A называется составным.

Простые высказывания (а в некоторых случаях и составные) будем обозначать большими буквами латинского алфавита, а факт истинности или ложности высказывания: $A = 1$ или $A = 0$. Подобно тому, как в школьной математике рассматривались конкретные числа и неизвестные или переменные числа, обозначенные той или иной буквой, так и здесь мы будем рассматривать всякую большую букву латинского алфавита как некоторое переменное высказывание, которое может принимать значения 0 или 1 , если не сказано, что данная буква обозначает какое-то конкретное высказывание. Буквы, обозначающие переменные высказывания, будем называть *высказывательными переменными.*

1.2. Основные логические связки. Конструирование составных высказываний из простых осуществляется при помощи связок, см. таблицу 1.

1.3. Логические операции над высказываниями. Во избежание неодинаковой трактовки смысла каждой из связок определим этот смысл следующими ниже таблицами 2–6.

1.4. Формулы и их логические возможности.

Определение 1. *Формулами называются:*

1) большие буквы латинского алфавита, снабженные, быть может, штрихами или индексами и обозначающие высказывания или высказывательные переменные

2) если $\mathfrak{a}$ *и* $\mathfrak{b}$ *— формулы, то выражения:*

$$\neg\mathfrak{a},\ (\mathfrak{a}\ \&\ \mathfrak{b}),\ (\mathfrak{a}\vee\mathfrak{b}),\ (\mathfrak{a}\to\mathfrak{b}),\ (\mathfrak{a}\sim\mathfrak{b})$$

также являются формулами;

3) Других формул, кроме тех, которые определены пунктами 1) и 2), нет.

Табл. 1: Основные логические связки.

Связки	Обозначения	Название соответствующих операций
нет; не; неверно; ...	$\neg$ ($\overline{\ }$)	отрицание
и; а; но; ...	& ($\wedge$)	конъюнкция
или; либо; ...	$\vee$	дизъюнкция
следует; влечет; если ..., то ...; тогда; вытекает ...	$\rightarrow$	импликация
эквивалентно; равносильно; если и только если; тогда и только тогда; в том и только в том случае; ...	$\sim$ ($\leftrightarrow$)	эквиваленция

Табл. 2: Логическая связка $\neg$.

A	$\neg A$
1	0
0	1

Табл. 3: Логическая связка &.

A	B	A & B
1	1	1
1	0	0
0	1	0
0	0	0

Табл. 4: Логическая связка $\vee$.

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

Табл. 5: Логическая связка $\rightarrow$.

A	B	$A \rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Табл. 6: Логическая связка $\sim$.

A	B	$A \sim B$
1	1	1
1	0	0
0	1	0
0	0	1

Формулы будем обозначать малыми готическими буквами: $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ... Если $A_1, A_2, \ldots, A_n$ — все буквы, участвующие в записи формулы $\mathfrak{a}$, то будем писать $\mathfrak{a} = \mathfrak{a}(A_1, A_2, \ldots, A_n)$. Например, $\mathfrak{a}(A) = \neg A$, $\mathfrak{b}(A_1, A_2, A_3) = (A_3 \to (A_2 \to A_1))$, $\mathfrak{c}(A, B, C) = ((A \vee B) \to C)$ и т. д. Для уменьшения количества скобок в формулах условимся считать, что связка $\neg$ связывает высказывания сильнее, чем все остальные связки, $\&$ и $\vee$ — сильнее, чем $\to$ и $\sim$. Кроме того, внешние скобки будем иногда опускать.

Определение 2. *Логической возможностью формулы $\mathfrak{a}(A_1, A_2, \ldots, A_n)$ от высказывательных переменных $A_1, A_2, \ldots, A_n$ называется всякий набор конкретных значений истинности для букв $A_1, A_2, \ldots, A_n$.*

Таблица, содержащая перечень всевозможных логических возможностей формулы $\mathfrak{a}$, называется таблицей логических возможностей этой формулы.

Так, например, всякая формула от одной буквы имеет две логические возможности: 0 и 1. Всякая формула от двух букв имеет четыре логических возможности: $(1, 1)$, $(1, 0)$, $(0, 1)$, $(0, 0)$.

Таблица вида

1	1
1	0
0	1
0	0

является таблицей логических возможностей для всякой формулы от 2 букв (высказывательных переменных) A и B.

1.5. Равносильные формулы.

Определение 1 (общей логической возможности). *Пусть $\mathfrak{a}$ и $\mathfrak{b}$ две формулы, а $A_1, A_2, \ldots, A_n$ все высказывательные переменные, входящие в запись хотя бы одной из этих формул. Общей логической возможностью формул $\mathfrak{a}$ и $\mathfrak{b}$ называется всякий набор конкретных значений истинности для высказывательных переменных $A_1, A_2, \ldots, A_n$.*

Можно определить понятие общей логической возможности для любого конечного числа формул.

Определение 2 (равносильных формул). *Две формулы $\mathfrak{a}$ и $\mathfrak{b}$ называются равносильными: $\mathfrak{a} \equiv \mathfrak{b}$, если во всякой общей для $\mathfrak{a}$ и $\mathfrak{b}$ логической возможности $\mathfrak{a}$ и $\mathfrak{b}$ принимают одинаковые значения.*

Теорема 1. *Отношение $\equiv$ на множестве всех формул от букв из некоторого алфавита $\mathfrak{M}$ является отношением эквивалентности.*

Доказательство проведите самостоятельно.

1.6. Тавтологии и противоречия. Таблицы истинности.

Определение 1 (тавтологии и противоречия). *Формула* $\mathfrak{a}$ *называется тождественно истинной (тождественно ложной) или тавтологией (противоречием) и обозначается:* $\mathfrak{a} \equiv 1$ $(\mathfrak{a} \equiv 0)$, *если во всех логических возможностях она принимает одно и то же значение, равное 1 (равное 0). Запись* $\models \mathfrak{a}$ *означает, что* $\mathfrak{a}$ *— тавтология.*

Теорема 1. *Для любых двух формул* $\mathfrak{a}$ *и* $\mathfrak{b}$ *истинно утверждение:*

$$\mathfrak{a} \equiv \mathfrak{b} \Longleftrightarrow \models (\mathfrak{a} \sim \mathfrak{b}).$$

Доказательство проведите самостоятельно.

Определение 2 (таблицы истинности). *Таблица, в которой приведен перечень всех логических возможностей формулы* $\mathfrak{a}$ *(общих логических возможностей формул* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$*) вместе с указанием значений* $\mathfrak{a}$ *(значений* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$*) в каждой логической возможности (общей логической возможности), называется таблицей истинности формулы* $\mathfrak{a}$ *(формул* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$*).*

1.7. Свойства логических операций (законы логики).

Теорема 1. *Для любых логических формул* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ *истинны следующие равносильности.*

1. *Закон двойного отрицания:*

   $\neg\neg\mathfrak{a} \equiv \mathfrak{a}$.

2. *Идемпотентность операций* $\&$ *и* $\vee$*:*

   $\mathfrak{a} \,\&\, \mathfrak{a} \equiv \mathfrak{a}$, $\mathfrak{a} \vee \mathfrak{a} \equiv \mathfrak{a}$.

3. *Коммутативность операций* $\&$ *и* $\vee$*:*

   $\mathfrak{a} \,\&\, \mathfrak{b} \equiv \mathfrak{b} \,\&\, \mathfrak{a}$, $\mathfrak{a} \vee \mathfrak{b} \equiv \mathfrak{b} \vee \mathfrak{a}$.

4. *Ассоциативность операций* $\&$ *и* $\vee$*:*

   $\mathfrak{a} \,\&\, (\mathfrak{b} \,\&\, \mathfrak{c}) \equiv (\mathfrak{a} \,\&\, \mathfrak{b}) \,\&\, \mathfrak{c}$, $\mathfrak{a} \vee (\mathfrak{b} \vee \mathfrak{c}) \equiv (\mathfrak{a} \vee \mathfrak{b}) \vee \mathfrak{c}$.

5. *Дистрибутивные законы каждой из операций* $\&$ *и* $\vee$ *относительно другой:*

   $\mathfrak{a} \,\&\, (\mathfrak{b} \vee \mathfrak{c}) \equiv (\mathfrak{a} \,\&\, \mathfrak{b}) \vee (\mathfrak{a} \,\&\, \mathfrak{c})$, $\mathfrak{a} \vee (\mathfrak{b} \,\&\, \mathfrak{c}) \equiv (\mathfrak{a} \vee \mathfrak{b}) \,\&\, (\mathfrak{a} \vee \mathfrak{c})$.

6. *Законы поглощения:*

   $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b}) \equiv \mathfrak{a}$, $\mathfrak{a} \vee (\mathfrak{a} \,\&\, \mathfrak{b}) \equiv \mathfrak{a}$.

7. *Законы де Моргана:*

   $\neg(\mathfrak{a} \,\&\, \mathfrak{b}) \equiv \neg\mathfrak{a} \vee \neg\mathfrak{b}$, $\neg(\mathfrak{a} \vee \mathfrak{b}) \equiv \neg\mathfrak{a} \,\&\, \neg\mathfrak{b}$.

8. *Закон исключенного третьего:*

   $\mathfrak{a} \vee \neg\mathfrak{a} \equiv 1$,

9. *Закон противоречия:*

   $\mathfrak{a} \,\&\, \neg\mathfrak{a} \equiv 0$.

10. *Свойства тавтологии и противоречия:*

    $\mathfrak{a} \,\&\, 1 \equiv \mathfrak{a} \qquad \mathfrak{a} \vee 0 \equiv \mathfrak{a}$,
    $\mathfrak{a} \vee 1 \equiv 1 \qquad \mathfrak{a} \,\&\, 0 \equiv 0$,
    $\neg 1 \equiv 0 \qquad\quad \neg 0 \equiv 1$.

11. *Закон контрапозиции:*

    $\mathfrak{a} \to \mathfrak{b} \equiv \neg\mathfrak{b} \to \neg\mathfrak{a}$.

12. Правило исключения импликации:

$\mathfrak{a} \to \mathfrak{b} \equiv \neg\mathfrak{a} \vee \mathfrak{b}$,

13. Правило исключения эквиваленции:

$\mathfrak{a} \sim \mathfrak{b} \equiv (\mathfrak{a} \to \mathfrak{b}) \,\&\, (\mathfrak{b} \to \mathfrak{a})$.

Доказательство. Свойства 1–4, 8–10 непосредственно следуют из определения соответствующих операций. Все остальные свойства доказываются стандартным методом — составлением и сравнением таблиц истинности для левой и правой части доказываемой равносильности. ■

Проведите эти доказательства самостоятельно.

1.8. Алгебра высказываний. Пусть $\mathfrak{M}$ — некоторое множество больших латинских букв, снабженных, быть может, штрихами или индексами, то есть $\mathfrak{M}$ — некоторое множество высказывательных переменных. $\Phi(\mathfrak{M})$ — множество всевозможных формул от букв из $\mathfrak{M}$. Понятно, что применение логических операций $\neg$, $\&$, $\vee$, $\to$, $\sim$ к формулам из $\Phi(\mathfrak{M})$ дает снова формулы из $\Phi(\mathfrak{M})$, то есть $\Phi(\mathfrak{M})$ замкнуто относительно этих операций и, следовательно, является алгеброй, которую обозначим через $\langle \Phi(\mathfrak{M}), \neg, \&, \vee, \to, \sim \rangle$ и будем называть *алгеброй высказываний* в алфавите $\mathfrak{M}$.

1.9. Новые термины. Высказывания: простые и составные. Значения истинности: 0 и 1. Высказывательные переменные. Логические операции над высказываниями: отрицание, конъюнкция, дизъюнкция, импликация, эквиваленция. Логическая возможность формулы. Общая логическая возможность двух формул. Равносильные формулы. Тавтологии и противоречия. Таблица истинности. Законы логики: двойного отрицания, идемпотентности, коммутативности, ассоциативности, дистрибутивности, поглощения, де-Моргана, исключенного третьего, противоречия, контрапозиции, правила исключения импликации и эквиваленции. Алгебра высказываний.

1.10. Контрольные вопросы.

1. Приведите примеры высказываний (истинных и ложных) и предложений, не являющихся высказываниями.
2. Является ли высказывание “неверно, что 6 делится на 3” простым?
3. Покажите на примере, что значение истинности составного высказывания зависит от типа связок, участвующих в образовании составного высказывания.
4. Подсчитайте количество логических возможностей формулы от 3-х высказывательных переменных, 4-х высказывательных переменных.
5. Перечислите общие логические возможности формул

   $A \to \neg A$ и $(A \to \neg A) \,\&\, (B \vee \neg B)$.
6. Можно ли описание формул, приведенное в п. III.1.4. считать определением? Почему?
7. Дайте словесное определение операциям $\neg$, $\&$, $\vee$, $\to$, $\sim$. Их табличное определение см. в п. III.1.3.
8. Известно, что высказывание $A \to B$ истинно. Что можно сказать об истинности высказываний A и B?
9. Известно, что высказывание $A \to B$ ложно. Что можно сказать об истинности A и B?
10. Известно, что $A \to B$ и A истинны. Что можно сказать об истинности B?
11. $A \sim B$ истинно. Что можно сказать об истинности формул $\neg A \sim B$ и $A \to B$?
12. $A \,\&\, \neg B$ и $A \sim B$ ложны. Что можно сказать об истинности A и B?

13. Равносильны ли формулы задания 5?

14. Не прибегая к записям докажите законы логики 1–4, 6, 8–10.

15. Сколько существует попарно неравносильных формул от одной высказывательной переменной. От двух высказывательных переменных?

1.11. Упражнения.

1. Обозначив простые высказывания большими латинскими буквами, а логические связки соответствующими символами, записать в виде формул следующие высказывания:

   "если диагонали параллелограмма взаимно перпендикулярны или являются биссектрисами углов, то этот параллелограмм есть ромб";

   "если при пересечении двух прямых третьей, внутренние накрестлежащие углы равны, то эти прямые параллельны";

   "если целое число положительно и является четным, то либо оно простое либо больше двух";

2. Пусть буквы A, B, C, D обозначают высказывания:

   A — "это число является целым",

   B — "это число положительно",

   C — "это число является простым",

   D — "данное число делится на три".

   Переведите на обычный язык следующие формулы: $A \vee B$, $A \,\&\, B$, $A \vee \neg A$, $B \,\&\, \neg B$, $D \sim C$, $(A \,\&\, C) \to \neg D$, $(A \,\&\, D) \to \neg C$, $(A \vee B) \,\&\, (C \vee D)$, $\neg A \vee \neg D$, $(A \,\&\, B \,\&\, C) \vee D$.

   Какие из сформулированных высказываний являются истинными?

3. Составьте таблицу логических возможностей для формулы от трех букв. Для формулы от четырех букв.

4. Докажите, что формула от n букв имеет 2^n логических возможностей.

5. Придумайте удобный способ построения таблицы логических возможностей для формулы от n букв.

6. Докажите теорему п. III.1.5. и п. III.1.7.

7. Внимательно изучите доказательство одного из законов поглощения, приведенное ниже.

$$\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b}) \equiv \mathfrak{a}$$

   а) Пусть в некоторой логической возможности формула $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b})$ принимает значение, равное 1, то есть $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b}) = 1$. По определению операции & отсюда следует, что $\mathfrak{a} = 1$. Так что, если $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b}) = 1$, то и $\mathfrak{a} = 1$.

   б) Пусть теперь в какой-то логической возможности $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b}) = 0$. По определению операции &, отсюда следует, что $\mathfrak{a} = 0$ или же $\mathfrak{a} \vee \mathfrak{b} = 0$. Если $\mathfrak{a} \vee \mathfrak{b} = 0$, то из определения операции $\vee$ вытекает, что $\mathfrak{a} = 0$. Таким образом, все равно $\mathfrak{a} = 0$. То есть, если $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b}) = 0$, то и $\mathfrak{a} = 0$.

   Из а) и б) получаем, что формулы $\mathfrak{a} \,\&\, (\mathfrak{a} \vee \mathfrak{b})$ и $\mathfrak{a}$ в любой логической возможности принимают одинаковые значения истинности, что означает, что эти формулы равносильны.

   Воспроизведите схему приведенного способа доказательства равносильности формул. Что вы можете сказать о таком методе и методе составления таблиц истинности в плане их сравнения?

8. Способом, указанном в предыдущем упражнении докажите ассоциативность операции $\vee$, дистрибутивность операции $\&$ относительно $\vee$, не доказанный вами закон де-Моргана, правила исключения импликации и эквиваленции.

9. Используя лишь законы поглощения и дистрибутивные законы, доказать законы идемпотентности.

10. Следующие формулы привести к более простому виду:

    (a) $(\mathfrak{a} \,\&\, \neg\mathfrak{b}) \vee (\mathfrak{a} \,\&\, \neg\mathfrak{c}) \vee (\mathfrak{b} \,\&\, \mathfrak{c}) \vee \mathfrak{b} \vee \mathfrak{c}$,

    (b) $(\mathfrak{a} \,\&\, \mathfrak{b} \,\&\, \mathfrak{c}) \vee (\mathfrak{a} \,\&\, \mathfrak{b} \,\&\, \neg\mathfrak{c}) \vee (\mathfrak{a} \,\&\, \neg\mathfrak{b})$,

    (c) $\neg((\mathfrak{a} \to \mathfrak{b}) \,\&\, (\mathfrak{b} \to \neg\mathfrak{a}))$,

    (d) $(\mathfrak{a} \to \neg\mathfrak{b}) \vee \neg(\mathfrak{a} \vee \mathfrak{b})$,

    (e) $\neg(\neg\mathfrak{a} \,\&\, \neg\mathfrak{b}) \vee ((\mathfrak{a} \to \mathfrak{b}) \,\&\, \mathfrak{a})$.

11. Докажите, что каждая формула алгебры высказываний равносильна формуле:

    (a) не содержащей операций импликации и эквиваленции и в которой операция отрицания отнесена лишь к буквам;

    (b) содержащей лишь операции $\neg$ и $\&$;

    (c) содержащей лишь операции $\neg$ и $\vee$.

    (d) содержащей лишь операции $\neg$ и $\to$.

12. Докажите тождественную истинность формул, используя законы логики.

    (a) $\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{a})$,

    (b) $(\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c})) \to ((\mathfrak{a} \to \mathfrak{b}) \to (\mathfrak{a} \to \mathfrak{c}))$,

    (c) $(\neg\mathfrak{b} \to \neg\mathfrak{a}) \to ((\neg\mathfrak{b} \to \mathfrak{a}) \to \mathfrak{b})$,

13. Сколько попарно неравносильных формул можно составить в алфавите, содержащем в точности n высказывательных переменных?

§ 2. Совершенные нормальные формы. Применение алгебры высказываний к переключательным схемам

Построение формул по заданным таблицам истинности. Нормальные дизъюнктивные (конъюнктивные) формы. Совершенные нормальные дизъюнктивные (конъюнктивные) формы. Логические операции над двухполюсными переключателями. Задачи синтеза и анализа переключательных схем.

2.1. Построение формул по заданным таблицам истинности. Рассмотрим вначале решение этой задачи на примере. Пусть формула $\mathfrak{a} = \mathfrak{a}(A_1, A_2, A_3)$ от трех высказывательных переменных задана такой таблицей истинности (см. таблицу 7).

Табл. 7: Таблица истинности формулы от трех высказывательных переменных.

A_1	A_2	A_3	$\mathfrak{a}(A_1, A_2, A_3)$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

Понятно, что существует бесконечно много равносильных формул алгебры высказываний, имеющих эту таблицу истинности. Укажем способ нахождения двух таких формул.

Помечаем те строки таблицы, в которых $\mathfrak{a}(A_1, A_2, A_3)$ принимает значение, равное 1. Это строки 1, 3, 7. Для каждой строки (логической возможности) составим формулу, истинную только в этой логической возможности и ложную во всех остальных логических возможностях:

$$\text{1-я строка} — A_1 \,\&\, A_2 \,\&\, A_3$$
$$\text{3-я строка} — A_1 \,\&\, \neg A_2 \,\&\, A_3$$
$$\text{7-я строка} — \neg A_1 \,\&\, \neg A_2 \,\&\, A_3.$$

Если возьмем теперь дизъюнкцию всех этих формул, то это и будет искомой формулой:

$$\mathfrak{a} = (A_1 \,\&\, A_2 \,\&\, A_3) \vee (A_1 \,\&\, \neg A_2 \,\&\, A_3) \vee (\neg A_1 \,\&\, \neg A_2 \,\&\, A_3). \tag{1}$$

Рассмотрим другое решение этой задачи. Помечаем теперь те строки таблицы, в которых $\mathfrak{a}(A_1, A_2, A_3)$ принимает значение, равное 0. Это строки 2, 4, 5, 6, 8. Для каждой логической возможности составим формулу, ложную только в этой логической возможности и истинную во всех остальных логических возможностях:

$$\text{2-я строка} — \neg A_1 \vee \neg A_2 \vee A_3$$
$$\text{4-я строка} — \neg A_1 \vee A_2 \vee A_3$$
$$\text{5-я строка} — A_1 \vee \neg A_2 \vee \neg A_3$$
$$\text{6-я строка} — A_1 \vee \neg A_2 \vee A_3$$
$$\text{8-я строка} — A_1 \vee A_2 \vee A_3.$$

Если теперь возьмем конъюнкцию этих формул, то это также будет искомой, то есть имеющей заданную таблицу истинности, формулой:

$$\mathfrak{a} = (\neg A_1 \vee \neg A_2 \vee A_3) \,\&\, (\neg A_1 \vee A_2 \vee A_3) \,\&\, (A_1 \vee \neg A_2 \vee \neg A_3) \,\&\, (A_1 \vee \neg A_2 \vee A_3) \,\&\, (A_1 \vee A_2 \vee A_3). \tag{2}$$

Формулы (1) и (2) равносильны, так как имеют одну и ту же таблицу истинности. Отметим, что в данном случае удобнее строить формулу (1).

Легко понять, что проведенные рассуждения годятся и для общей ситуации, то есть нахождения формулы по заданной произвольной таблице истинности.

2.2. Нормальные формы. Для каждой формулы алгебры высказываний можно указать равносильную ей формулу, содержащую из логических связок лишь отрицание, конъюнкцию и дизъюнкцию. Для этого достаточно воспользоваться правилами удаления импликации и эквиваленции (см. III.1.7.). Рассмотрение особого вида таких формул и составляет цель последующих трех пунктов.

Определение 1. *Конъюнктивным одночленом от высказывательных переменных $A_1, \ldots, A_n$ называется конъюнкция этих переменных или их отрицаний.*

Например, формулы

$$A_1 \,\&\, \neg A_2 \,\&\, A_3,$$
$$A_2 \,\&\, A_3 \,\&\, \neg A_2 \,\&\, A_5,$$
$$A_1 \,\&\, A_2 \,\&\, \neg A_1 \,\&\, A_3 \,\&\, A_1$$

являются конъюнктивными одночленами.

Определение 2. *Дизъюнктивным одночленом от высказывательных переменных $A_1, \ldots, A_n$ называется дизъюнкция этих переменных или их отрицаний.*

Например, формулы

$$\neg A_1 \vee A_2 \vee A_4,$$
$$A_3 \vee A_3 \vee A_3,$$
$$\neg A_1 \vee A_5 \vee A_4 \vee \neg A_4,$$

являются дизъюнктивными одночленами.

Определение 3. *Дизъюнктивной нормальной формой называется дизъюнкция конъюнктивных одночленов, то есть выражение вида $\mathfrak{a}_1 \vee \mathfrak{a}_2 \vee \ldots \vee \mathfrak{a}_k$, где все $\mathfrak{a}_i$, $i = 1, 2, \ldots, k$ являются конъюнктивными одночленами (не обязательно различными).*

Определение 4. *Конъюнктивной нормальной формой называется конъюнкция дизъюнктивных одночленов $\mathfrak{b}_1 \,\&\, \mathfrak{b}_2 \,\&\, \ldots \,\&\, \mathfrak{b}_l$, где все $\mathfrak{b}_i$, $i = 1, 2, \ldots, l$ являются дизъюнктивными одночленами (не обязательно различными).*

Также будем называть дизъюнктивной (конъюнктивной) нормальной формой указанные выражения при $k = 1$ или $l = 1$.

Нормальную форму, представляющую формулу $\mathfrak{a}$ (то есть равносильную $\mathfrak{a}$) будем называть просто *нормальной формой этой формулы.*

Нетрудно понять что всякая формула обладает как дизъюнктивной, так и конъюнктивной нормальными формами. Более того, у данной формулы $\mathfrak{a}$ существует неограничено много как дизъюнктивных, так и конъюнктивных нормальных форм.

2.3. Совершенные нормальные формы. Среди множества дизъюнктивных (равно как и конъюнктивных) нормальных форм, которыми обладает данная формула алгебры высказываний, существует уникальная форма: она единственна для данной формулы. Это так называемая совершенная дизъюнктивная нормальная форма (среди конъюнктивных форм — совершенная конъюнктивная нормальная форма).

Определение 1. *Одночлен (конъюнктивный или дизъюнктивный) от высказывательных переменных $A_1, \ldots, A_n$ называется совершенным, если в него от каждой пары формул $A_i, \neg A_i$ $(i = 1, 2, \ldots, n)$ входит ровно одна формула.*

Нормальная форма (дизъюнктивная или конъюнктивная) от переменных $A_1, \ldots, A_n$ называется совершенной от этих переменных, если в нее входят лишь неповторяющиеся совершенные одночлены (конъюнктивные или дизъюнктивные соответственно) от $A_1, \ldots, A_n$

Например, формула

$$(A \,\&\, B) \vee (\neg A \,\&\, B) \vee (A \,\&\, \neg B)$$

является совершенной дизъюнктивной формой от высказывательных переменных A и B. Примерами совершенной конъюнктивной и дизъюнктивной форм являются также формулы (2) и (1) соответственно.

2.4. Представление формул алгебры высказываний совершенными нормальными формами.

Теорема 1. *Каждая не тождественно ложная формула алгебры высказываний имеет единственную (с точностью до перестановки дизъюнктивных членов) совершенную дизъюнктивную нормальную форму.*

Теорема 2. *Каждая формула алгебры высказываний, которая не является тавтологией, имеет единственную (с точностью до перестановки конъюнктивных членов) совершенную конъюнктивную нормальную форму.*

2.5. Логические операции над двухполюсными переключателями. Рассмотрим двухполюсные переключатели, то есть такие, которые имеют два состояния: "замкнуто" — 1 и "разомкнуто" — 0. Будем их обозначать большими латинскими буквами и на схемах изображать так:

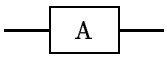

Рис. III.1.

Переключатель, который сблокирован с переключателем A так, что он замкнут, если A разомкнут, и разомкнут, если A замкнут, назовем *инверсным* и будем обозначать $\neg A$ (сравните с операцией отрицания над высказываниями). Операцию последовательного соединения двух переключателей будем обозначать &:

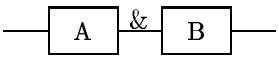

Рис. III.2.

Сравните с операцией конъюнкции высказываний.

Операцию параллельного соединения двух переключателей обозначим через $\vee$:

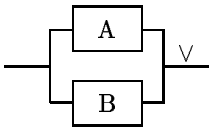

Рис. III.3.

Сравните с операцией дизъюнкции высказываний.

Таким образом, всякую формулу алгебры высказываний от связок $\neg$, &, $\vee$ можно трактовать как некоторую последовательно-параллельную схему от двухполюсных переключателей. Совершенно очевидно, что все свойства операций $\neg$, &, $\vee$ над высказываниями переносятся на соответствующие операции над переключателями (последовательно-параллельными схемами). Таким образом, мы имеем алгебру переключательных схем.

2.6. Задачи синтеза и анализа переключательных схем. Отмеченную выше связь между алгеброй высказываний и алгеброй переключательных схем коротко можно выразить так: эти алгебры одинаково устроены (изоморфны). Этот изоморфизм может быть использован при решении задач следующих двух типов, которые условно назовем *анализ схем* и *синтез схем.*

1. *Анализ схем* заключается в следующем. Для данной схемы составляется соответствующая формула, которая на основании законов логики упрощается и для нее строится новая более простая схема, которая (в силу отмеченного выше изоморфизма алгебр) обладает теми же электрическими свойствами, что и исходная схема. Приведем соответствующий пример. Дана схема

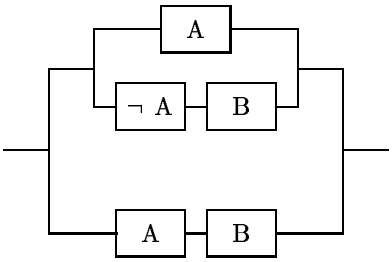

Рис. III.4.

Запишем соответствующую ей формулу и преобразуем ее равносильными преобразованиями.
$(A \vee (\neg A \ \& \ B)) \vee (A \ \& \ B) \equiv A \vee (\neg A \ \& \ B) \vee (A \ \& \ B) \equiv A \vee (A \ \& \ B) \vee (\neg A \ \& \ B) \equiv$
$\equiv A \vee (\neg A \ \& \ B) \equiv (A \vee \neg A) \ \& \ (A \vee B) \equiv 1 \ \& \ (A \vee B) \equiv A \vee B.$
Таким образом, исходная схема равносильна такой:

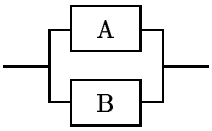

Рис. III.5.

2. *Синтез схем* заключается в построении схем с заданными электрическими свойствами. Это делается так. На основании заданных электрических свойств строится формула алгебры высказываний, а по ней соответствующая схема. Приведем

Пример 1. Актив студенческой группы, состоящий из трех человек, хочет применить электрическую схему для регистрации тайного голосования простым большинством голосов. Построим такую схему, чтобы каждый голосующий "за" нажимал свою кнопку, а каждый голосующий "против" не нажимал соответствующей кнопки. В случае принятия решения должна загореться сигнальная лампочка.

Решение. Пусть A, B, C — обозначают соответственно высказывания "1 – ый за", "2 – ой за", "3 – ий за". Составим таблицу истинности формулы $\mathfrak{a}(A, B, C)$, которой будет соответствовать искомая схема.

A	B	C	$\mathfrak{a}(A, B, C)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Теперь способом, указанным в п. III.2.1., составляем формулу $\mathfrak{a} = \mathfrak{a}(A, B, C)$.

$$\mathfrak{a} = (A \ \& \ B \ \& \ C) \vee (A \ \& \ B \ \& \ \neg C) \vee (A \ \& \ \neg B \ \& \ C) \vee (\neg A \ \& \ B \ \& \ C).$$

И, наконец, составим схему, которая соответствует построенной формуле (см. рис. III.6.).

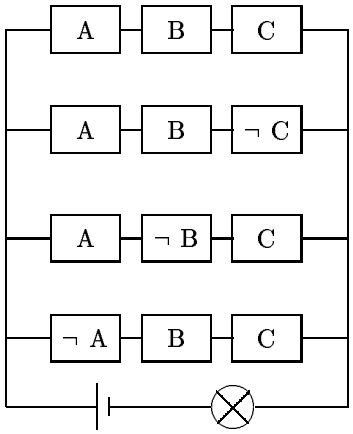

Рис. III.6. ■

Полученную в этом примере схему можно упростить, осуществляя ее анализ. Равносильными преобразованиями упрощаем формулу:

$$\mathfrak{a} = (A \,\&\, B \,\&\, C) \vee (A \,\&\, B \,\&\, \neg C) \vee (A \,\&\, \neg B \,\&\, C) \vee (\neg A \,\&\, B \,\&\, C) \equiv$$
$$\equiv (A \,\&\, B \,\&\, (C \vee \neg C)) \vee ((A \vee \neg A) \,\&\, (A \vee B) \,\&\, (A \vee C) \,\&$$
$$\&\, (\neg B \vee \neg A) \,\&\, (\neg B \vee B) \,\&\, (\neg B \vee C) \,\&\, (C \vee \neg A) \,\&\, (C \vee B) \,\&\, (C \vee C)) \equiv$$
$$\equiv (A \,\&\, B) \vee (C \,\&\, (A \vee C) \,\&\, (C \vee B) \,\&\, (C \vee \neg A) \,\&\, (C \vee \neg B) \,\&\, (A \vee B) \,\&\, (\neg B \vee \neg A)) \equiv$$
$$\equiv (A \,\&\, B) \vee (C \,\&\, (A \vee B) \,\&\, (\neg A \vee \neg B)) \equiv (A \,\&\, B) \vee (C \,\&\, (A \vee B) \,\&\, \neg(A \,\&\, B)) \equiv$$
$$\equiv ((A \,\&\, B) \vee C) \,\&\, ((A \,\&\, B) \vee A \vee B) \,\&\, ((A \,\&\, B) \vee \neg(A \,\&\, B)) \equiv ((A \,\&\, B) \vee C) \,\&\, (A \vee B)$$

Упрощенная схема приведена на рис. III.7.

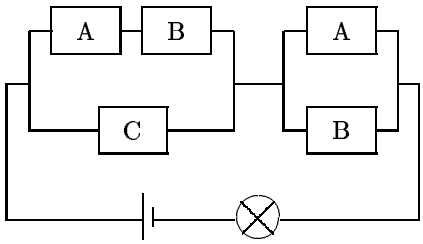

Рис. III.7.

2.7. Новые термины. Конъюнктивный (дизъюнктивный) одночлен. Нормальная конъюнктивная (дизъюнктивная) форма. Совершенный конъюнктивный (дизъюнктивный) одночлен. Совершенная нормальная конъюнктивная (дизъюнктивная) форма. Двухполюсной переключатель. Инверсный к данному переключатель. Операции последовательного и параллельного соединения переключателей. Алгебра переключательных схем. Анализ и синтез схем.

2.8. Контрольные вопросы.

1. Известно, что формула $\mathfrak{a} = \mathfrak{a}(A, B, C)$ истина в одном единственном случае: $\mathfrak{a}(1, 1, 0) = 1$. Запишите эту формулу.
2. Известно, что формула $\mathfrak{a} = \mathfrak{a}(A, B, C)$ истина в точности в двух случаях: $\mathfrak{a}(0, 1, 0) = \mathfrak{a}(0, 0, 0) = 1$. Запишите эту формулу.
3. Каким схемам соответствуют равносильные формулы?

4. Какой схеме соответствует тождественно истинная формула? Тождественно ложная?

5. Перескажите смысл анализа схем.

6. Перескажите смысл синтеза схем.

2.9. Упражнения.

1. Постройте формулу от трех букв, истинную тогда и только тогда, когда в точности две буквы принимают значение, равное 1. Когда в точности одна буква принимает значение, равное 0.

2. Придумайте формулу от трех букв, ложную в одном единственном случае, когда $A = 1$, $B = 0$, $C = 1$. Когда $A = 0$, $B = 1$, $C = 1$.

3. Придумайте формулу от трех букв, ложную тогда и только тогда, когда $\mathfrak{a}(1, 0, 1) = 0$ и $\mathfrak{a}(0, 0, 1) = 0$. Когда $\mathfrak{a}(0, 1, 1) = \mathfrak{a}(1, 1, 1) = \mathfrak{a}(0, 0, 0) = 0$.

4. Постройте схему, соответствующую формуле

$$((A \vee B) \,\&\, \neg C) \vee ((\neg A \,\&\, C) \vee B).$$

5. Упростите схему

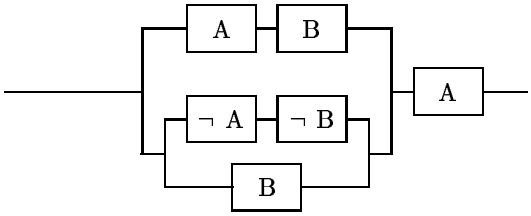

Рис. III.8.

6. Имеется одна лампочка в лестничном пролете двухэтажного здания. Постройте схему так, чтобы на каждом этаже своим выключателем можно было бы гасить и зажигать лампу независимо от положения другого переключателя.

7. Необходимо, чтобы в большом зале можно было включать и выключать свет при помощи любого из трех переключателей, расположенных на трех стенах. Составьте такую схему.

8. Группа студентов сдает зачет, состоящий из 4-х вопросов, требующих установить истинность или ложность каких-то утверждений. Построить схему, позволяющую отвечать на каждый вопрос нажатием или ненажатием соответствующей кнопки. Схема должна при этом показывать количество правильных ответов.

9. Составьте схему с четырьмя переключателями, которая проводит ток тогда и только тогда, когда замыкаются не все переключатели, а только некоторые из них.

10. Начертите схему с 5 переключателями, которая замыкается, если и только если замкнуты ровно 4 из этих переключателей.

§ 3. Полные системы связок

Определение полной системы связок. Свойства полных систем связок. Описание п. с. с. из Θ. Одноэлементные п. с. с. Исключительность связок $\overline{\&}$ и ∇.

3.1. Определение полной системы связок. Ранее были однозначно определены пять основных логических связок, используемых в языке алгебры высказываний для записи формул. Обозначим:

$$\Theta = \{\neg, \&, \vee, \to, \sim\}.$$

Отметим, что что можно ввести и другие связки (определить таблицами истинности), отличные от связок из Θ.

Всего различных унарных связок можно определить 4, а бинарных — 16 (см. упр. 1). В Θ же всего одна унарная связка и 4 бинарных. Связки из Θ будем называть *основными связками*. Множество всех унарных и бинарных связок (а всего их 20) обозначим через Ω. Понятно, что $\Theta \subset \Omega$. Если Ω_1 — некоторое множество связок, то есть $\Omega_1 \subseteq \Omega$, то обозначим через $\Phi\{\Omega_1\}$ множество всевозможных формул АВ, в записи которых могут участвовать лишь связки из Ω_1. Иначе говоря, $\Phi\{\Omega_1\}$ состоит из формул, не содержащих в своей записи связок из $\Omega \setminus \Omega_1$. Так, например, простейшие формулы, то есть буквы латинского алфавита, снабженные, быть может, штрихами или индексами, входят в $\Phi\{\Omega_1\}$ для любого подмножества Ω_1 множества Ω. Из определения $\Phi\{\Omega_1\}$ непосредственно следуют очевидные свойства 1–2.

1. $\Phi\{\Theta\}$ — множество всевозможных формул алгебры высказываний (АВ).
2. Если $\Omega_1 \subseteq \Omega_2 \subseteq \Omega$, то $\Phi\{\Omega_1\} \subseteq \Phi\{\Omega_2\}$.

Определение 1. *Множество Ω_1 связок из Ω называется полной системой связок (п. с. с.), если всякая формула из $\Phi\{\Theta\}$ равносильна некоторой формуле из $\Phi\{\Omega_1\}$.*

Пример 1. Если в качестве Ω_1 возьмем Θ, то понятно, что всякая формула из $\Phi(\Theta)$ равносильна некоторой формуле из $\Phi\{\Theta\}$. Таким образом, Θ — полная система связок.

Пример 2. Пользуясь правилом исключения эквиваленции

$$\mathfrak{a} \sim \mathfrak{b} \equiv (\mathfrak{a} \to \mathfrak{b}) \,\&\, (\mathfrak{b} \to \mathfrak{a}),$$

равносильными преобразованиями всякую формулу можно привести к виду, в котором нет операции $\sim$. Следовательно, всякая формула из $\Phi\{\Theta\}$ равносильна некоторой формуле из $\Phi\{\neg, \&, \vee, \to\}$. Это означает, что множество $\{\neg, \&, \vee, \to\}$ — п. с. с.

3.2. Свойства полных систем связок.

Теорема 1. *Полные системы связок обладают следующими свойствами:*

1) если какое-то множество связок Ω_1 содержит некоторую п. с. с., то Ω_1 — тоже п. с. с.;

2) если Ω_1 — п. с. с. и всякая формула из $\Phi(\Omega_1)$ равносильна какой-то формуле из $\Phi(\Omega_2)$ для некоторой системы связок Ω_2, то Ω_2 тоже п. с. с.

Доказательство. 1) Непосредственно следует из определения п. с. с.

2) Пусть $\mathfrak{a} \in \Phi(\Theta)$. Так как Ω_1 — п. с. с., то $\mathfrak{a} \equiv \mathfrak{b}$ для некоторой формулы $\mathfrak{b}$ из $\Phi(\Omega_1)$. По условию $\mathfrak{b} \equiv \mathfrak{c}$ для некоторой $\mathfrak{c}$ из $\Phi(\Omega_2)$. По транзитивности отношения равносильности имеем:

$$\mathfrak{a} \equiv \mathfrak{c} \text{ и } \mathfrak{c} \in \Phi(\Omega_2)$$

Это означает, что Ω_2 — п. с. с. ■

Пример 1. Пользуясь правилом исключения импликации

$$\mathfrak{a} \to \mathfrak{b} \equiv \neg\mathfrak{a} \vee \mathfrak{b},$$

равносильными преобразованиями всякую формулу АВ из $\Phi\{\neg, \&, \vee, \to\}$ можно привести к виду, в котором нет операции $\to$. Это означает, что всякая формула из $\Phi\{\neg, \&, \vee, \to\}$ равносильна некоторой формуле из $\Phi\{\neg, \&, \vee\}$ и $\{\neg, \& \vee, \to\}$ — п. с. с., см. пример 3.1.2. Применяя п. 2 теоремы 3.2.1, получаем, что $\{\neg, \&, \vee\}$ — п. с. с.

Теорема 2. *Всякая полная система связок из* Θ *содержит связку* $\neg$.

Доказательство. Пусть $\mathfrak{M}$ — множество всех формул АВ, не содержащих в своей записи связки $\neg$, то есть $\mathfrak{M} = \Phi\{\&, \vee, \to, \sim\}$. Легко убедиться в том, что если $\mathfrak{a}(A_1, \ldots, A_n) \in \mathfrak{M}$, то $\mathfrak{a}(1, \ldots, 1) = 1$. Рассмотрим формулу $\mathfrak{b}(A, B) = \neg A \ \& \ B$. Очевидно, $\mathfrak{b}(1, 1) = 0$, значит $\mathfrak{b}(A, B) \in \Phi\{\Theta\}$, но $\mathfrak{b}(A, B)$ неравносильна никакой формуле из $\Phi\{\&, \vee, \to, \sim\}$. Это означает, что множество $\{\&, \vee, \to, \sim\}$ не является п. с. с. По теореме 3.2.1, п. 1, никакое подмножество множества $\{\&, \vee, \to, \sim\}$ не является п. с. с. Это и означает, что всякая п. с. с. из Θ обязана содержать операцию $\neg$. ■

3.3. Описание полных систем связок из Θ. По теореме 3.2.2, всякая п. с. с. из Θ содержит $\neg$. Возникает вопрос о том, а не является ли одноэлементное множество $\{\neg\}$ п. с. с.? Ответ дает

Теорема 1. *Множество* $\{\neg\}$ *не является п. с. с.*

Доказательство. Отметим, что $\Phi\{\neg\}$ состоит из всех букв алфавита и формул вида $\underbrace{\neg\neg\ldots\neg}_{n} A$, $n \in N$. Однако, ни одна из этих формул не является тавтологией. Следовательно, формула $A \vee \neg A$, например, неравносильна никакой формуле из $\Phi\{\neg\}$. Следовательно, множество $\{\neg\}$ не является п. с. с. ■

Теорема 2. *Следующие ниже множества связок из* Θ *является п. с. с.:*
1) $\{\neg, \&\}$*;*
2) $\{\neg, \vee\}$*;*
3) $\{\neg, \to\}$.

Доказательство. 1) $\{\neg, \&\}$. В примере 3.2.1 показано, что множество $\{\neg, \&, \vee\}$ — п. с. с. Пользуясь равносильностью

$$\mathfrak{a} \vee \mathfrak{b} \equiv \neg(\neg\mathfrak{a} \ \& \ \neg\mathfrak{b})$$

всякую формулу из $\Phi\{\neg, \&, \vee\}$ равносильными преобразованиями можно привести к формуле, в записи которой нет операции $\vee$. Это означает, что всякая формула из $\Phi\{\neg, \&, \vee\}$ равносильна некоторой формуле из $\Phi\{\neg, \&\}$. А так как $\{\neg, \&, \vee\}$ — п. с. с., то по теореме 3.2.1, п. 2, $\{\neg, \&\}$ — тоже п. с. с.

2) $\{\neg, \vee\}$. Рассуждения такие же, как и в предыдущем пункте с использованием равносильности $\mathfrak{a} \ \& \ \mathfrak{b} \equiv \neg(\neg\mathfrak{a} \vee \neg\mathfrak{b})$.

3) $\{\neg, \to\}$. Пользуясь равносильностью $\mathfrak{a} \vee \mathfrak{b} \equiv \neg\mathfrak{a} \to \mathfrak{b}$, всякую формулу из $\Phi\{\neg, \vee\}$ равносильными преобразованиями можно привести к формуле из $\Phi\{\neg, \to\}$, то есть всякая формула из $\Phi\{\neg, \vee\}$ равносильна некоторой формуле из $\Phi\{\neg, \to\}$ и $\{\neg, \vee\}$ — п. с. с. Следовательно, по теореме 3.2.1, п.2, $\{\neg, \to\}$ — тоже п. с. с. ■

Следствие 1. *Всякая система связок из* Ω*, содержащая связку* $\neg$ *и хотя бы одну из связок* $\&$, $\vee$, $\to$, *является п. с. с.*

Доказательство следует непосредственно из предыдущей теоремы и теоремы 3.2.1, п. 1.

3.4. Одноэлементные полные системы связок. В п. III.3.3. доказано, что среди связок из Θ нет такой связки, которая составляла бы п. с. с. Есть ли такие связки не в Θ? Ответ положительный. Введем две связки, которые обозначим $\overline{\&}$ и $\overline{\vee}$, а смысл их определим таблицами истинности:

A	B	$A \,\overline{\&}\, B$	$A \,\overline{\vee}\, B$
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

Связку $\overline{\&}$ принято называть "Штрих Шефера" и обозначать символом $|$. Связку $\overline{\vee}$ иногда называют "операция Пирса" и обозначают $\downarrow$. Однако мы предпочтем мнемонический подход к обозначению этих связок.

Теорема 1. *Множества* $\{\overline{\&}\}$ *и* $\{\overline{\vee}\}$ *являются полными системами связок.*

Доказательство. 1. Из таблицы истинности для связки $\overline{\&}$ легко усматривается равносильность:

$$\neg(\mathfrak{a} \,\&\, \mathfrak{b}) \equiv \mathfrak{a} \,\overline{\&}\, \mathfrak{b}.$$

Воспользовавшись ею, получим:

$$\begin{aligned}
&\neg\mathfrak{a} \equiv \neg(\mathfrak{a} \,\&\, \mathfrak{a}) \equiv \mathfrak{a} \,\overline{\&}\, \mathfrak{a},\\
&\mathfrak{a} \vee \mathfrak{b} \equiv \neg(\neg\mathfrak{a} \,\&\, \neg\mathfrak{b}) \equiv \neg(\neg(\mathfrak{a} \,\&\, \mathfrak{a}) \,\&\, \neg(\mathfrak{b} \,\&\, \mathfrak{b})) \equiv\\
&\qquad \equiv \neg((\mathfrak{a} \,\overline{\&}\, \mathfrak{a}) \,\&\, (\mathfrak{b} \,\overline{\&}\, \mathfrak{b})) \equiv (\mathfrak{a} \,\overline{\&}\, \mathfrak{a}) \,\overline{\&}\, (\mathfrak{b} \,\overline{\&}\, \mathfrak{b}).
\end{aligned}$$

Таким образом, получены равносильности:

$$\begin{aligned}
&\neg\mathfrak{a} \equiv \mathfrak{a} \,\overline{\&}\, \mathfrak{a},\\
&\mathfrak{a} \vee \mathfrak{b} \equiv (\mathfrak{a} \,\overline{\&}\, \mathfrak{a}) \,\overline{\&}\, (\mathfrak{b} \,\overline{\&}\, \mathfrak{b}).
\end{aligned}$$

Используя их, равносильными преобразованиями каждую формулу из $\Phi\{\neg, \vee\}$ можно привести к некоторой формуле из $\Phi\{\overline{\&}\}$, то есть всякая формула из $\Phi\{\neg, \vee\}$ равносильна некоторой формуле из $\Phi\{\overline{\&}\}$. Кроме того, $\{\neg, \vee\}$ — п. с. с. По теореме 3.2.1, п. 2, $\{\overline{\&}\}$ — тоже п. с. с.

2. Полнота системы связок $\{\overline{\vee}\}$ доказывается аналогично предыдущему. Поэтому мы приведем лишь необходимые для рассуждения равносильности, которые также необходимо проверить.

$$\begin{aligned}
&\neg\mathfrak{a} \equiv (\mathfrak{a} \,\overline{\vee}\, \mathfrak{a}),\\
&\mathfrak{a} \,\&\, \mathfrak{b} \equiv (\mathfrak{a} \,\overline{\vee}\, \mathfrak{a}) \,\overline{\vee}\, (\mathfrak{b} \,\overline{\vee}\, \mathfrak{b}). \blacksquare
\end{aligned}$$

3.5. Исключительность связок $\overline{\&}$ и $\overline{\vee}$.

Теорема 1. *Если* $* \in \Omega$ *и* $\{*\}$ *— п. с. с., то* $* = \overline{\&}$ *или* $* = \overline{\vee}$.

Доказательство. 1. Предположим, что связка $*$ одноместная. Тогда всякая формула из $\Phi\{*\}$ имеет вид: $\mathfrak{a} = **\ldots*A$, где A — некоторая высказывательная переменная. Тогда при $A = 1$, $\mathfrak{a} = 1$ либо $\mathfrak{a} = 0$.

Пусть при $A = 1$, $\mathfrak{a} = 1$. Формула $A \,\&\, B$ при $A = 1$, $B = 0$ принимает значение $A \,\&\, B = 0$, а при $A = 1$, $B = 1$, $A \,\&\, B = 1$, то есть формула $A \,\&\, B$ при $A = 1$ может принимать как значение равное 0, так и равное 1. Тоже самое верно и для всякой формулы вида $\mathfrak{b} = **\ldots*B$. Таким образом, формула $A \,\&\, B$ неравносильна никакой формуле из $\Phi\{*\}$. Следовательно, одноместные связки не могут удовлетворять условию теоремы.

2. Пусть $*$ — двуместная связка, A и B — высказывательные переменные.

a) Предположим, что $A*B = 1$, при $A = 1$ и $B = 1$. Тогда любая формула $\mathfrak{a} = \mathfrak{a}(A_1, A_2, \ldots A_n)$, содержащая лишь связку $*$, при $A_1 = A_2 = \cdots = A_n = 1$ принимает значение, равное 1, и потому неравносильна, например, формуле $\mathfrak{b}(A_1, A_2) = \neg A_1 \,\&\, A_2$, так как $\mathfrak{b}(1, 1) = 0$. Таким образом, $A * B = 0$ при $A = B = 1$.

b) Теперь предположим, что $A * B = 0$, при $A = B = 0$. В этом случае всякая формула $\mathfrak{a} = \mathfrak{a}(A_1, A_2, \ldots, A_n) \in \Phi\{*\}$, при $A_1 = A_2 = \cdots = A_n = 0$ принимает значение, равное 0, а потому не может быть равносильна, например, формуле $\mathfrak{b}(A_1, A_2) = \neg A_1 \vee A_2$, так как $\mathfrak{b}(0, 0) = 1$. Таким образом, $A * B = 1$, при $A = B = 0$

c) Таким образом, для $A * B$ имеем следующую, не до конца определенную, таблицу истинности.

A	B	$A * B$
1	1	0
1	0	
0	1	
0	0	1

d) Предположим, что для формулы $\mathfrak{a}(A,B) = A * B$ имеет место:

$$\mathfrak{a}(1,0) = 1,\ \mathfrak{a}(0,1) = 0.$$

Тогда имеем:

A	B	$A * B$	$\neg B$
1	1	0	0
1	0	1	1
0	1	0	0
0	0	1	1

Эта таблица истинности показывает, что: $\mathfrak{a}(A,B) = A * B \equiv \neg B$. Это означает, что всякая формула из $\Phi\{*\}$ равносильна некоторой формуле из $\Phi\{\neg\}$. А так как $\{*\}$ — п. с. с., то и $\{\neg\}$ — п. с. с. Противоречие. Следовательно, невозможно, чтобы $\mathfrak{a}(1,0) = 1$, а $\mathfrak{a}(0,1) = 0$.

e) Пусть $\mathfrak{a}(1,0) = 0$, а $\mathfrak{a}(0,1) = 1$.

Тогда имеем:

A	B	$A * B$	$\neg A$
1	1	0	0
1	0	0	0
0	1	1	1
0	0	1	1

Это означает, что

$$\mathfrak{a}(A,B) = A * B \equiv \neg A$$

Как и в случае d) получаем, что $\{\neg\}$ — п. с. с., что противоречит теореме 3.3.2. Таким образом, также невозможно, чтобы

$$\mathfrak{a}(1,0) = 0, \text{ а } \mathfrak{a}(0,1) = 1.$$

f) Таким образом, для $\mathfrak{a}(A,B) = A * B$ осталось лишь две возможные, определяющие связку $*$, таблицы истинности.

A	B	$A *_1 B$
1	1	0
1	0	0
0	1	0
0	0	1

A	B	$A *_2 B$
1	1	0
1	0	1
0	1	1
0	0	1

Но это означает, что $*_1 = \overline{\&}$, а $*_2 = \overline{\vee}$. ■

3.6. Новые термины. Основные связки. Полные системы связок (п. с. с.). Отрицание конъюнкции $\overline{\&}$ (штрих Шеффера). Отрицание дизъюнкции $\overline{\vee}$ (операция Пирса).

3.7. Контрольные вопросы.

1. Сколько элементов во множествах Θ и Ω?
2. Какое множество обозначено через $\Phi\{\Omega_1\}$ для $\Omega_1 \subseteq \Omega$?
3. Охарактеризуйте множество $\Phi\{\varnothing\}$.
4. Охарактеризуйте множество $\Phi\{\Theta\}$.
5. Верно ли, что $\Phi\{\varnothing\} \subseteq \Phi\{\Theta\}$?
6. Какие из приведенных ниже множеств является п. с. с.:

   a) $\{\neg, \to\}$; b) $\{\neg, \to, \sim\}$;
   c) $\{\neg, \sim\}$; d) $\{\neg\}$;
   e) $\{\&, \vee\}$; f) $\{\&, \vee, \to, \sim\}$;
   g) Θ.
7. Сформулируйте основные результаты о п. с. с. из Θ.
8. Дайте словесное определение связок $\overline{\&}$ и $\overline{\vee}$.
9. Какие из приведенных ниже множеств являются п. с. с.:

   a) $\{\overline{\&}\}$; b) $\{\overline{\&}, \neg\}$;
   c) $\{\overline{\&}\} \cup \Theta$; d) $\{\overline{\vee}, \to\}$;
   e) $\{\overline{\vee}\}$.
10. Перечислите все одноэлементные п. с. с.

3.8. Упражнения.

1. Докажите, что количество всех унарных связок равно 4, а бинарных — 16.
2. Воспроизведите более детально, чем в тексте, доказательство теоремы 3.2.1, п. 2.
3. Приведите доказательство п. 2 теоремы 3.3.2.
4. Приведите доказательство п. 2 теоремы 3.4.1.
5. Равносильными преобразованиями приведите следующие ниже формулы к виду, содержащему лишь связку $\overline{\&}$ (лишь связку $\overline{\vee}$):

   (a) $\neg\mathfrak{a}$; (b) $\mathfrak{a} \,\&\, \mathfrak{b}$; (c) $\mathfrak{a} \vee \mathfrak{b}$;
   (d) $\mathfrak{a} \to \mathfrak{b}$; (e) $\mathfrak{a} \sim \mathfrak{b}$.

Глава IV

Булевы функции

§ 1. Булевы функции. Реализация булевых функций формулами

Булевы функции. Примеры булевых функций. Реализация булевых функций формулами. Равносильные формулы. Двойственные функции. Принцип двойственности.

1.1. Определение и примеры булевых функций.

Определение 1. *Функции $f\colon\{0,1\}^n \to \{0,1\}$ называются функциями алгебры логики или булевыми функциями.*

Множество булевых функций от n переменных обозначим P_n:

$$P_n = \{f \mid f\colon\{0,1\}^n \to \{0,1\}\}.$$

Нетрудно перечислить все булевы функции от одной переменной:

Аргумент	Булевы функции			
x	0	x	$\neg x$, $\overline{x}$, x'	1
	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
1	0	1	0	1
0	0	0	1	1

Всего имеется четыре различных булевых функций от одной переменной:
$f_0(x) = 0$ — функция тождественно равная нулю или *тождественный нуль*,
$f_1(x) = x$ — тождественная функция,
$f_2(x) = x'$ — функция, которую называют *отрицанием*,
$f_3(x) = 1$ — функция, тождественно равная единице или *тождественная единица*.
Перечислим все возможные булевы функции от двух переменных, указав наиболее употребительные обозначения для некоторых из них:

Аргументы		Булевы функции															
		0	$\cdot$, &			$\downarrow$	x	$+$, $\oplus$	x'	$\sim$	y	y'	$\vee$	$\mid$	$\to$		1
x	y	g_0	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8	g_9	g_{10}	g_{11}	g_{12}	g_{13}	g_{14}	g_{15}
1	1	0	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1
1	0	0	0	1	0	0	1	1	0	0	0	1	1	1	0	1	1
0	1	0	0	0	1	0	0	1	1	0	1	0	1	1	1	0	1
0	0	0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1

Всего имеется шестнадцать различных булевых функций от двух переменных. Многие из них имеют специальные названия:
$g_1(x,y) = x \cdot y$ — *конъюнкция*,
$g_4(x,y) = x \downarrow y$ — *стрелка Пирса*,
$g_6(x,y) = x + y$ — *сложение по модулю 2* или *сумма Жегалкина*,

$g_8(x,y) = x \sim y$ — *эквиваленция*,
$g_{11}(x,y) = x \vee y$ — *дизъюнкция*,
$g_{12}(x,y) = x \,|\, y$ — *штрих Шеффера*,
$g_{13}(x,y) = x \to y$ — *импликация*.

Таблица значений булевой функции называется *таблицей истинности*. Любую булеву функцию от n переменных $f(x_1, x_2, \ldots, x_n)$ можно задать таблицей истинности:

x_1	x_2	$\ldots$	x_n	$f(x_1, x_2, \ldots, x_n)$
0	0	$\ldots$	0	λ_1
1	0	$\ldots$	0	λ_2
0	1	$\ldots$	0	λ_3
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	1	$\ldots$	1	λ_{2^n}

где $\lambda_i \in \{0,1\}$, $i = 1, 2, \ldots, 2^n$. В этой таблице имеется 2^n строк, соответствующих различным комбинациям значений переменных, которым можно сопоставить 2^{2^n} различных столбцов. Но каждый такой столбец соответствует какой-то булевой функции от n переменных. Таким образом, доказана

Теорема 1. *Число различных булевых функций от n переменных равно 2^{2^n} или $|P_n| = 2^{2^n}$.*

1.2. Существенные и несущественные переменные.

Определение 1. *Говорят, что булева функция $f \in P_n$ существенно зависит от переменной x_i, если существует такой набор значений переменных $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$, что*

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

В этом случае x_i называется *существенной переменной*, в противном случае x_i — *несущественная (фиктивная) переменная*.

Пример 1. Пусть булевы функции f_1, f_2 и f_3 заданы таблицами истинности:

x	y	f_1	f_2	f_3
1	1	0	1	1
1	0	0	1	0
0	1	1	1	0
0	0	1	1	0

Видно, что для f_1 переменная x является существенной, а y — несущественной; для f_2 обе переменные несущественные; для f_3 обе переменные существенные.

По определению будем считать булевы функции равными, если одна из другой получается удалением или введением несущественных переменных. Поэтому далее булевы функции рассматриваются с точностью до несущественных переменных. Это позволяет считать, что все булевы функции данного множества булевых функций от ограниченного в совокупности числа переменных зависят от одних и тех же переменных. Такое множество булевых функций можно также обозначать P_n, $n = \max m_i$, где m_i — количество существенных переменных i-ой функции из P_n.

1.3. Реализация булевых функций формулами. Пусть $\Phi = \{f_1, f_2, \ldots, f_m\}$ — множество булевых функций.

Определение 1. *Формулой над Φ называется выражение вида*

$$F[\Phi] = f(t_1, t_2, \ldots, t_n),$$

где $f \in \Phi$ и t_i либо переменная, либо формула над Φ.

Множество Φ называется *базисом*, f — *главной (внешней) операцией (функцией)*, а t_i — *подформулами*. Всякой формуле F однозначно соответствует некоторая булева функция f. В этом случае говорят, что формула F *реализует функцию* f и обозначают:

$$f = \operatorname{func} F.$$

Зная таблицы истинности для функций базиса, можно вычислить таблицу истинности той функции, которую реализует данная формула.

Пример 1. Пусть $\Phi = \{\cdot, \to\}$ и $F = (x \cdot y) \to x$. Тогда

x	y	$x \cdot y$	$(x \cdot y) \to x = F$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

Пример 2. Пусть $\Phi = \{\vee, \cdot, '\}$ и $F = (x \cdot y) \vee (x \cdot y')$. Тогда

x	y	$x \cdot y$	$x \cdot y'$	$(x \cdot y) \vee (x \cdot y') = F$
1	1	1	0	1
1	0	0	1	1
0	1	0	0	0
0	0	0	0	0

1.4. Равносильные формулы. Легко понять, что одна булева функция над данным базисом Φ может иметь много реализаций.

Определение 1. *Формулы, реализующие одну и ту же булеву функцию называются равносильными, то есть*

$$F_1 \equiv F_2 \Longleftrightarrow \operatorname{func} F_1 = \operatorname{func} F_2.$$

Теорема 1. *Для любых булевых функций f, g и h истинны следующие равносильности.*

1. $f'' \equiv f$.
2. *Идемпотентность конъюнкции, дизъюнкции и сложения по модулю два:*
   $f \cdot f \equiv f$, $f \vee f \equiv f$, $f + f \equiv f$.
3. *Коммутативность конъюнкции, дизъюнкции и сложения по модулю два:*
   $f \cdot g \equiv g \cdot f$, $f \vee g \equiv g \vee f$, $f + g \equiv g + f$,
4. *Ассоциативность конъюнкции, дизъюнкции и сложения по модулю два:*
   $f \cdot (g \cdot h) \equiv (f \cdot g) \cdot h$, $f \vee (g \vee h) \equiv (f \vee g) \vee h$, $f + (g + h) \equiv (f + g) + h$.
5. *Дистрибутивные законы:*
   $f \cdot (g \vee h) \equiv (f \cdot g) \vee (f \cdot h)$, $f \vee (g \cdot h) \equiv (f \vee g) \cdot (f \vee h)$, $f \cdot (g + h) \equiv (f \cdot g) + (f \cdot h)$.
6. *Законы поглощения:*
   $f \cdot (f \vee g) \equiv f$, $f \vee (f \cdot g) \equiv f$.
7. *Законы де Моргана:*
   $(f \cdot g)' \equiv f' \vee g'$, $(f \vee g)' \equiv f' \cdot g'$.
8. $f \vee f' \equiv 1$, $f \cdot f' \equiv 0$.

9. $f \cdot 1 \equiv f$, $f \vee 0 \equiv f$, $f \vee 1 \equiv 1$, $f \cdot 0 \equiv 0$, $1' \equiv 0$, $0' \equiv 1$.

10. *Закон контрапозиции:*
$f \to g \equiv g' \to f'$.

11. *Правило исключения импликации:*
$f \to g \equiv f' \vee g$,

12. *Правило исключения эквиваленции:*
$f \sim g \equiv (f \to g) \cdot (g \to f)$.

13. $f' \equiv f \,|\, f \equiv f \downarrow f \equiv f + 1$.

14. $f \,|\, g \equiv (f \cdot g)'$, $f \downarrow g \equiv (f \vee g)'$.

15. $f \vee g \equiv (f \,|\, f) \,|\, (g \,|\, g)$, $f \cdot g \equiv (f \downarrow f) \downarrow (g \downarrow g)$, $f \to g \equiv f \,|\, (g \,|\, g)$.

16. $f + g \equiv (f \sim g)'$.

Доказательство этих равносильностей проводится построением таблиц истинности.

1.5. Подстановка и замена. Если в формулу F входит переменная x, то этот факт будем обозначать $F(\ldots, x, \ldots)$. Запись $F(\ldots, G, \ldots)$ обозначает, что формула F содержит в своей записи подформулу G. Вместо подформулы (в частности, вместо переменной) в формулу можно подставить другую формулу (в частности, переменную), в результате получится новая правильно построенная формула. Если постановка производится вместо *некоторых* вхождений (в том числе вместо одного), то результат подстановки обозначим $F(\ldots, G_1, \ldots)\{G_2/G_1\}$. Если же подстановка производится вместо *всех* вхождений заменяемой подформулы (или переменной), то результат подстановки обозначим $F(\ldots, G_1, \ldots)\{G_2//G_1\}$.

Пример 1.
1. $x \vee x'\{y \cdot z//x\} = (y \cdot z) \vee (y \cdot z)'$.
2. $x \to (y \vee z)\{x'//y \vee z\} = x \to x'$.
3. Замена первого вхождения переменной: $x \cdot x'\{y/x\} = y \cdot x'$.
4. Замена второго вхождения подформулы: $x \vee (y \cdot z)' \vee (y \cdot z)\{x/y \cdot z\} = x \vee (y \cdot z)' \vee x$.

Правило замены. *Если в формуле заменить некоторую подформулу на равносильную ей, то получится равносильная формула*

$$G_1 \equiv G_2 \Longrightarrow F(\ldots, G_1, \ldots) \equiv F(\ldots, G_1, \ldots)\{G_2/G_1\}.$$

Правило подстановки. *Если в равносильных формулах вместо <u>всех</u> вхождений некоторой переменной x поставить одну и ту же формулу, то получатся равносильные формулы*

$$F_1(\ldots, x, \ldots) \equiv F_2(\ldots, x, \ldots) \Longrightarrow F_1(\ldots, x, \ldots)\{G//x\} \equiv F_2(\ldots, x, \ldots)\{G//x\}.$$

Пример 2. Так как $x \to y \equiv x' \vee y$, то, по правилу замены

$$(z \cdot (x \to y)) \vee (x \to y) \equiv (z \cdot (x \to y)) \vee (x' \vee y) = (z \cdot (x \to y)) \vee (x \to y)\{x' \vee y/x \to y\}.$$

Так как $x' \cdot (y \to x) \equiv (x + 1) \cdot (y \to x)$, то, по правилу замены, имеем

$$x' \cdot (y \to x)\{x \vee z//x\} \equiv (x + 1) \cdot (y \to x)\{x \vee z//x\}$$

или

$$(x \vee z)' \cdot (y \to (x \vee z)) \equiv ((x \vee z) + 1) \cdot (y \to (x \vee z)).$$

Отметим, что в правиле подстановки условие замены всех вхождений существенно. Например, $x \vee x' \equiv 1$ и $x \vee x'\{y//x\} = y \vee y' \equiv 1$, но $x \vee x'\{y/x\} = y \vee x' \not\equiv 1$.

1.6. Принцип двойственности.

Определение 1. *Пусть* $f(x_1,\dots,x_n)\in P_n$ *— булева функция, тогда функция*

$$f^*(x_1,\dots,x_n)=f'(x_1',\dots,x_n')$$

называется двойственной к булевой функции f.

Из определения непосредственно видно, что для любой булевой функции f выполняется равенство $f^{**}=f$.

Пример 1. Пусть $f=x\vee y$, $g=x$, $h=x'$, тогда, из определения следует, что $f^*=(x'\vee y')'\equiv x\cdot y$, $g^*=(x')'=x''\equiv x$, $h^*=(x'')'=x'''\equiv x'$.

Будем называть функцию f *самодвойственной,* если $f^*\equiv f$. Из предыдущего примера видно, что отрицание и тождественная функция являются самодвойственными, а дизъюнкция не самодвойственная.

Теорема 1. *Если булева функция* $\varphi(x_1,\dots,x_n)$ *реализована формулой*

$$f(f_1(x_1,\dots,x_n),\dots,f_n(x_1,\dots,x_n)),$$

где $f,f_1,\dots,f_n$ *— булевы функции, то формула*

$$f^*(f_1^*(x_1,\dots,x_n),\dots,f_n^*(x_1,\dots,x_n))$$

реализует функцию $\varphi^*(x_1,\dots,x_n)$.

Доказательство. $\varphi^*(x_1,\dots,x_n)=\varphi'(x_1',\dots,x_n')=\operatorname{func}f'(f_1(x_1',\dots,x_n'),\dots,f_n(x_1',\dots,x_n'))=$
$=\operatorname{func}f'(f_1''(x_1',\dots,x_n'),\dots,f_n''(x_1',\dots,x_n'))=\operatorname{func}f'(f_1^{*\prime}(x_1,\dots,x_n),\dots,f_n^{*\prime}(x_1,\dots,x_n)=$
$=\operatorname{func}f^*(f_1^*(x_1,\dots,x_n),\dots,f_n^*(x_1,\dots,x_n))$. ■

Следующая теорема носит название “принцип двойственности” и доказывается методом математической индукции, при этом индукционный переход происходит на основе только что доказанной теоремы.

Теорема 2 (Принцип двойственности). *Пусть* $\Phi=\{f_1,\dots,f_m\}$ *и* $\Phi^*=\{f_1^*,\dots,f_m^*\}$ *— базисы. Тогда, если формула* F *над базисом* Φ *реализует функцию* f*, то формула* F^* *над базисом* Φ^**, полученная из формулы* F *заменой* f_i *на двойственные функции* f_i^**, реализует функцию* f^**, то есть*

$$f=\operatorname{func}F[\Phi]\Longrightarrow f^*=\operatorname{func}F^*[\Phi^*],$$

где $F^*[\Phi^*]=F[\Phi]\{f_i^*//f_i\}_{i=1}^m$.

1.7. Новые термины. Булевы функции. Существенные и несущественные переменные. Базис, главная (внешняя) операция (функция), подформула. Равносильные формулы. Подстановка и замена. Двойственная и самодвойственная функции. Принцип двойственности.

1.8. Контрольные вопросы.

1. Сколько существует различных булевых функций от трех переменных?
2. Сколько формул реализует данную функцию f над данным базисом Φ?
3. Если Φ состоит из самодвойственных булевых функций, то что можно сказать о Φ^*?
4. Чему равна формула $(x\cdot y)\vee(z+(x\cdot y)')\{x//x\cdot y\}$?

1.9. Упражнения.

1. Докажите, что число булевых функций от n переменных, среди которых ровно k несущественных равно 2^{2^n-k}.
2. Проверьте равносильности теоремы 1.4.1 путем построения таблиц истинности.
3. Найдите функции, двойственные функциям $\cdot$, $\to$, $\sim$, $+$, $|$, $\downarrow$.
4. Выразите функции $\vee$, $\to$, $\sim$, $+$, $|$, $\downarrow$ через функции $\cdot$ и $'$.
5. Выразите функции $\vee$, $\cdot$, $\sim$, $+$, $|$, $\downarrow$ через функции $\to$ и $'$.

§ 2. Полные классы булевых функций

Разложение булевой функции по переменной. Выражение булевых функций через отрицание, конъюнкцию и дизъюнкцию. Совершенные нормальные формы булевых функций. Замкнутые, собственные м полные классы булевых функций. Примеры полных классов. Теорема о полноте системы булевых функций.

В современных ЭВМ система команд центрального процессора представляет собой, фактически, некоторое конечное множество булевых функций. В связи с этим возникает вопрос: существуют ли (и если существуют, то какие) классы булевых функций, обладающие тем свойством, что с их помощью можно выразить все другие булевы функции? В этом параграфе будет доказана теорема Поста о полноте класса булевых функций в которой устанавливаются необходимые и достаточные условия того, чтобы класс булевых функций обладал этим свойством

2.1. Выражение булевых функций через отрицание, конъюнкцию и дизъюнкцию.

В этом пункте доказывается, что все булевы функции (от любого количества аргументов) реализуются формулами над базисом $\{', \cdot, \vee\}$.

Лемма 1 (о разложении функции по переменной). *Для произвольной булевой функции от n переменных $f(x_1, \ldots, x_n)$ верны следующие формулы, называемые формулами разложения этой функции по переменной x_n:*

$$f(x_1, \ldots, x_n) \equiv \big(f(x_1, \ldots, x_{n-1}, 1) \cdot x_n\big) \vee \big(f(x_1, \ldots, x_{n-1}, 0) \cdot x_n'\big) \tag{1}$$

$$f(x_1, \ldots, x_n) \equiv \big(f(x_1, \ldots, x_{n-1}, 1) \vee x_n'\big) \cdot \big(f(x_1, \ldots, x_{n-1}, 0) \vee x_n\big) \tag{2}$$

Доказательство. Докажем формулу (1). Нужно проверить, что функции, стоящие в левой и правой частях равносильности, при одинаковых значениях аргументов имеют равные значения. Рассмотрим сначала всевозможные наборы аргументов вида $(a_1, \ldots, a_{n-1}, 1)$, где $a_1, \ldots, a_{n-1} \in \{0, 1\}$ и вычислим какие значения принимают на наборах такого вида функции, стоящие в правой и левой частях доказываемой равносильности.

$$\big(f(a_1, \ldots, a_{n-1}, 1) \cdot 1\big) \vee \big(f(a_1, \ldots, a_{n-1}, 0) \cdot 0\big) = f(a_1, \ldots, a_{n-1}, 1).$$

Видно, что на этом наборе переменных левая и правая часть доказываемой равносильности совпадают.

Для всевозможных наборов значений переменных вида $(a_1, \ldots, a_{n-1}, 0)$ также левая и правая части совпадают, так как

$$\big(f(a_1, \ldots, a_{n-1}, 1) \cdot 0\big) \vee \big(f(a_1, \ldots, a_{n-1}, 0) \cdot 1\big) = f(a_1, \ldots, a_{n-1}, 0).$$

Итак, функции из обеих частей доказываемой равносильности принимают одинаковые значения при одинаковых значениях их аргументов. Следовательно, эти функции равносильны и равносильность (1) справедлива.

Равносильность (2) доказывается аналогично. Проделайте это самостоятельно. ■

Заметим, что подобные формулы верны и для остальных переменных $x_1, \ldots, x_{n-1}$.

Теорема 1. *Всякая булева функция может быть представлена в виде суперпозиции отрицания, конъюнкции и дизъюнкции, то есть любая булева функция реализуется формулой над базисом $\{', \cdot \vee\}$.*

Доказательство. Метод математической индукции по числу n аргументов булевой функции. В предыдущем параграфе перечислены все булевы функции от одного аргумента. Так как

$$f_0(x) = 0 \equiv x \cdot x'$$
$$f_1(x) = x$$
$$f_2(x) = x'$$
$$f_3(x) = 1 \equiv x \vee x',$$

то утверждение теоремы справедливо для $n = 1$.

Пусть теорема верна для всех функций от k аргументов. Докажем ее для функций от $k+1$ аргументов. Пусть $f(x_1, \ldots, x_{k+1})$ — произвольная булева функция от $k+1$ аргумента. Тогда, по предыдущей лемме 2.1.1,

$$f(x_1, \ldots, x_{k+1}) = \big(f(x_1, \ldots, x_k, 1) \cdot x_{k+1}\big) \vee \big(f(x_1, \ldots, x_k, 0) \cdot x'_{k+1}\big)$$

Легко понять, что фиксирование в булевой функции одного аргумента приводит к булевой функции с числом аргументов на единицу меньшим числа аргументов исходной функции. Поэтому каждая из булевых функций $f(x_1, \ldots, x_k, 1)$ и $f(x_1, \ldots, x_k, 0)$ является булевой функцией от k аргументов. Но, по предположению индукции, каждая такая функция выражается через отрицание, конъюнкцию и дизъюнкцию. Принимая это во внимание видим, что правая часть последнего равенства равносильна булевой функции представляющей суперпозицию отрицания, конъюнкции и дизъюнкции. ■

Отметим, что доказательство этой теоремы практически предоставляет алгоритм для нахождения формулы над базисом $\{', \cdot, \vee\}$ реализующей данную булеву функцию. Для пояснения приведем следующий

Пример 1. Запишем формулу, выражающую булеву функцию $f(x, y) = x + y$ через отрицание, конъюнкцию и дизъюнкцию.

Воспользуемся формулой (1)

$$f(x, y) \equiv \big(f(x, 1) \cdot y\big) \vee \big(f(x, 0) \cdot y'\big). \tag{3}$$

Но, по той же формуле

$$f(x, 1) \equiv \big(f(1, 1) \cdot x\big) \vee \big(f(0, 1) \cdot x'\big),$$
$$f(x, 0) \equiv \big(f(1, 0) \cdot x\big) \vee \big(f(0, 0) \cdot x'\big).$$

Так как $f(1, 1) = f(0, 0) = 0$, $f(1, 0) = f(0, 1) = 1$, то

$$f(x, 1) \equiv \big(0 \cdot x\big) \vee \big(1 \cdot x'\big) \equiv x',$$
$$f(x, 0) \equiv \big(1 \cdot x\big) \vee \big(0 \cdot x'\big) \equiv x.$$

Подставляя в (3), получим

$$f(x, y) = x + y \equiv (x' \cdot y) \vee (x \cdot y').$$

2.2. Нормальные формы булевых функций. На основе теоремы 2.1.1, всякая булева функция может быть представлена некоторой формулой алгебры высказываний. Легко понять, что и всякая формула алгебры высказываний, представляет некоторую булеву функцию. В частности, одной из таких представляющих формул будет совершенная дизъюнктивная нормальная форма (если данная булева функция не является тождественным нулем) или совершенная конъюнктивная нормальная форма (если булева функция не тождественная единица). Отыскав совершенные нормальные формы для формулы алгебры высказываний, представляющей данную булеву функцию, можно перейти от этой формулы к формульному выражению для данной булевой функции. Его будем называть *совершенной дизъюнктивной (или конъюнктивной) нормальной формой* данной булевой функции. Каждая из них для данной булевой функции, ели она существует, единственна с точностью до перестановок.

Нахождение совершенных форм для булевых функций, заданных таблицей значений, проводится аналогично тому, как это делается в алгебре высказываний. Если функция задана в виде формулы, то необходимо сначала найти формулу, выражающую данную функцию через отрицание, конъюнкцию и дизъюнкцию.

2.3. Замкнутые и собственные классы булевых функций. Выше было показано, что любая булева функция выражается через функции базиса $\{', \cdot, \vee\}$. Это означает, что можно построить любой двоичный процессор, имея в распоряжении элементы, реализующие отрицание,

конъюнкцию и дизъюнкцию. Этот и следующий пункты посвящены нахождению критериев, которым должен удовлетворять базис булевых функций, чтобы через функции этого базиса можно было выразить любую булеву функцию.

Введем вначале несколько определений, обозначая через B множество всех булевых функций от произвольного числа аргументов.

Определение 1. *Пусть* $\Phi = \{f_1, \ldots, f_m\}$, $f_i \in B$, *Замыканием* $[\Phi]$ *класса* Φ *называется множество всех булевых, реализуемых формулами над* Φ, *то есть*

$$[\Phi] = \{f \in B \mid f = \operatorname{func} F[\Phi]\}.$$

Свойства замыканий, формулируемые в следующей теореме очевидным образом следуют из определения.

Теорема 1. *Для любых (не обязательно конечных) классов булевых функций* Φ, Φ_1 *и* Φ_2 *выполняются свойства:*

1. $\Phi \subseteq [\Phi]$,
2. $[[\Phi]] = [\Phi]$,
3. $\Phi_1 \subseteq \Phi_2 \Longrightarrow [\Phi_1] \subseteq [\Phi_2]$,
4. $\big([\Phi_1] \cup [\Phi_2]\big) \subseteq [\Phi_1 \cup \Phi_2]$.

Определение 2. *Класс булевых функций* Φ *называется замкнутым, если* $\Phi = [\Phi]$.

Определение 3. *Класс булевых функций* Φ *называется собственным, если он не пуст и не совпадает с классом всех булевых функций, то есть* $\Phi \neq \varnothing$ *и* $\Phi \neq B$.

В качестве примера рассмотрим следующие классы булевых функций, которые необходимы для дальнейшего изложения.

$T_0 = \{f \in B \mid f(0, \ldots, 0) = 0\}$ — класс функций, сохраняющих нуль.

$T_1 = \{f \in B \mid f(1, \ldots, 1) = 1\}$ — класс функций, сохраняющих единицу.

$T_* = \{f \in B \mid f \equiv f_*\}$ — класс самодвойственных функций.

$T_\leq = \{f \in B \mid \alpha \leq \beta \to f(\alpha) \leq f(\beta)\}$ — класс монотонных функций, где $\alpha = (a_1, \ldots, a_n)$, $\beta = (b_1, \ldots, b_n)$ и $a_i, b_i \in \{0, 1\}$. При этом $\alpha \leq \beta$ тогда и только тогда, когда $a_i \leq b_i$, $i \in \{1, \ldots, n\}$.

$T_L = \{f \in B \mid f(x_1, \ldots, x_n) \equiv a_0 + a_1x_1 + a_2x_2 + \ldots + a_nx_n\}$ — класс линейных функций, где $a_i \in \{0, 1\}$ и в записи a_ix_i опущен знак конъюнкции. Про функцию $f(x_1, \ldots, x_n)$ в этом случае говорят, что она представима в виде *линейного полинома Жегалкина.*

Теорема 2. *Классы* T_0, T_1, T_*, $T_\leq$, T_L *являются собственными замкнутыми классами булевых функций.*

Доказательство. Для того, чтобы убедиться в том, что эти классы собственные, приведем следующую таблицу, в которой знаком $+$ $(-)$ обозначается принадлежность (не принадлежность) функции соответствующему классу. Обосновать эту таблицу предлагается самостоятельно.

	T_0	T_1	T_*	$T_\leq$	T_L
0	$+$	$-$	$-$	$+$	$+$
1	$-$	$+$	$-$	$+$	$+$
x'	$-$	$-$	$+$	$-$	$+$
$x_1 \cdot x_2$	$+$	$+$	$-$	$+$	$-$
x	$+$	$+$	$+$	$+$	$+$

Из таблицы видно, что все эти классы непусты и не совпадают с B, причем $f(x) = x$ принадлежит всем этим классам, то есть они являются собственными.

Чтобы доказать замкнутость надо показать, что если функция реализована над классом, то она принадлежит этому классу.

1. Пусть $f, f_1, \ldots, f_n \in T_0$ и $F(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Тогда

$$F(0, \ldots, 0) = f(f_1(0, \ldots, 0), \ldots, f_n(0, \ldots, 0)) = f(0, \ldots, 0) = 0.$$

Следовательно, $\operatorname{func} F \in T_0$, то есть T_0 замкнут.

2. Пусть $f, f_1, \ldots, f_n \in T_1$ и $F(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Тогда

$$F(1, \ldots, 1) = f(f_1(1, \ldots, 1), \ldots, f_n(1, \ldots, 1)) = f(1, \ldots, 1) = 1.$$

Следовательно, $\operatorname{func} F \in T_1$, то есть T_1 замкнут.

3. Пусть $f, f_1, \ldots, f_n \in T_*$ и $F(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Тогда, по теореме 1.6.1, $F^* = f^*(f_1^*(x_1, \ldots, x_n), \ldots, f_n^*(x_1, \ldots, x_n)) \equiv f(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) = F(x_1, \ldots, x_n)$. Следовательно, $\operatorname{func} F \in T_*$, то есть T_* замкнут.

4. Пусть $f, f_1, \ldots, f_n \in T_\leq$ и $F(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Тогда, для $\alpha, \beta \in \{0,1\}^n$, из $\alpha \leq \beta$ следует $(f_1(\alpha), \ldots, f_n(\alpha)) \leq (f_1(\beta), \ldots, f_n(\beta))$, а отсюда следует, что $f(f_1(\alpha), \ldots, f_n(\alpha)) \leq f(f_1(\beta), \ldots, f_n(\beta))$, то есть $F(\alpha) \leq F(\beta)$. Это означает, что $\operatorname{func} F \in T_\leq$, то есть $T_\leq$ замкнут.

5. Пусть $f, f_1, \ldots, f_n \in T_L$ и $F(x_1, \ldots, x_n) = f(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$. Тогда

$$\begin{aligned} f &\equiv a_0 + a_1 x_1 + \ldots + a_n x_n \\ f_1 &\equiv a_{10} + a_{11} x_1 + \ldots + a_{1n} x_n \\ &\ldots \\ f_n &\equiv a_{n0} + a_{n1} x_1 + \ldots + a_{nn} x_n \end{aligned}$$

Подставляя эти выражения в запись формулы F получим

$$\begin{aligned} F(x_1, \ldots, x_n) \equiv a_0 + a_1(a_{10} + a_{11} x_1 + \ldots a_{1n} x_n) + \ldots + a_n(a_{n0} + a_{n1} x_1 + \ldots a_{nn} x_n) \equiv \\ \equiv d_0 + d_1 x_1 + \ldots + d_n x_n. \end{aligned}$$

Следовательно, $\operatorname{func} F \in T_L$, то есть T_L замкнут. ■

2.4. Полные классы булевых функций.

Определение 1. *Класс булевых функций Φ называется полным, если его замыкание совпадает с классом всех булевых функций, то есть*

$$[\Phi] = B.$$

Таким образом, множество булевых функций Φ образует полный класс, если любая булева функция реализуема в виде формулы над Φ.

Теорема 1. *Пусть заданы два класса булевых функций Φ_1 и Φ_2. Тогда, если класс Φ_1 полный и все функции из Φ_1 реализуемы формулами над Φ_2, то класс Φ_2 также полный.*

Доказательство. Пусть h — произвольная булева функция. Тогда, так как класс Φ_1 полный, то $h = \operatorname{func} F[\Phi_1]$. Пусть $\{f_1, \ldots, f_n\}$ — все булевы функции из класса Φ_1, которые входят в запись формулы $F[\Phi_1]$. Тогда, по условию, $f_i = \operatorname{func} G_i[\Phi_2]$. Значит $h = \operatorname{func} G[\Phi_2]$, где $G[\Phi_2] = F[\Phi_1]\{G_i//f_i\}_{i=1}^n$. Таким образом, произвольная булева функция h реализуема над базисом Φ_2, то есть Φ_2 является полным. ■

Пример 1. Классы булевых функций $\{', \cdot\}$, $\{', \vee\}$, $\{|\}$, $\{\downarrow\}$, $\{0, 1, \cdot, +\}$ являются полными в силу только что доказанной теоремы, так как в силу равносильностей теоремы 1.4.1 каждая из функций класса $\{', \cdot, \vee\}$ выражается через функции этих классов, а полнота класса $\{', \cdot, \vee\}$ доказана в п. IV.2.1.

Заметим, что формула над базисом $\{0, 1, \cdot, +\}$ называется *полиномом Жегалкина* и этот пример показывает, что каждая булева функция равносильна некоторому (не обязательно линейному) полиному Жегалкина.

Следующая теорема устанавливает необходимые и достаточные условия полноты классов булевых функций и была доказана американским математиком Э. Постом в 1921 году.

Теорема 2 (Пост). *Класс булевых функций Φ является полным тогда и только тогда, когда в этом классе есть функция не принадлежащая классу T_0, есть функция не принадлежащая классу T_1, есть функция не принадлежащая классу T_*, есть функция не принадлежащая классу $T_\leq$, есть функция не принадлежащая классу T_L, то есть*

$$[\Phi] = B \Longleftrightarrow \neg(\Phi \subseteq T_0 \vee \Phi \subseteq T_1 \vee \Phi \subseteq T_* \vee \Phi \subseteq T_\leq \vee \Phi \subseteq T_L).$$

Доказательство. *Необходимость.* Пусть $[\Phi] = B$ и $\Phi \subseteq T_0 \vee \Phi \subseteq T_1 \vee \Phi \subseteq T_* \vee \Phi \subseteq T_\leq \vee \Phi \subseteq T_L$. Тогда существует такое $i \in \{0, 1, *, \leq, L\}$, что $\Phi \subseteq T_i$. Отсюда, по теореме 2.3.1, $[\Phi] = B \subseteq [T_i]$. Но так как класс T_i замкнутый по теореме 2.3.2, то $B = T_i$, что противоречит тому, что T_i является собственным классом.

Достаточность. Пусть $\neg(\Phi \subseteq T_0 \vee \Phi \subseteq T_1 \vee \Phi \subseteq T_* \vee \Phi \subseteq T_\leq \vee \Phi \subseteq T_L)$. Тогда существует $\Phi' \subseteq \Phi$, $\Phi' = \{f_0, f_1, f_*, f_\leq, f_L\}$, где $f_0 \notin T_0$, $f_1 \notin T_1$, $f_* \notin T_*$, $f_\leq \notin T_\leq$, $f_L \notin T_L$, причем эти функции не обязательно различны и не обязательно $\Phi' = \Phi$.

Покажем, что булевы функции $'$ и $\cdot$ реализуемы в виде формул над Φ'. Построение будет проводиться в три этапа: на первом строятся формулы над Φ', реализующие константы 0 и 1, которые нужны на третьем этапе; на втором этапе строится формула, реализующая отрицание; на третьем этапе строится формула, реализующая конъюнкцию.

1. Построим формулу над Φ', реализующую 1. Пусть $\varphi(x) = f_0(x, \ldots, x)$. Тогда

$$\varphi(0) = f_0(0, \ldots, 0) \neq 0 \Longrightarrow \varphi(0) = 1.$$

Возможны два случая $\varphi(1) = 1$ и $\varphi(1) = 0$.

а) $\varphi(1) = 1$. В этом случае формула φ реализует 1.

б) $\varphi(1) = 0$. В этом случае формула φ реализует отрицание. Тогда рассмотрим функцию f_*. Так как $f_* \notin T_*$, то существуют $a_1, \ldots, a_n \in \{0, 1\}$ такие, что $f_*(a_1, \ldots, a_n) \neq f_*'(a_1', \ldots, a_n')$. Следовательно, $f_*(a_1, \ldots, a_n) = f_*(a_1', \ldots, a_n')$.

Обозначим для $x, \alpha \in \{0, 1\}$

$$x^\alpha = \begin{cases} x, & \text{если } \alpha = 0, \\ x', & \text{если } \alpha = 1. \end{cases}$$

Тогда $0^\alpha = \alpha$ и $1^\alpha = \alpha'$. Пусть теперь $\psi(x) = f_*(x^{a_1}, \ldots, x^{a_n})$. Тогда

$$\psi(0) = f_*(0^{a_1}, \ldots, 0^{a_n}) = f_*(a_1, \ldots, a_n) = f_*(a_1', \ldots, a_n') = f_*(1^{a_1}, \ldots, 1^{a_n}) = \psi(1).$$

Таким образом, $\psi(0) = \psi(1)$, то есть $\psi(x) \equiv 1$ или $\psi(x) \equiv 0$. Если $\psi(x) \equiv 1$, то искомая константа 1 построена. Если же ψ реализует 0, то функция $\varphi(\psi(x))$ реализует единицу.

Построение константы 0 проводится аналогично, только вместо f_0 нужно использовать f_1.

2. Построим формулу, реализующую отрицание. Рассмотрим функцию $f_\leq$. Так как $f_\leq \notin T_\leq$, то существуют $\alpha = (a_1, \ldots, a_n)$ и $\beta = (b_1, \ldots, b_n)$, $a_i, b_i \in \{0, 1\}$ такие, что $\alpha \leq \beta$ и $f_\leq(\alpha) > f_\leq(\beta)$. Из того, что $f_\leq(\alpha) \neq f_\leq(\beta)$ следует, что $\alpha \neq \beta$. Значит множество $J = \big\{j \in \{1, \ldots, n\} \mid a_j = 0, b_j = 1\big\}$ непусто. То есть J — множество индексов j на которых $a_j \neq b_j$, а на остальных индексах $k \in \{1, \ldots, n\} \setminus J$, $a_k = b_k$.

Пусть $\varphi(x) = f_\leq(c_1, \ldots, c_n)$, где $c_j = \begin{cases} x, & \text{если } j \in J, \\ a_j = b_j, & \text{если } j \notin J. \end{cases}$

Тогда

$$\varphi(0) = f_\leq(c_1, \ldots, c_n)\{0//x\} = f_\leq(\alpha) > f_\leq(\beta) = f_\leq(c_1, \ldots, c_n)\{1//x\} = \varphi(1),$$

то есть $\varphi(0) > \varphi(1)$. Это означает, что $\varphi(0) = 1$, а $\varphi(1) = 0$, то есть $\varphi(x) \equiv x'$.

3. Постоим функцию, реализующую конъюнкцию. Рассмотрим функцию f_L. Эта функция реализуема над полным классом $\{0, 1, +, \cdot\}$ в виде полинома Жегалкина, но $f_L \notin T_L$, следовательно, этот полином не является линейным. Значит f_L содержит нелинейное слагаемое, содержащее конъюнкцию по крайней мере двух переменных. Пусть, для определенности, это x_1 и x_2. Тогда

$$f_L(x_1, x_2, \ldots, x_n) = x_1 \cdot x_2 \cdot f_a(x_3, \ldots, x_n) + x_1 \cdot f_b(x_3, \ldots, x_n) + x_2 \cdot f_c(x_3, \ldots, x_n) + f_d(x_3, \ldots, x_n),$$

причем $f_a(x_3, \ldots, x_n) \not\equiv 0$, то есть существуют такие $a_3, \ldots, a_n \in \{0, 1\}$, что $f_a(a_3, \ldots, a_n) = 1$. Обозначим $f_b(a_3, \ldots, a_n) = b$, $f_c(a_3, \ldots, a_n) = c$, $f_d(a_3, \ldots, a_n) = d$, то есть $b, c, d \in \{0, 1\}$.

Пусть

$$\varphi(x_1, x_2) = f_L(x_1, x_2, a_3, \ldots, a_n) = x_1 \cdot x_2 + b \cdot x_1 + c \cdot x_2 + d,$$
$$\psi(x_1, x_2) = \varphi(x_1 + c, x_2 + b) + b \cdot c + d.$$

Тогда

$$\psi(x_1, x_2) = (x_1 + c) \cdot (x_2 + b) + b \cdot (x_1 + c) + c \cdot (x_2 + b) + d + b \cdot c + d \equiv$$
$$\equiv x_1 \cdot x_2 + c \cdot x_2 + b \cdot x_1 + b \cdot c + b \cdot x_1 + b \cdot c + c \cdot x_2 + b \cdot c + d + b \cdot c + d \equiv x_1 \cdot x_2.$$

Заметим, что функции вида $x + a$ реализуемы, так как $x + 1 \equiv x'$, $x + 0 \equiv x$, а константы 0, 1 и отрицание уже построены.

Итак, доказано, что каждая функция полного (см. пример 2.4.1) класса $\{', \cdot\}$ выражается через функции класса Φ'. Значит, по теореме 2.4.1, класс булевых функций Φ', а, следовательно, и его надкласс Φ являются полными. ■

2.5. Новые термины. Совершенные нормальные формы булевых функций. Замкнутые, собственные и полные классы булевых функций.

2.6. Контрольные вопросы.

1. Является ли класс всех булевых функций замкнутым, полным, собственным?
2. Может ли полный класс булевых функций быть незамкнутым?
3. Является ли произвольный надкласс полного класса булевых функций полным?

2.7. Упражнения.

1. Запишите и докажите формулы разложения булевой функции $f(x_1, \ldots, x_n)$ по переменной x_1.
2. Постройте СДНФ и СКНФ для булевых функций $x \,|\, y$, $x \downarrow y$, $x \to y$, $x + y$.
3. Докажите теорему 2.3.1.
4. Проверьте принадлежность классам T_0, T_1, T_*, $T_\leq$, T_L функций $|$, $\downarrow$, $\vee$, $\to$, $+$.
5. Докажите, что если $f \notin T_0$, то тогда $f \in T_*$ или $f \notin (T_1 \cup T_\leq)$.
6. Найдите все самодвойственные булевы функции от двух переменных.
7. Среди булевых функций от одного и двух переменных найдите все функции, сохраняющие 0 и все функции, сохраняющие 1.
8. Докажите, что среди булевых функций от n переменных число функций, сохраняющих 0, равно числу функций, сохраняющих 1.
9. В доказательстве теоремы Поста 2.4.2, постройте формулу, реализующую константу 0.
10. Являются ли полными следующие классы булевых функций:
    (a) $\{', \vee\}$;
    (b) $\{\cdot, \vee, \to\}$;
    (c) $\{', \sim\}$;
    (d) $\{+, \cdot, 1\}$;
    (e) $\{'\}$;
    (f) $\{h_3\}$, где $h_3(x, y, z) = (x \vee y \vee z)'$;
    (g) $\{h_n\}$, где $h_n(x_1, x_2, \ldots, x_n) = (x_1 \vee x_2 \vee \ldots \vee x_n)'$;
11. Докажите, что из всякого полного класса булевых функций можно выделить конечный полный подкласс.

Глава V

Исчисление высказываний

§ 1. Язык и аксиомы исчисления высказываний. Теорема дедукции

Формальные и содержательные аксиоматические теории. Принцип построения формальных аксиоматических теорий. Выводимые формулы (теоремы). Выводимость из множества формул. Язык исчисления высказываний (ИВ). Аксиомы и правила вывода ИВ. Пример выводимости в ИВ. Теорема дедукции. Следствия из теоремы дедукции.

1.1. Формальные и содержательные аксиоматические теории. Всякая аксиоматическая теория строится по следующему принципу. Вначале определяются какие-то первоначальные неопределяемые понятия, вводится система обозначений и т. д. Иными словами строится язык теории. Затем на этом языке вводится список первичных соотношений между первичными понятиями: эти первичные соотношения называются аксиомами данной теории. И затем осуществляется развитие этой теории. То есть на основании аксиом доказываются новые соотношения между первичными понятиями. Путем определений через первичные понятия и определенные ранее вводятся новые понятия. Доказываются соотношения между вновь введенными понятиями, вновь введенными и первичными и т. д. Доказываемые соотношения называются теоремами (леммами, следствиями, предложениями). Возникает вопрос о том, какими средствами осуществляется вывод одних теорем из других, то есть вопрос правилах вывода. Совокупность этих правил назовем *логическими средствами* теории. С этой точки зрения все аксиоматические теории можно разделить на два класса: *содержательные* и *формальные*. Содержательные аксиоматические теории — это теории, правила вывода в которых считаются интуитивно известными и вопрос о их формализации не ставится. К таким теориям относятся, например, геометрия, изучаемая в школьном курсе. Формальные аксиоматические теории — это теории, в которых логический аппарат постулируется, то есть указывается перечень правил, которыми и только которыми можно пользоваться при выводе одних утверждений из других. Отсюда становится понятным, что формальные аксиоматические теории — это теории более высокого уровня строгости. Одна и та же теория, по существу, может строиться как содержательная и как формальная теория. В главе III изучалась алгебра высказываний как теория содержательная. Цель настоящей главы формализовать эту теорию. Ее формализацию будем называть *исчислением высказываний*. По сути дела формализован будет класс всех тавтологий. То есть некоторые из тавтологий будут объявлены аксиомами и будут приведены правила вывода так, что выводимыми из аксиом окажутся тавтологии и только они.

1.2. Принцип построения формальных аксиоматических теорий. Формальная теория $\mathfrak{T}$ считается заданной, если выполнены условия 1–4.

1. Задан счетный алфавит X этой теории.

2. Во множестве $F(X)$ всех слов в алфавите X выделено подмножество $\Phi \subseteq F(X)$. Слова из Φ называются *формулами* этой теории.

3. В Φ выделено некоторое подмножество $\Phi_A \subset \Phi$. Формулы из Φ_A называются аксиомами теории $\mathfrak{T}$. Пара $\langle F(X), \Phi \rangle$ называется *языком* теории $\mathfrak{T}$.

4. Имеется конечное множество $f_1, \ldots, f_n$ частичных функций из множества формул Φ в Φ. Эти частичные функции называются *правилами вывода* теории $\mathfrak{T}$. При этом, если f_i — m-местная частичная функция и $f_i(\mathfrak{a}_1, \ldots, \mathfrak{a}_m) = \mathfrak{a}$, то говорят, что $\mathfrak{a}$ выводима из $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ по правилу f_i.

Определение 1. *Выводом теории* $\mathfrak{T}$ *называется всякая конечная последовательность формул этой теории, каждая из которых является либо аксиомой, либо получена из предыдущих формул по одному из правил вывода.*

Формула $\mathfrak{a}$ *называется выводимой формулой (теоремой) теории* $\mathfrak{T}$*, если существует вывод, оканчивающийся этой формулой. Вывод этот называется выводом (доказательством) формулы (теоремы)* $\mathfrak{a}$*. Для выводимой формулы* $\mathfrak{a}$ *принято обозначение* $\vdash \mathfrak{a}$.

1.3. Выводимость из множества формул.

Определение 1. *Конечная последовательность формул называется выводом из множества формул* Γ*, если каждая формула этой последовательности является либо аксиомой, либо принадлежит* Γ*, либо получена из предыдущих формул применением одного из правил вывода.*

Формула $\mathfrak{a}$ *называется выводимой из множества формул* Γ*, если существует вывод из* Γ*, оканчивающийся формулой* $\mathfrak{a}$*. Обозначается* $\Gamma \vdash \mathfrak{a}$*. Формулы из* Γ *называются гипотезами.*

Понятно, что если $\Gamma = \varnothing$, то в действительности $\mathfrak{a}$ — выводимая формула. При этом вместо записи $\varnothing \vdash \mathfrak{a}$ пишут $\vdash \mathfrak{a}$.

Отметим, что между понятиями выводимости и выводимости из гипотез существует тесная связь, которая выражается теоремой дедукции. Она будет в дальнейшем доказана.

Теорема 1. *Понятие выводимости из гипотез обладает следующими свойствами 1–3.*

1. $\Delta \subseteq \Gamma$ *и* $\Delta \vdash \mathfrak{a}$*, то* $\Gamma \vdash \mathfrak{a}$.

2. $\Gamma \vdash \mathfrak{a}$ *тогда и только тогда когда в* Γ *существует конечное подмножество* Δ*, для которого* $\Delta \vdash \mathfrak{a}$.

3. Если $\Gamma \vdash \mathfrak{b}$ *для любой формулы* $\mathfrak{b}$ *из* Δ *и* $\Delta \vdash \mathfrak{a}$*, то* $\Gamma \vdash \mathfrak{a}$.

Доказательство. 1. Очевидно.

2. Если в Γ существует подмножество (не обязательно конечное) Δ, для которого $\Delta \vdash \mathfrak{a}$, то по свойству 1, $\Gamma \vdash \mathfrak{a}$.

Пусть теперь $\Gamma \vdash \mathfrak{a}$. Тогда существует вывод из Γ, оканчивающийся $\mathfrak{a}$:

$$\mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{a}.$$

Обозначим через Δ множество формул из этого вывода, принадлежащих Γ. Понятно, что $\Delta \vdash \mathfrak{a}$, $\Delta \subseteq \Gamma$ и Δ — конечное.

3. Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n, \mathfrak{a}$ — вывод $\mathfrak{a}$ из Δ и пусть $\mathfrak{a}'_1, \mathfrak{a}'_2, \ldots, \mathfrak{a}'_s$ — формулы этого вывода, принадлежащие Δ. По условию они выводимы из Γ. Запишем их соответствующие выводы из Γ:

$$\begin{gathered}\mathfrak{b}_{11}, \mathfrak{b}_{12}, \ldots, \mathfrak{b}_{1k_1}, \mathfrak{a}'_1;\\ \mathfrak{b}_{21}, \mathfrak{b}_{22}, \ldots, \mathfrak{b}_{2k_2}, \mathfrak{a}'_2;\\ \ldots\ldots\ldots\ldots\ldots\\ \mathfrak{b}_{s1}, \mathfrak{b}_{s2}, \ldots, \mathfrak{b}_{sk_s}, \mathfrak{a}'_s.\end{gathered}$$

Вставив в вывод $\mathfrak{a}$ из Δ вместо формул $\mathfrak{a}'_1, \mathfrak{a}'_2, \ldots, \mathfrak{a}'_s$ их соответствующие выводы из Γ, получим вывод формулы $\mathfrak{a}$ из Γ. ■

1.4. Язык ИВ.

Алфавит ИВ состоит из следующих символов.

1. $\{A_1, A_2, \ldots\}$ — счетное множество букв.
2. $\neg$, $\to$ — связки (логические символы).
3.), (— вспомогательные символы (правая и левая скобки).

Определение 1 (формулы). *1. Все буквы алфавита ИВ являются формулами.*

2. Если $\mathfrak{a}$ *и* $\mathfrak{b}$ *— формулы, то* $\neg\mathfrak{a}$ *и* $(\mathfrak{a} \to \mathfrak{b})$ *также являются формулами.*

3. Других формул, кроме указанных в пунктах 1–2 нет.

В дальнейшем условимся внешние скобки в формулах опускать.

1.5. Аксиомы и правила вывода ИВ. Для любых формул $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{C}$ следующие формулы являются аксиомами ИВ.

Аксиома 1. $\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{a})$.

Аксиома 2. $(\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c})) \to ((\mathfrak{a} \to \mathfrak{b}) \to (\mathfrak{a} \to \mathfrak{c}))$.

Аксиома 3. $(\neg\mathfrak{b} \to \neg\mathfrak{a}) \to ((\neg\mathfrak{b} \to \mathfrak{a}) \to \mathfrak{b})$.

Единственным правилом вывода ИВ является частичная функция f вида:

$$f(\mathfrak{a}, \mathfrak{a} \to \mathfrak{b}) = f(\mathfrak{a} \to \mathfrak{b}, \mathfrak{a}) = \mathfrak{b}.$$

Будем его записывать в виде: $\mathfrak{a}, \mathfrak{a} \to \mathfrak{b} \vdash \mathfrak{b}$.

Это правило вывода называют правилом *отделения* (посылки) или *Modus ponens,* сокращенно MP.

В действительности, аксиом бесконечное множество, а выше приведены лишь схемы аксиом. Так например, является аксиомой 1 формула:

$$(\mathfrak{a} \to \mathfrak{b}) \to (\mathfrak{c} \to (\mathfrak{a} \to \mathfrak{b})).$$

1.6. Пример выводимости в ИВ.

Лемма 1. *Для любой формулы* $\mathfrak{a}$ *справедлива выводимость:*

$$\vdash (\mathfrak{a} \to \mathfrak{a})$$

Доказательство. Построим вывод, оканчивающийся формулой $(\mathfrak{a} \to \mathfrak{a})$.

1. $(\mathfrak{a} \to ((\mathfrak{a} \to \mathfrak{a}) \to \mathfrak{a})) \to ((\mathfrak{a} \to (\mathfrak{a} \to \mathfrak{a})) \to (\mathfrak{a} \to \mathfrak{a}))$ — Аксиома 2.
2. $\mathfrak{a} \to ((\mathfrak{a} \to \mathfrak{a}) \to \mathfrak{a})$ — Аксиома 1.
3. $(\mathfrak{a} \to (\mathfrak{a} \to \mathfrak{a})) \to (\mathfrak{a} \to \mathfrak{a})$ — MP 2, 1.
4. $\mathfrak{a} \to (\mathfrak{a} \to \mathfrak{a})$ — Аксиома 1.
5. $(\mathfrak{a} \to \mathfrak{a})$ — MP 4, 3. ■

1.7. Теорема дедукции. Теорема дедукции, как было отмечено ранее, устанавливает важную связь между понятиями выводимости и выводимости из гипотез. Во многих случаях она существенно облегчает доказательство выводимости тех или иных формул.

Теорема 1. *Пусть* Γ *— множество формул,* $\mathfrak{a}$ *и* $\mathfrak{b}$ *какие-то формулы ИВ.*

Если $\Gamma, \mathfrak{a} \vdash \mathfrak{b}$, *то* $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b})$.

Доказательство. Так как $\mathfrak{b}$ выводима из Γ и $\mathfrak{a}$, то существует вывод $\mathfrak{b}$ из Γ и $\mathfrak{a}$. Пусть $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_n = \mathfrak{b}$ — вывод $\mathfrak{b}$ из Γ и $\mathfrak{a}$, то есть формула этого вывода либо из Γ, либо совпадает с $\mathfrak{a}$, либо получена из предыдущих применением правила вывода MP. Индукцией по i, $1 \le i \le n$, покажем, что: $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_i)$. При $i = n$ это будет, в частности, заключение теоремы.

Пусть $i = 1$. Докажем, что $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_1)$. Так как $\mathfrak{b}_1$ — первая формула вывода, то она не может быть получена при помощи MP из предыдущих. Тогда для $\mathfrak{b}_1$ возможны следующие случаи:

a) $\mathfrak{b}_1$ — аксиома;

b) $\mathfrak{b}_1 \in \Gamma$;

c) $\mathfrak{b}_1 = \mathfrak{a}$.

Рассмотрим каждый из этих случаев.

a) Строим вывод для $(\mathfrak{a} \to \mathfrak{b}_1)$.

1. $\mathfrak{b}_1$ — Аксиома.
2. $\mathfrak{b}_1 \to (\mathfrak{a} \to \mathfrak{b}_1)$ — Аксиома 1.
3. $\mathfrak{a} \to \mathfrak{b}_1$ — MP 1, 2.

$\vdash (\mathfrak{a} \to \mathfrak{b}_1)$, следовательно $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_1)$.

b) Также строим вывод для $(\mathfrak{a} \to \mathfrak{b}_1)$.

1. $\mathfrak{b}_1$ — Гипотеза из Γ.
2. $\mathfrak{b}_1 \to (\mathfrak{a} \to \mathfrak{b}_1)$ — Аксиома 1.
3. $(\mathfrak{a} \to \mathfrak{b}_1)$ — MP 1, 2.

$\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_1)$.

c) Так как в этом случае $\mathfrak{b}_1 = \mathfrak{a}$, то по лемме 1.6.1 $\vdash (\mathfrak{a} \to \mathfrak{b}_1)$.

Итак, для $i = 1$ теорема доказана. Пусть теперь для всякого k, $1 \leq k < i$,

$$\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_k).$$

Для $\mathfrak{b}_i$ теперь имеется 4 возможных случая:

a) $\mathfrak{b}_i$ — аксиома;

b) $\mathfrak{b}_i \in \Gamma$;

c) $\mathfrak{b}_i = \mathfrak{a}$;

d) $\mathfrak{b}_i$ получена из предыдущих формул при помощи правила MP.

Случаи a) — c) доказываются точно также как и для $i = 1$.

d) Пусть $\mathfrak{b}_i$ получена из формул $\mathfrak{c}$ и $\mathfrak{d}$ при помощи правила MP. Это означает, что $\mathfrak{c}$ есть некоторая формула $\mathfrak{b}_j$, $j < i$, а формула $\mathfrak{d}$ обязана иметь вид $\mathfrak{b}_j \to \mathfrak{b}_i$.

1. $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_j)$ — индуктивное предположение.
2. $\Gamma \vdash (\mathfrak{a} \to (\mathfrak{b}_j \to \mathfrak{b}_i))$ — индуктивное предположение.
3. $\Gamma \vdash (\mathfrak{a} \to (\mathfrak{b}_j \to \mathfrak{b}_i)) \to ((\mathfrak{a} \to \mathfrak{b}_j) \to (\mathfrak{a} \to \mathfrak{b}_i))$ — Аксиома 2.
4. $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_j) \to (\mathfrak{a} \to \mathfrak{b}_i)$ — MP 2, 3.
5. $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b}_i)$ — MP 1, 4.

Как отмечалось выше, при $i = n$ получаем: $\Gamma \vdash (\mathfrak{a} \to \mathfrak{b})$. ■

1.8. Следствия из теоремы дедукции.

Следствие 1 (Правило силлогизма). *Для любых формул* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ *справедлива выводимость:*

$$(\mathfrak{a} \to \mathfrak{b}),\ (\mathfrak{b} \to \mathfrak{c}) \vdash (\mathfrak{a} \to \mathfrak{c}).$$

Доказательство. В качестве множества формул Γ возьмем

$$\Gamma = \{(\mathfrak{a} \to \mathfrak{b}), (\mathfrak{b} \to \mathfrak{c})\},$$

а в качестве формулы $\mathfrak{a}$ — формулу $\mathfrak{a}$.

1. $(\mathfrak{a} \to \mathfrak{b})$ — гипотеза.
2. $(\mathfrak{b} \to \mathfrak{c})$ — гипотеза.
3. $\mathfrak{a}$ — гипотеза.
4. $\mathfrak{b}$ — MP 3, 1.
5. $\mathfrak{c}$ — MP 4, 2.

$(\mathfrak{a} \to \mathfrak{b}), (\mathfrak{b} \to \mathfrak{c}), \mathfrak{a} \vdash \mathfrak{c}$.

Применяем теорему дедукции: $(\mathfrak{a} \to \mathfrak{b}), (\mathfrak{b} \to \mathfrak{c}) \vdash (\mathfrak{a} \to \mathfrak{c})$. ■

В дальнейшем будем пользоваться этим дополнительным правилом вывода и будем его обозначать ПС.

Следствие 2 (Правило исключения промежуточной посылки ПИПП). *Для любых формул* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ *справедлива выводимость:* $\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c}),\ \mathfrak{b} \vdash (\mathfrak{a} \to \mathfrak{c})$.

Доказательство.

1. $\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c})$ — гипотеза.
2. $\mathfrak{b}$ — гипотеза.
3. $\mathfrak{a}$ — гипотеза.
4. $(\mathfrak{b} \to \mathfrak{c})$ — MP 3, 1.
5. $\mathfrak{c}$ — MP 2, 4.

$\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c}),\ \mathfrak{b},\ \mathfrak{a} \vdash \mathfrak{c} \Longrightarrow \mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c}),\ \mathfrak{b} \vdash (\mathfrak{a} \to \mathfrak{c})$. ■

Будем в дальнейшем пользоваться и этим дополнительным правилом вывода и обозначать ПИПП.

1.9. Новые термины. Аксиоматические теории: формальные и содержательные. Логические средства формальной теории. Язык теории. Правила вывода. Вывод теории. Вывод данной формулы (доказательство). Выводимость из гипотез. Правило отделения (modus ponens). Правило силлогизма, правило исключения промежуточной посылки.

1.10. Контрольные вопросы.

1. Чем отличаются формальные от содержательных аксиоматических теорий?
2. Изложите принцип построения формальных аксиоматических теорий.
3. Почему в формализации АВ используются лишь две связки, а не все пять?
4. Дайте определение выводимости и выводимости из гипотез. Сравните их.
5. Что можно сказать о первых двух формулах вывода ИВ?
6. Что можно сказать о первых двух формулах вывода из множества формул Г?
7. Являются ли выводимыми формулами аксиомы ИВ? Если да, то какова длина их минимального вывода?
8. Из каких символов состоит алфавит ИВ?

1.11. Упражнения.

1. Приведите доказательство для случаев а) – с) (см. доказательство теоремы дедукции, индукционный шаг).
2. Доказать, построив вывод:
   (a) $\vdash (\neg\mathfrak{a} \to \mathfrak{a}) \to \mathfrak{a}$;
   (b) правило силлогизма;
   (c) $\mathfrak{a} \to (\mathfrak{b} \to \mathfrak{c}) \vdash \mathfrak{b} \to (\mathfrak{a} \to \mathfrak{c})$;
   (d) $\vdash (\neg\mathfrak{b} \to \neg\mathfrak{a}) \to (\mathfrak{a} \to \mathfrak{b})$.
3. Используя теорему дедукции, докажите, что
   если $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n \vdash \mathfrak{b}$, то $\vdash \mathfrak{a}_1 \to (\ldots(\mathfrak{a}_{n-1} \to (\mathfrak{a}_n \to \mathfrak{b}))\ldots)$.
4. Доказать, используя теорему дедукции:
   (a) $\vdash (\mathfrak{a} \to \mathfrak{b}) \to ((\mathfrak{a} \to \neg\mathfrak{b}) \to \neg\mathfrak{a})$;
   (b) $\vdash (\mathfrak{a} \to \mathfrak{b}) \to ((\neg\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b})$;
   (c) $\vdash \neg(\mathfrak{a} \to \neg\mathfrak{b}) \to \mathfrak{a}$;
   (d) $\mathfrak{a} \vdash \neg a \to \mathfrak{b}$;
   (e) $\vdash ((\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{a}) \to \mathfrak{a}$.

§ 2. Теорема о выводимости

Закон двойного отрицания. Закон противоречивой посылки. Законы контрапозиции. Первое правило отрицания импликации. Обобщенное правило противоречивой посылки. Теорема о выводимости.

В нижеследующих пяти пунктах (V.2.1.–V.2.5.) $\mathfrak{a}$ и $\mathfrak{b}$ — произвольные формулы ИВ.

2.1. Закон двойного отрицания.

Лемма 1. *Справедливы выводимости:*

a) $\vdash \neg\neg\mathfrak{b} \to \mathfrak{b}$;

b) $\vdash \mathfrak{b} \to \neg\neg\mathfrak{b}$.

Доказательство.

a)
1. $(\neg\mathfrak{b} \to \neg\neg\mathfrak{b}) \to ((\neg\mathfrak{b} \to \neg\mathfrak{b}) \to \mathfrak{b})$ — Аксиома 3.
2. $(\neg\mathfrak{b} \to \neg\mathfrak{b})$ — Лемма 1.6.1.
3. $(\neg\mathfrak{b} \to \neg\neg\mathfrak{b}) \to \mathfrak{b}$ — ПИПП 1, 2.
4. $\neg\neg\mathfrak{b} \to (\neg\mathfrak{b} \to \neg\neg\mathfrak{b})$ — Аксиома 1.
5. $\neg\neg\mathfrak{b} \to \mathfrak{b}$ — ПС 4, 3.

b)
1. $(\neg\neg\neg\mathfrak{b} \to \neg\mathfrak{b}) \to ((\neg\neg\neg\mathfrak{b} \to \mathfrak{b}) \to \neg\neg\mathfrak{b})$ — Аксиома 3.
2. $\neg\neg\neg\mathfrak{b} \to \neg\mathfrak{b}$ — п. a).
3. $(\neg\neg\neg\mathfrak{b} \to \mathfrak{b}) \to \neg\neg\mathfrak{b}$ — MP 2, 1.
4. $\mathfrak{b} \to (\neg\neg\neg\mathfrak{b} \to \mathfrak{b})$ — Аксиома 1.
5. $\mathfrak{b} \to \neg\neg\mathfrak{b}$ — ПС 4, 3. ■

2.2. Закон противоречивой посылки.

Лемма 1. $\vdash \neg\mathfrak{a} \to (\mathfrak{a} \to \mathfrak{b})$.

Доказательство.

1. $\neg\mathfrak{a}$ — гипотеза.
2. $\mathfrak{a}$ — гипотеза.
3. $\neg\mathfrak{a} \to (\neg\mathfrak{b} \to \neg\mathfrak{a})$ — Аксиома 1.
4. $\mathfrak{a} \to (\neg\mathfrak{b} \to \mathfrak{a})$ — Аксиома 1.
5. $\neg\mathfrak{b} \to \neg\mathfrak{a}$ — MP 1, 3.
6. $\neg\mathfrak{b} \to \mathfrak{a}$ — MP 2, 4.
7. $(\neg\mathfrak{b} \to \neg\mathfrak{a}) \to ((\neg\mathfrak{b} \to \mathfrak{a}) \to \mathfrak{b})$ — Аксиома 3.
8. $(\neg\mathfrak{b} \to \mathfrak{a}) \to \mathfrak{b}$ — MP 5, 7.
9. $\mathfrak{b}$ — MP 6, 8.

Имеем $\neg\mathfrak{a}, \mathfrak{a} \vdash \mathfrak{b}$. Следовательно, по теореме дедукции, $\neg\mathfrak{a} \vdash (\mathfrak{a} \to \mathfrak{b})$. Еще раз применяя теорему дедукции получим $\vdash \neg\mathfrak{a} \to (\mathfrak{a} \to \mathfrak{b})$. ■

2.3. Закон контрапозиции.

Лемма 1. *Справедливы выводимости:*

a) $(\neg\mathfrak{b} \to \neg\mathfrak{a}) \to (\mathfrak{a} \to \mathfrak{b})$;

b) $(\mathfrak{a} \to \mathfrak{b}) \to (\neg\mathfrak{b} \to \neg\mathfrak{a})$.

Доказательство.

a) 1. $\neg\mathfrak{b} \to \neg\mathfrak{a}$ — гипотеза.
2. $\mathfrak{a}$ — гипотеза.
3. $(\neg\mathfrak{b} \to \neg\mathfrak{a}) \to ((\neg\mathfrak{b} \to \mathfrak{a}) \to \mathfrak{b})$ — Аксиома 3.
4. $(\neg\mathfrak{b} \to \mathfrak{a}) \to \mathfrak{b}$ — MP 1, 3.
5. $\mathfrak{a} \to (\neg\mathfrak{b} \to \mathfrak{a})$ — Аксиома 1.
6. $\neg\mathfrak{b} \to \mathfrak{a}$ — MP 2, 5.
7. $\mathfrak{b}$ — MP 6, 4.

Имеем $\mathfrak{b} \to \neg\mathfrak{a}, \mathfrak{a} \vdash \mathfrak{b}$. Следовательно, по теореме дедукции, $\neg\mathfrak{b} \to \neg\mathfrak{a} \vdash (\mathfrak{a} \to \mathfrak{b})$. Еще раз применяя теорему дедукции получим $\vdash (\neg\mathfrak{b} \to \neg\mathfrak{a}) \to (\mathfrak{a} \to \mathfrak{b})$.

b) 1. $\mathfrak{a} \to \mathfrak{b}$ — гипотеза.
2. $\neg\neg\mathfrak{a} \to \mathfrak{a}$ — Лемма 2.1.1 a).
3. $\mathfrak{b} \to \neg\neg\mathfrak{b}$ — Лемма 2.1.1 b).
4. $(\neg\neg\mathfrak{a} \to \mathfrak{b})$ — ПС 2, 1.
5. $\neg\neg\mathfrak{a} \to \neg\neg\mathfrak{b}$ — ПС 4, 3.
6. $(\neg\neg\mathfrak{a} \to \neg\neg\mathfrak{b}) \to (\neg\mathfrak{b} \to \neg\mathfrak{a})$ — п. a).
7. $\neg\mathfrak{b} \to \neg\mathfrak{a}$ — MP 5, 6.

Имеем $\mathfrak{a} \to \mathfrak{b} \vdash \neg\mathfrak{b} \to \neg\mathfrak{a}$. Следовательно, по теореме дедукции $\vdash (\mathfrak{a} \to \mathfrak{b}) \to (\neg\mathfrak{b} \to \neg\mathfrak{a})$. ■

2.4. Первое правило отрицания импликации.

Лемма 1. $\vdash \mathfrak{a} \to (\neg\mathfrak{b} \to \neg(\mathfrak{a} \to \mathfrak{b}))$.

Доказательство.

1. $\mathfrak{a}, \mathfrak{a} \to \mathfrak{b} \vdash \mathfrak{b}$ — правило MP
2. $\mathfrak{a} \vdash (\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b}$ — теорема дедукции к 1.
3. $\vdash \mathfrak{a} \to ((\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b})$ — теорема дедукции к 2.
4. $\vdash ((\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b}) \to (\neg\mathfrak{b} \to \neg(\mathfrak{a} \to \mathfrak{b}))$ — Лемма 2.3.1 b).
5. $\vdash \mathfrak{a} \to (\neg\mathfrak{b} \to \neg(\mathfrak{a} \to \mathfrak{b}))$ — ПС 3, 4. ■

2.5. Обобщенное правило противоречивой посылки.

Лемма 1. $\vdash (\mathfrak{a} \to \mathfrak{b}) \to ((\neg\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b})$.

Доказательство.

1. $\mathfrak{a} \to \mathfrak{b}$ — гипотеза.
2. $\neg\mathfrak{a} \to \mathfrak{b}$ — гипотеза.
3. $(\mathfrak{a} \to \mathfrak{b}) \to (\neg\mathfrak{b} \to \neg\mathfrak{a})$ — Лемма 2.3.1 b).
4. $\neg\mathfrak{b} \to \neg\mathfrak{a}$ — MP 1, 3.
5. $(\neg\mathfrak{a} \to \mathfrak{b}) \to (\neg\mathfrak{b} \to \neg\neg\mathfrak{a})$ — Лемма 2.3.1 b).
6. $\neg\mathfrak{b} \to \neg\neg\mathfrak{a}$ — MP 2, 5.
7. $(\neg\mathfrak{b} \to \neg\neg\mathfrak{a}) \to ((\neg\mathfrak{b} \to \neg\mathfrak{a}) \to \mathfrak{b})$ — Аксиома 3.
8. $(\neg\mathfrak{b} \to \neg\mathfrak{a}) \to \mathfrak{b}$ — MP 6, 7.
9. $\mathfrak{b}$ — MP 4, 8.

Имеем $\mathfrak{a} \to \mathfrak{b}, \neg\mathfrak{a} \to \mathfrak{b} \vdash \mathfrak{b}$. Следовательно, по теореме дедукции $\mathfrak{a} \to \mathfrak{b} \vdash (\neg\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b}$. Еще раз применяя теорему дедукции получим $\vdash (\mathfrak{a} \to \mathfrak{b}) \to ((\neg\mathfrak{a} \to \mathfrak{b}) \to \mathfrak{b})$. ■

2.6. Теорема о выводимости. Пусть $\mathfrak{a} = \mathfrak{a}(B_1, \ldots, B_k)$ — формула от $B_1, \ldots, B_k$ высказывательных переменных. α — некоторая логическая возможность формулы $\mathfrak{a}$. Положим:

$$B_i' = \begin{cases} B_i, & \text{если } B_i = 1 \text{ в логической возможности } \alpha, \\ \neg B_i, & \text{если } B_i = 0 \text{ в логической возможности } \alpha. \end{cases}$$

$$\mathfrak{a}' = \begin{cases} \mathfrak{a}, & \text{если } \mathfrak{a} = 1 \text{ в логической возможности } \alpha, \\ \neg\mathfrak{a}, & \text{если } \mathfrak{a} = 0 \text{ в логической возможности } \alpha. \end{cases}$$

Теорема 1. $B_1', B_2', \ldots, B_k' \vdash \mathfrak{a}'$.

Прежде, чем приступить к доказательству теоремы, проиллюстрируем ее смысл на примере. Пусть $\mathfrak{a}(A, B) = A \to (B \to \neg A)$. Составим таблицу истинности этой формулы.

A	B	$B \to \neg A$	$A \to (B \to \neg A)$
1	1	0	0
1	0	1	1
0	1	1	1
0	0	1	1

Рассмотрим первую строку этой таблицы истинности. Очевидно, что

$$A' = A,\ B' = B,\ \mathfrak{a}'(A, B) = \neg(A \to (B \to \neg A)).$$

Теорема утверждает, что для этой логической возможности справедлива выводимость:

$$A', B' \vdash \mathfrak{a}'(A, B),$$

то есть

$$A, B \vdash \neg(A \to (B \to \neg A)).$$

Аналогично, для второй, третьей и четвертой строк соответствующие выводимости имеют вид:

$$A, \neg B \vdash A \to (B \to \neg A),$$
$$\neg A,\ \ B \vdash A \to (B \to \neg A),$$
$$\neg A, \neg B \vdash A \to (B \to \neg A).$$

Теперь приступим к доказательству теоремы.

Доказательство. Индукция по количеству n логических связок в $\mathfrak{a}$.

$n = 0$. Тогда формула $\mathfrak{a}$ есть буква B_1. Так как $\mathfrak{a} = B_1$, то при $B_1 = 1$ и $\mathfrak{a} = 1$. Следовательно $B_1' = B_1$, $\mathfrak{a}' = \mathfrak{a} = B_1$. Очевидно, что $B_1 \vdash B_1 = \mathfrak{a}$. При $B_1 = 0$ и $\mathfrak{a} = 0$. Следовательно $B_1' = \neg B_1$, $\mathfrak{a}' = \neg\mathfrak{a} = \neg B_1$. Также очевидно, что $\neg B_1 \vdash \neg B_1$.

Предположим теперь, что теорема верна для любого j, $0 \le j < n$, а формула $\mathfrak{a}$ содержит n связок. Так как $n \ge 1$, то формула $\mathfrak{a}$ может иметь один из двух видов (см. определение формулы):

1. $\mathfrak{a} = \neg\mathfrak{b}$ для некоторой формулы $\mathfrak{b}$.

2. $\mathfrak{a} = (\mathfrak{b} \to \mathfrak{c})$ для некоторых формул $\mathfrak{b}$ и $\mathfrak{c}$.

Рассмотрим каждый из этих случаев в отдельности.

1. $\mathfrak{a} = \neg\mathfrak{b}$. Для формулы $\mathfrak{b}$ утверждение теоремы верно, так как $\mathfrak{b}$ содержит $(n-1)$ связок.

1а. $\mathfrak{b} = 1$. Следовательно, $\mathfrak{a} = 0$, тогда $\mathfrak{b}' = \mathfrak{b}$, $\mathfrak{a}' = \neg\mathfrak{a} = \neg\neg\mathfrak{b}$. По индуктивному предположению

$$B_1', \ldots, B_k' \vdash \mathfrak{b}' = \mathfrak{b} \tag{1}$$

Но, по лемме 2.1.1 b), $\vdash (\mathfrak{b} \to \neg\neg\mathfrak{b})$. Следовательно

$$B_1', \ldots, B_k' \vdash \mathfrak{b} \to \neg\neg\mathfrak{b}. \tag{2}$$

Из (1) и (2) по МР получаем:

$$B'_1, \ldots, B'_k \vdash \neg\neg\mathfrak{b} = \mathfrak{a}'.$$

1b. $\mathfrak{b} = 0$. Следовательно, $\mathfrak{b}' = \neg\mathfrak{b}$, тогда $\mathfrak{a} = 1$ и $\mathfrak{a}' = \mathfrak{a} = \neg\mathfrak{b} = \mathfrak{b}'$. Так как $\mathfrak{a}' = \mathfrak{b}'$, а для $\mathfrak{b}'$ теорема верна, то она верна и для $\mathfrak{a}'$.

2. $\mathfrak{a} = (\mathfrak{b} \to \mathfrak{c})$. По индуктивному предположению

$$B'_1, B'_2, \ldots, B'_k \vdash \mathfrak{b}',$$
$$B'_1, B'_2, \ldots, B'_k \vdash \mathfrak{c}'$$

2a. $\mathfrak{b} = 0$. Следовательно, $\mathfrak{b}' = \neg\mathfrak{b}$, тогда $\mathfrak{a} = 1 \Rightarrow \mathfrak{a}' = \mathfrak{a} = (\mathfrak{b} \to \mathfrak{c})$. В этом случае имеем:

$$B'_1, \ldots, B'_k \vdash \mathfrak{b}' = \neg\mathfrak{b}. \tag{3}$$

По лемме 2.2.1 имеем:

$$\vdash \neg\mathfrak{b} \to (\mathfrak{b} \to \mathfrak{c}) \tag{4}$$

Из (3) и (4) по MP получим:

$$B'_1, \ldots, B'_k \vdash (\mathfrak{b} \to \mathfrak{c}) = \mathfrak{a}'$$

2b. $\mathfrak{c} = 1$. Следовательно, $\mathfrak{c}' = \mathfrak{c}$, тогда $\mathfrak{a}' = \mathfrak{a} = (\mathfrak{b} \to \mathfrak{c})$. Имеем:

$$B'_1, \ldots, B'_k \vdash \mathfrak{c}' = \mathfrak{c}. \tag{5}$$

Запишем одну из аксиом 1:

$$\vdash \mathfrak{c} \to (\mathfrak{b} \to \mathfrak{c}) \tag{6}$$

Из (5) и (6) по MP имеем:

$$B'_1, \ldots, B'_k \vdash (\mathfrak{b} \to \mathfrak{c}) = \mathfrak{a}'$$

2c. $\mathfrak{b} = 1$, $\mathfrak{c} = 0$. Следовательно, $\mathfrak{a} = 0$ и $\mathfrak{b}' = \mathfrak{b}$, $\mathfrak{c}' = \neg\mathfrak{c}$, $\mathfrak{a}' = \neg\mathfrak{a} = \neg(\mathfrak{b} \to \mathfrak{c})$.
По индуктивному предположению

$$B'_1, \ldots, B'_k \vdash \mathfrak{b}' = \mathfrak{b}, \tag{7}$$

$$B'_1, \ldots, B'_k \vdash \mathfrak{c}' = \neg\mathfrak{c}. \tag{8}$$

По лемме 2.4.1 имеем

$$\vdash \mathfrak{b} \to (\neg\mathfrak{c} \to \neg(\mathfrak{b} \to \mathfrak{c})) \tag{9}$$

Применяя правило MP вначале к (7) и (9), а затем к (8) и полученной формуле, получим:

$$B'_1, B'_2, \ldots, B'_k \vdash \neg(\mathfrak{b} \to \mathfrak{c}) = \mathfrak{a}' \ \blacksquare.$$

Отметим, что в данной теореме и предыдущих леммах доказательство выводимости тех или иных формул проводилось не всегда (чаще всего) предъявлением вывода в полном смысле этого слова, так как по определению вывода, в нем не могут участвовать дополнительные правила вывода (ПС и ПИПП в нашем случае), а равно и никакие иные вспомогательные средства (теорема дедукции, например, в нашем случае). Однако, из доказательства теоремы дедукции и дополнительных правил вывода следует, что те части, где они применяются, в принципе могут быть заменены на соответствующие части вывода, быть может, и достаточно длинные.

2.7. Новые термины. Закон двойного отрицания. Закон противоречивой посылки. Законы контрапозиции. Первое правило отрицания импликации. Обобщенное правило противоречивой посылки. Теорема о выводимости.

2.8. Контрольные вопросы.

1. Перечислите все леммы данного параграфа под их "именами", приведенных в названиях пунктов.
2. Перечислите все леммы, используемые в доказательстве теоремы о выводимости. Какие из доказанных лемм не используются в доказательстве теоремы о выводимости?
3. Для формулы $\mathfrak{a}(A) = A$ перечислите все выводимости, которые имеют место в соответствии с теоремой о выводимости.
4. То же самое задание, что и предыдущее, для формулы $\mathfrak{a}(A) = \neg A$.

2.9. Упражнения.

1. Воспроизведите по памяти доказательство каждой из лемм данного параграфа.
2. Для формулы $\mathfrak{a}(A, B) = A \to \neg(A \to B)$ перечислите все выводимости, которые имеют место в соответствии с теоремой о выводимости.
3. То же самое задание, что и предыдущее, для формулы $\mathfrak{a}(A, B, C) = A \to (B \to \neg C)$.
4. Докажите выводимость следующих формул:
   (a) $\neg(\mathfrak{a} \to \neg\mathfrak{b}) \to \mathfrak{a}$;
   (b) $\neg(\mathfrak{a} \to \neg\mathfrak{b}) \to \mathfrak{b}$;
   (c) $\mathfrak{a} \to (\mathfrak{b} \to \neg(\mathfrak{a} \to \neg\mathfrak{b}))$.

§ 3. Полнота, непротиворечивость и разрешимость ИВ Независимость аксиом ИВ

Полнота ИВ относительно АВ. Непротиворечивость ИВ. Разрешимость ИВ. Независимость схем аксиом ИВ. Многозначные логики.

3.1. Полнота ИВ относительно АВ.

Определение 1. *Пусть $\mathfrak{T}$ — некоторая содержательная аксиоматическая теория, $\mathfrak{T}'$ — ее формализация. Теория $\mathfrak{T}'$ называется полной относительно теории $\mathfrak{T}$, если выводимые формулы теории $\mathfrak{T}'$ и только они являются теоремами теории $\mathfrak{T}$.*

Теорема 1. *ИВ является полной теорией относительно АВ, то есть формула АВ является тавтологией тогда и только тогда, когда существует равносильная ей формула, выводимая в ИВ.*

Доказательство. 1. Ранее показано, что все аксиомы ИВ являются тавтологиями. Кроме того, легко показать, что применение правила MP к тавтологии дает в результате также тавтологию. Это и означает, что всякая формула, выводимая в ИВ является тавтологией в АВ.

2. Пусть $\mathfrak{c}$ — тавтология АВ. Так как система связок $\{\neg, \to\}$ является полной, то любую формулу АВ равносильными преобразованиями можно привести к формуле, содержащей в качестве логических связок лишь $\{\neg, \to\}$. Поэтому

$$\mathfrak{c} \equiv \mathfrak{a},$$

где $\mathfrak{a}$ — формула от связок $\{\neg, \to\}$ и потому $\mathfrak{a}$ — формула ИВ.

Пусть $\mathfrak{a} = \mathfrak{a}(B_1, B_2, \ldots, B_k)$. По теореме о выводимости

$$B'_1, B'_2, \ldots, B'_k \vdash \mathfrak{a}'.$$

так как $\mathfrak{a}$ — тавтология, то в любой логической возможности $\mathfrak{a}' = \mathfrak{a}$, то есть

$$B'_1, B'_2, \ldots, B'_k \vdash \mathfrak{a}. \tag{1}$$

При $B_k = 1$ получаем

$$B'_1, \ldots, B'_{k-1}, B_k \vdash \mathfrak{a}, \tag{2}$$

а при $B_k = 0$ получаем

$$B'_1, \ldots, B'_{k-1}, \neg B_k \vdash \mathfrak{a}. \tag{3}$$

Применяя теорему дедукции к (2) и (3), получаем:

$$B'_1, \ldots, B'_{k-1} \vdash (B_k \to \mathfrak{a}) \tag{4}$$

$$B'_1, \ldots, B'_{k-1} \vdash (\neg B_k \to \mathfrak{a}) \tag{5}$$

По лемме 2.5.1 имеем:

$$\vdash (B_k \to \mathfrak{a}) \to ((\neg B_k \to \mathfrak{a}) \to \mathfrak{a}) \tag{6}$$

Применяя MP к (4), (6), а затем к (5) и полученной формуле, получим, что

$$B'_1, \ldots, B'_{k-1} \vdash \mathfrak{a}. \tag{7}$$

Сравнивая (7) с (1) замечаем, что B'_k можно просто удалить из посылки без ущерба для истинности выводимости. Но тоже самое можно сделать и с B'_{k-1}, затем с B'_{k-2} и т. д. В конце концов мы придем к следующей выводимости: $\vdash \mathfrak{a}$. ■

3.2. Непротиворечивость ИВ.

Определение 1. *Теория $\mathfrak{T}$, содержащая ИВ в качестве подтеории, называется противоречивой, если для некоторой формулы $\mathfrak{a}$ этой теории выполняется:*

$$\vdash \mathfrak{a} \text{ и } \vdash \neg\mathfrak{a}.$$

В противном случае теория $\mathfrak{T}$ называется непротиворечивой.

Теорема 1. *ИВ является непротиворечивой теорией.*

Доказательство. Пусть для некоторой формулы $\mathfrak{a}$ выполняются выводимости: $\vdash \mathfrak{a}$ и $\vdash \neg\mathfrak{a}$. Если $\mathfrak{b}$ — произвольная формула ИВ, то имеем:

$$\vdash \mathfrak{a} \tag{8}$$

$$\vdash \neg\mathfrak{a} \tag{9}$$

$$\vdash \mathfrak{a} \to (\neg\mathfrak{a} \to \mathfrak{b}) \text{ — лемма 2.2.1} \tag{10}$$

Применяя MP к (8) и (10), а затем к (9) и полученной формуле, получим: $\vdash \mathfrak{b}$, то есть мы получили, что всякая формула ИВ выводима. По теореме о полноте это означает, что всякая формула ИВ является тавтологией, но это не так. ■

Из доказательства этой теоремы видно, что в противоречивой теории любая формула является выводимой. Это значит, что противоречивые теории не имеют права на существование в математике, так как никакой содержательной информации не несут.

3.3. Разрешимость ИВ.

Определение 1. *Формальная аксиоматическая теория $\mathfrak{T}$ называется разрешимой, если существует алгоритм, позволяющий для каждой формулы установить, является она выводимой или нет.*

Теорема 1. *ИВ — разрешимая теория.*

Доказательство. Пусть $\mathfrak{a}$ — формула. Составив таблицу истинности (конечная процедура) можно установить, является она тавтологией или нет. По теореме о полноте заключаем, что если $\mathfrak{a}$ — тавтология, то она выводима. Если же $\mathfrak{a}$ не тавтология, то она не выводима. ■

3.4. Независимость системы аксиом ИВ.

Определение 1. *Пусть Σ — система аксиом некоторой теории $\mathfrak{T}$, $\alpha \in \Sigma$. Аксиома α называется независимой, если она не выводима из $\Sigma\backslash\{\alpha\}$. Система аксиом Σ называется независимой, если все аксиомы этой системы независимы.*

Теорема 1. *Каждая из схем аксиом ИВ независима.*

Доказательство. *Независимость Аксиомы 1.* Будем считать, что буквы ИВ могут принимать 3 значения: 0, 1, 2. Определим связки $\neg$ и $\to$ следующими таблицами.

A	$\neg A$
0	1
1	1
2	0

A	B	$A \to B$
0	0	0
0	1	2
0	2	2
1	0	2
1	1	2
1	2	0
2	0	0
2	1	0
2	2	0

Назовем формулу *привилегированной*, если в любой своей логической возможности она принимает значение, равное 0.

Можно убедиться в том, что всякая аксиома, получающаяся по схеме аксиом 2, 3 является привилегированной формулой. Это чисто техническая проверка. Также легко убедиться в том, что применение правила MP к привилегированным формулам дает формулу привилегированную. Это означает, что если бы схема аксиом 1 была выводима из схем аксиом 2, 3, то схема аксиом 1 была бы тоже привилегированной. Но $A \to (B \to A)$ не является привилегированной, так как при $A = 0$, $B = 1$ она принимает значение, равное 2. Таким образом, схема аксиом 1 независима от двух других схем.

Независимость Аксиомы 2. Как и выше будем считать, что буквы ИВ могут принимать три значения: 0, 1, 2. Связки $\neg$, $\to$ определим таблицами.

A	$\neg A$
0	1
1	0
2	1

A	B	$A \to B$
0	0	0
0	1	2
0	2	1
1	0	0
1	1	2
1	2	0
2	0	0
2	1	0
2	2	0

Назовем формулу *особенной*, если в любой своей логической возможности она принимает значение, равное 0.

Несложно убедиться в том, что всякая аксиома, получающаяся из схем аксиом 1, 3 является особенной. И, кроме того, применение правила MP к особенным формулам дает формулу особенную.

Если бы схема аксиом 2 была выводима из схем аксиом 1, 3, то схема аксиом 2 была бы тоже особенной. Однако, например, аксиома

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$$

при $A = 0$, $B = 0$, $C = 1$ принимает значение, равное 2.

Независимость Аксиомы 3. Пусть $\mathfrak{a}$ — произвольная формула ИВ. $h(\mathfrak{a})$ — формула, полученная из $\mathfrak{a}$ удалением всех связок отрицания.

Очевидно, что если $\mathfrak{a}$ — аксиома 1 или 2, то $h(\mathfrak{a})$ — тавтология. Пусть $h(\mathfrak{a})$ и $h(\mathfrak{a} \to \mathfrak{b})$ — тавтологии, то есть $h(\mathfrak{a})$ и $h(\mathfrak{a}) \to h(\mathfrak{b})$ — тавтологии. Тогда и $h(\mathfrak{b})$ — тавтология. Таким образом, применение правила MP к формулам, значение оператора h на которых — тавтологии, дает формулу, значение оператора h на которой — тавтология. Тогда значение оператора h на всякой формуле, выводимой из аксиомы 1, 2, есть тавтология. Но для аксиомы 3

$$(\neg A \to \neg A) \to ((\neg A \to A) \to A)$$

значение оператора h равно :

$$(A \to A) \to ((A \to A) \to A).$$

Но эта формула не является тавтологией, так как при $A = 0$ она принимает значение, равное 0. Следовательно, схема аксиомы 3 не выводима из схем аксиом 1, 2. ■

3.5. Многозначные логики. Обобщение идеи, использованной для доказательства независимости аксиом исчисления высказываний приводит к понятию многозначной логики. В многозначных логиках высказывательные (или *пропозициональные*) переменные и формулы принимают более двух различных значений. Если число различных значений конечно, то такие логики называются конечнозначными или k-значными, в противном случае многозначные логики называются бесконечнозначными.

3.6. k-значные логики. Назовем числа $0, 1, \ldots, k-1$ "истинностными значениями" и выберем какое-нибудь число m с условием $1 \leq m \leq k-1$. Числа $0, 1, \ldots, m$ будем называть *выделенными истинностными значениями.* Возьмем некоторое конечное число "истинностных таблиц", представляющих функции, отображающие множество $\{0, 1, \ldots, k-1\}$ в себя. Для каждой таблицы введем знак, который будем называть соответствующей этой таблице логической связкой. С помощью этих связок и пропозициональных букв мы можем строить формулы. Каждая такая формула определяет некоторую "истинностную функцию", отображающую множество $\{0, 1, \ldots, k-1\}$ в себя. Формула, принимающие только выделенные значения, называется *выделенной.* Говорят, что числа k, m и основные истинностные таблицы определяют некоторую k-значную логику M.

Пример 1. Алгебра высказываний является 2-значной логикой, соответствующей случаю $k = 2$, $m = 0$ и истинностными таблицами для связок $\neg$, $\&$, $\vee$, $\to$, $\sim$, которые вводятся аналогично таблицам главы III с заменой символа 0 на 1 и наоборот. Выделенные формулы этой логики назывались тавтологиями.

Пример 2. Две различные 3-значные логики, соответствующие случаю $k = 3$, $m = 0$ и введенными истинностными таблицами для связок $\neg$, $\to$ (см. п. V.3.4.). Эти логики использовались для доказательства независимости схем аксиом A1 и A2 исчисления высказываний.

Для многозначных логик так же как и для алгебры высказываний можно определить понятия логической возможности, совместной логической возможности, равносильности формул и т. д.

Легко понять, что каждая таблица истинности от n пропозициональных букв определяет бесконечно много равносильных формул k-значной логики M. Таким образом, количество всевозможных таких таблиц истинности равно числу всех попарно неравносильных формул логики M от n букв.

Обозначим через P_k множество всех попарно неравносильных формул логики M от n пропозициональных букв $A_1, A_2, \ldots, A_n$. Так как число различных наборов $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ значений букв $A_1, A_2, \ldots, A_n$ равно k^n, то имеем следующий результат

Теорема 1. *Число формул логики M, зависящих от n букв в P_k равно k^{k^n}.*

Определение 1. *Формальная аксиоматическая теория, содержащая пропозициональные буквы и связки k-значной логики M называется подходящей для логики M, если множество теорем этой теории совпадает с множеством выделенных формул логики M.*

Очевидно, что все эти понятия могут быть обобщены на случай бесконечного множества истинностных значений.

Пример 3. Пусть M' — 2-значная логика полученная из алгебры высказываний M заменой всех формул в M на равносильные им формулы, содержащие в качестве логических связок только $\neg$ и $\to$, для которых в таблицах истинности 0 заменен на 1 и наоборот. Тогда исчисление высказываний будет подходящей формальной аксиоматической теорией для M', так как, в силу теорем о полноте (см. п. V.3.1.), множество всех теорем исчисления высказываний совпадает с множеством всех выделенных формул (тавтологий) логики M'.

3.7. Новые термины. Полнота формализации $\mathfrak{T}'$ теории $\mathfrak{T}$ относительно $\mathfrak{T}$. Непротиворечивость и разрешимость формальных аксиоматических теорий. Независимость аксиомы от других аксиом. Независимость системы аксиом. Многозначные логики.

3.8. Контрольные вопросы.

1. Дайте определение полной формальной аксиоматической теории $\mathfrak{T}'$ относительно содержательной теории $\mathfrak{T}$. Каково предполагаемое в определении соотношение между теориями $\mathfrak{T}$ и $\mathfrak{T}'$?

2. Какие формулы АВ в теореме 3.1.1 считаются теоремами ИВ?

3. Дайте определение противоречивой и непротиворечивой аксиоматической теории.

4. Дайте определение независимой аксиомы в некоторой системе аксиом и определение независимой системы аксиом.

5. Поясните в общих чертах идею доказательства теоремы о независимости схем аксиом ИВ.

6. Существует ли k-значная логика в которой все формулы являются выделенными?

7. Дайте определение логической возможности, совместной логической возможности и равносильности k-значной логики.

8. Дайте определение формулы k-значной логики, содержащей две — "$*$" и "$\circ$" унарные, а также две — "$\cong$" и "$\leftrightarrow$" бинарные логические связки.

3.9. Упражнения.

1. Докажите, что в противоречивой теории всякая формула является теоремой.

2. Доказать независимость схемы аксиомы 3 построением таблиц для связок $\neg, \to$.

3. Докажите, что если схему аксиом 3 в ИВ заменить схемой аксиом $(\neg \mathfrak{b} \to \neg \mathfrak{a}) \to (\mathfrak{a} \to \mathfrak{b})$, то класс теорем ИВ от этого не изменится.

4. Пусть в 3-х значной логике с логическими связками $\neg$ и $\to$, определяемыми таблицами

A	$\neg A$
0	1
1	0
2	1

A	B	$A \to B$
0	0	0
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	1
1	2	0
2	2	0

а выделенными являются формулы, которые принимают только значение 0. Являются ли выделенными формулы:

(a) $A \to (B \to A)$;

(b) $A \to (\neg A \to B)$;

(c) $(A \to B) \to (\neg B \to \neg A)$.

5. Докажите, что для любой k-значной логики M существует подходящая формальная аксиоматическая теория.

Глава VI

Алгебра предикатов

§ 1. Понятие предиката. Операции над предикатами

Высказывательные формы. Определение предиката. Логические возможности и таблицы истинности предиката. Способы задания предикатов. Предикатные переменные. Общие логические возможности двух предикатов. Операции над предикатами. Кванторные операции над предикатами.

1.1. Высказывательные формы.

Определение 1. *Пусть $\mathfrak{M}$ — некоторое множество, n — неотрицательное целое число.*

1. $n = 0$. 0-местной высказывательной формой на множестве $\mathfrak{M}$ называется всякое высказывание об элементах этого множества.

2. $n > 0$. n-местной высказывательной формой на множестве $\mathfrak{M}$ называется всякое высказывание с n переменными об элементах множества $\mathfrak{M}$.

Пример 1. "Всякое вещественное число, большее 1, является корнем уравнения $x^2 = 2$" — ложное высказывание об элементах множества R, 0-местная высказывательная форма на R.

Пример 2. "Вещественное число x, возведенное в квадрат, дает число 2" — одноместная высказывательная форма.

Пример 3. 3. "$x^2 + y^2 = z^2$" —это высказывательная форма от трех переменных, которую можно рассматривать на R, но можно рассматривать и на любом числовом множестве.

Отметим, что при подстановке в высказывательную форму на множестве $\mathfrak{M}$ вместо переменных конкретных элементов множества, эта высказывательная форма обращается в конкретное высказывание, принимающее значение 0 или 1. Таким образом всякая n-местная высказывательная форма определяет некоторую функцию от n переменных, заданную на множестве $\mathfrak{M}$ со значениями во множестве $\{0, 1\}$.

Обозначим через A, $P(x)$ и $Q(x, y, z)$ функции, определяемые высказывательными формами из примеров 1.1.1, 1.1.2 и 1.1.3 соответственно. Тогда можно утверждать, например, что $A = 0$, $P(1) = 0$, $P(17) = 0$, $P(\sqrt{2}) = 1$, $P(-\sqrt{2}) = 1$, $Q(1, 1, 1) = 0$, $Q(3, 4, 5) = 1$, $Q(4, 3, 5) = 1$, $Q(5, 3, 4) = 0$ и т. д.

В дальнейшем, в действительности, мы будем изучать n-местные функции, заданные на множествах со значениями во множестве $\{0, 1\}$, а высказывательные формы будут рассматриваться нами лишь как один из способов задания этих функций.

1.2. Определение предиката.

Определение 1. *Пусть $\mathfrak{M}$ — некоторое множество, n — неотрицательное целое число.*

1. $n = 0$. 0-местным предикатом на множестве $\mathfrak{M}$ называется всякое конкретное высказывание A об элементах множества $\mathfrak{M}$.

2. $n > 0$. n-местным предикатом на множестве $\mathfrak{M}$ называется всякая функция P от n переменных, заданная на множестве $\mathfrak{M}$ со значениями во множестве $\{0, 1\}$. Обозначается $P(x_1, \ldots, x_n)$. При этом переменные $x_1, \ldots, x_n$, участвующие в записи предиката P, называются предметными переменными.

Пример 1. $\mathfrak{M}$ — любое фиксированное множество.

$$P(x,y) = \begin{cases} 1, & \text{если } x = y, \\ 0, & \text{если } x \neq y. \end{cases}$$

Пример 2. Пусть $\mathfrak{M} = R$.

$$Q(x,y) = \begin{cases} 1, & \text{если } x \leq y, \\ 0, & \text{если } x > y. \end{cases}$$

Очевидно, например, что $Q(1,2) = 1$, $Q(2,1) = 0$.

Пример 3. Пусть $\mathfrak{M} = R$.

$$S(x) = \begin{cases} 1, & \text{если } x^2 - 5x + 6 = 0, \\ 0, & \text{если } x^2 - 5x + 6 \neq 0. \end{cases}$$

Понятно, что $S(2) = S(3) = 1$, а для всякого числа $a \notin \{2,3\}$, $S(a) = 0$.

Отметим, что если $P(x_1, \ldots, x_n)$ есть некоторый предикат, заданный на множестве $\mathfrak{M}$, $n \geq 1$, то подставив в него вместо какой-либо предметной переменной конкретный элемент множества $\mathfrak{M}$, получим $(n-1)$-местный предикат. Так, например, в предыдущих примерах имеем:

$$P(x,\pi) = \begin{cases} 1, & \text{если } x = \pi, \\ 0, & \text{если } x \neq \pi. \end{cases}$$

— одноместный предикат;

$$Q(x,0) = \begin{cases} 1, & \text{если } x \leq 0, \\ 0, & \text{если } x > 0. \end{cases}$$

— одноместный предикат, а $Q(1,0)$ — ложное высказывание (0-местный предикат), $Q(0,0)$ — истинное высказывание.

1.3. Логические возможности и таблица истинности предиката. Пусть $\mathfrak{M}$ есть некоторое множество, а $P(x_1, \ldots, x_n)$ — n-местный предикат на этом множестве. Всякая последовательность $a_1, \ldots, a_n$ элементов из $\mathfrak{M}$, обращающая предикат $P(x_1, \ldots, x_n)$ в конкретное высказывание, называется *логической возможностью* предиката $P(x_1, \ldots, x_n)$ на множестве $\mathfrak{M}$.

Перечень всех логических возможностей предиката $P(x_1, \ldots, x_n)$ на множестве $\mathfrak{M}$ с указанием значений этого предиката в каждой логической возможности, помещенные в таблицу, называется *таблицей истинности* предиката $P(x_1, \ldots, x_n)$ на множестве $\mathfrak{M}$. Понятно, что о таблице истинности имеет смысл говорить лишь в случае, если $\mathfrak{M}$ — конечное множество.

Пример 1. Пусть $\mathfrak{M} = \{2,4\}$, а $P(x,y,z) =$ "$x + y = z$". Составим таблицу истинности предиката $P(x,y,z)$ на множестве $\mathfrak{M}$.

x	y	z	$P(x,y,z)$
2	2	2	0
2	2	4	1
2	4	2	0
2	4	4	0
4	2	2	0
4	2	4	0
4	4	2	0
4	4	4	0

1.4. Способы задания предикатов. Так как всякий предикат является функцией, то и все способы задания функций применимы и к предикатам. Наиболее употребительным способом задания предиката является задание его при помощи высказывательной формы, см. примеры 1.1.1–1.1.3. Этот способ, в сущности, можно назвать словесным способом.

Можно задавать предикаты табличным способом (таблицей истинности, см. пример 1.3.1), но практически это возможно лишь при весьма малых n и малом количестве элементов множества $\mathfrak{M}$.

1.5. Предикатные переменные. Подобно тому, как в школьной математике рассматривались конкретные числа и числа неизвестные или переменные, обозначенные той или иной буквой, так и здесь всякое выражение вида $P(x_1, \ldots, x_n)$ будем рассматривать как некоторый переменный предикат или предикатную переменную, которая может принимать значения из множества всевозможных предикатов, заданных на том или ином множестве, если, разумеется, не сказано в контексте, что $P(x_1, \ldots, x_n)$ обозначает какой-то конкретный предикат на конкретном множестве. Предикатным переменным можно придавать значения конкретных предикатов на тех или иных множествах.

1.6. Общие логические возможности двух предикатов.

Определение 1. *Пусть $P(x_1, \ldots, x_n)$ и $Q(y_1, \ldots, y_m)$ — два предиката, заданные на множестве $\mathfrak{M}$. Всякий набор $(a_1, \ldots, a_n; b_1, \ldots, b_m)$ значений из $\mathfrak{M}$. для предметных переменных $x_1, \ldots, x_n; y_1, \ldots, y_m$ называется общей логической возможностью для предикатов P и Q, если при этом всякая предметная переменная, одновременно входящая в запись предикатов P и Q, принимает одно и то же значение в P и Q.*

Пример 1. Пусть $P(x, y)$ и $Q(y, z)$ некоторые предикаты, заданные на множестве натуральных чисел. Набор чисел $(1, 2; 3, 4)$ не является общей логической возможностью для предикатов P и Q, так как в $P(x, y)$ предметная переменная y принимает значение $y = 2$, а в $Q(y, z)$ y принимает значение $y = 3$. Набор чисел $(1, 2; 2, 3)$ является общей логической возможностью для предикатов P и Q.

1.7. Операции $\neg$, $\&$, $\vee$, $\to$, $\sim$. Пусть $P(x_1, \ldots, x_n)$ и $Q(y_1, \ldots, y_m)$ — некоторые предикаты на некотором множестве $\mathfrak{M}$.

$$\neg P(x_1, \ldots, x_n),$$
$$P(x_1, \ldots, x_n) \,\&\, Q(y_1, \ldots, y_m),$$
$$P(x_1, \ldots, x_n) \vee Q(y_1, \ldots, y_m),$$
$$P(x_1, \ldots, x_n) \to Q(y_1, \ldots, y_m),$$
$$P(x_1, \ldots, x_n) \sim Q(y_1, \ldots, y_m)$$

есть предикаты на $\mathfrak{M}$, значения которых в каждой общей логической возможности $(a_1, \ldots, a_n; b_1, \ldots, b_m)$ определяется следующими ниже таблицами

$P(a_1, \ldots, a_n)$	$\neg P(a_1, \ldots, a_n)$
1	0
0	1

$P(a_1, \ldots, a_n)$	$Q(b_1, \ldots, b_m)$	$P(a_1, \ldots, a_n) \,\&\, Q(b_1, \ldots, b_m)$
1	1	1
1	0	0
0	1	0
0	0	0

$P(a_1,\ldots,a_n)$	$Q(b_1,\ldots,b_m)$	$P(a_1,\ldots,a_n)\vee Q(b_1,\ldots,b_m)$
1	1	1
1	0	1
0	1	1
0	0	0

$P(a_1,\ldots,a_n)$	$Q(b_1,\ldots,b_m)$	$P(a_1,\ldots,a_n)\to Q(b_1,\ldots,b_m)$
1	1	1
1	0	0
0	1	1
0	0	1

$P(a_1,\ldots,a_n)$	$Q(b_1,\ldots,b_m)$	$P(a_1,\ldots,a_n)\sim Q(b_1,\ldots,b_m)$
1	1	1
1	0	0
0	1	0
0	0	1

Таким образом, определенные выше операции над предикатами являются естественным обобщением соответствующих операций над 0-местными предикатами (высказываниями) на предикаты от произвольного числа переменных.

1.8. Кванторные операции над предикатами. Определим вначале кванторные операции для одноместных предикатов.

Пусть $P(x)$ — некоторый одноместный предикат на множестве $\mathfrak{M}$. Выражениями $\forall x\,P(x)$ и $\exists x\,P(x)$ обозначим высказывания (0-местные предикаты), истинностные значения которых определяются следующим образом.

1. $\forall x\,P(x)=1 \iff$ когда для любого элемента $a\in\mathfrak{M}$ выполняется $P(a)=1$.

2. $\exists x\,P(x)=1 \iff$ когда существует хотя бы один элемент $a\in\mathfrak{M}$ такой, что $P(a)=1$.

Символы $\forall$ и $\exists$ называются *кванторами* соответственно *общности* и *существования*, а соответствующие операции, определенные выше — *кванторными операциями*. Читается: $\forall x\,P(x)$ — "для любого x пэ от x"; $\exists x\,P(x)$— "существует x пэ от x". $P(x)$ называется *областью действия* соответственных кванторов в высказываниях $\forall x\,P(x)$ и $\exists x\,P(x)$. Отметим, что присутствие переменной x в записи высказываний $\forall x\,P(x)$ и $\exists x\,P(x)$ не влияет на значения истинности этих высказываний. Она называется *связанной предметной переменной* в этих высказываниях.

Пусть теперь $P(x_1,\ldots,x_n)$ — некоторый n-местный предикат на множестве $\mathfrak{M}$, $n>1$. $(n-1)$-местный предикат, сопоставляющий всякой последовательности $(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)$ длины $(n-1)$ значение $\forall x_i\,P(a_1,\ldots,a_{i-1},x_i,a_{i+1},\ldots,a_n)$:

$$(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)\mapsto\forall x_i\,P(a_1,\ldots,a_{i-1},x_i,a_{i+1},\ldots,a_n),$$

обозначим через $\forall x_i\,P(x_1,\ldots,x_n)$, а $(n-1)$-предикат, сопоставляющий указанной выше последовательности значение $\exists x_i\,P(a_1,\ldots,a_{i-1},x_i,a_{i+1},\ldots,a_n)$:

$$(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)\mapsto\exists x_i\,P(a_1,\ldots,a_{i-1},x_i,a_{i+1},\ldots,a_n),$$

обозначим через $\exists x_i\,P(x_1,\ldots,x_n)$. $P(x_1,\ldots,x_n)$ в предикатах $\forall x_i\,P(x_1,\ldots,x_n)$ и $\exists x_i\,P(x_1,\ldots,x_n)$ называется областью действия соответствующих кванторов, а переменная x_i *называется связанной переменной.*

1.9. Новые термины. Высказывательная форма. Предикат. Предметные переменные. Предикатные переменные. Логические возможности предиката. Таблица истинности предиката. Общая логическая возможность двух предикатов. Кванторы общности и существования. Кванторные операции. Область действия квантора. Связанные вхождения предметных переменных.

1.10. Контрольные вопросы.

1. Приведите примеры n-местных высказывательных форм на множестве натуральных чисел N для $n = 0, 1, 2, 3$. Запишите функции (предикаты), которые они определяют.
2. Можно ли систему N линейных уравнений с m неизвестными считать высказывательной формой? Если да, то какова ее "местность"?
3. Всякое ли высказывание можно считать 0-местной высказывательной формой?
4. В трехместную высказывательную форму вместо двух неизвестных поставили конкретные значения. Какова "местность" полученной высказывательной формы?
5. В чем различие между высказывательными формами и предикатами?
6. Для примеров 1.2.1–1.2.2 найдите $P(1,1)$, $P(1,0)$, $P(0,0)$, $Q(1,1)$, $Q(7,1)$, $Q(1,7)$.
7. Укажите количество логических возможностей для некоторого предиката $A(x,y)$, заданного на 2-элементном множестве? На трехэлементном множестве? Задайте 2-х и 3-х элементные множества и составьте таблицу логических возможностей предиката $A(x,y)$.
8. Чем отличается предикат от предикатной переменной?
9. Запишите одноместный предикат на множестве N, область истинности которого состоит из всех нечетных чисел.
10. Пусть $P(x,y)$ и $Q(y,z)$ — некоторые предикаты на множестве N. Какие из следующих наборов чисел являются общей логической возможностью предикатов P и Q? $(7,2;2,7)$, $(6,2;1,3)$, $(1,3,3)$, $(8,1;2,8)$, $(3,4;4,1)$, $(2,1)$.
11. Пусть $P(x,y,z)$ и $Q(y,z,t)$ — некоторые предикаты на множестве N. Какие из следующих наборов чисел являются общей логической возможностью для предикатов P и Q: $(7,2,1;2,7,11)$, $(1,2,1;2,1,7)$, $(2,3,1,2)$, $(2,1;1,2)$, $(3,2,1;2,1,3)$, $(17,2,3;3,2,17)$.
12. Определите "местность" предикатов:
$P(x) \vee Q(x,y)$, $P(x)\ \&\ Q(y)$, $P(x,y,z) \to Q(x,t)$, $P(x,y,z) \sim Q(y)$, $\neg P(x,y,z)$.
13. Пусть $P(x) =$ "$x \vdots 1$", $Q(y) =$ "$1 \vdots y$" — предикаты, заданные на N. Определите истинность высказываний: $\exists x\, P(x)$, $\forall x\, P(x)$, $\exists y\, Q(y)$, $\forall y\, Q(y)$.
14. Пусть $P(x,y,z) =$ "$x(yz) = (xy)z$", $Q(x,y,z) =$ "$x - (y - z) = (x - y) - z$" — предикаты на Z. Определите истинность высказываний:
$$\forall x\, \forall y\, \forall z\, P(x,y,z),$$
$$\forall x\, \forall y\, \forall z\, Q(x,y,z),$$
$$\exists x\, \exists y\, \exists z\, Q(x,y,z),$$
$$\forall x\, \exists y\, \exists z\, Q(x,y,z),$$
$$\forall x\, \exists z\, \forall y\, Q(x,y,z).$$
15. Пусть $P(x,y,z) =$ "$x + y = z$". Определите истинность высказываний на N и на Z:
$$\forall x\, \forall z\, \exists y\, P(x,y,z),$$
$$\forall z\, \exists x\, \exists y\, P(x,y,z),$$
$$\forall x\, \forall y\, \exists z\, P(x,y,z).$$
16. Пусть $P(x,y) =$ "$x + y = y$". Определите истинность высказываний на N и на Z:
$$\exists y\, \forall x\, P(x,y),$$
$$\exists x\, \forall y\, P(x,y),$$
$$\forall y\, \exists x\, P(x,y).$$
17. В следующих ниже предикатах укажите связанные вхождения предметных переменных:
$\forall x\, P(x)$, $\exists x\, \forall y\, Q(x,y,z)$, $\forall x\, P(x,y) \to \exists y\, Q(x,y,z)$.

1.11. Упражнения.

1. Сколько n-местных предикатов можно задать на m-элементном множестве?
2. Подсчитайте количество логических возможностей n-местного предиката на m-элементном множестве.
3. Задайте таблицами истинности три различных 2-местных предиката на множестве $\{a, b, c\}$.
4. Задайте таблицами истинности три различных 3-местных предиката на множестве $\{0, 1\}$.
5. Следующие ниже высказывания о натуральных числах запишите в символической форме, вводя предикаты и используя кванторные операции. Определите истинность этих высказываний

   (a) Если какое-то утверждение, зависящее от натурального числа n истинно при $n = 1$ и из предположения истинности для какого-то числа следует истинность его для следующего числа, то такое утверждение истинно для любого натурального числа.

   (b) Для любых двух натуральных чисел найдется такое третье натуральное число, которое в сумме с первым больше второго.

   (c) Для любого натурального числа существует большее его натуральное число.

   (d) Существует натуральное число, большее всех других натуральных чисел.

   (e) Существует натуральное число, не превосходящее всех натуральных чисел.

   (f) Уравнение $a + x = b$ разрешимо в N.

   (g) Уравнение $a + x = b$ неразрешимо в N.

   (h) Уравнение $ax = b$ разрешимо в N.

§ 2. Язык алгебры предикатов. Классификация формул

Определение формулы. Интерпретации формул языка алгебры предикатов. Классификация формул. Модели.

2.1. Определение формулы.

Элементарными формулами называются:

1) большие буквы латинского алфавита, снабженные штрихами или индексами и обозначающие переменные или постоянные (конкретные) 0-местные предикаты, которые являются переменными или постоянными высказываниями;

2) выражения вида $P(x_1, \ldots, x_n)$, обозначающие *переменные* или *постоянные n-местные предикаты,* где n может быть любым натуральным числом; P — любой большой буквой латинского алфавита, снабженной штрихами или индексами и называемой *предикатной переменной;* $x_1, \ldots, x_n$ — любыми малыми буквами латинского алфавита, снабженными штрихами или индексами и обозначающими *предметные переменные* или *конкретные предметы* из некоторого множества.

Формулами называются:

1) элементарные формулы;

2) если $\mathfrak{a}$ и $\mathfrak{b}$ — формулы, то выражения:

$$\neg\mathfrak{a},\ (\mathfrak{a}\ \&\ \mathfrak{b}),\ (\mathfrak{a}\vee\mathfrak{b}),\ (\mathfrak{a}\to\mathfrak{b}),\ (\mathfrak{a}\sim\mathfrak{b})$$

также являются формулами;

3) если $\mathfrak{a}$ — формула, а x — буква, обозначающая предметную переменную, то выражения:

$$\forall x\,\mathfrak{a} \text{ и } \exists x\,\mathfrak{a}$$

также являются формулами.

4) Других формул, кроме тех, которые определены пунктами 1)–3), нет.

Подформула $\mathfrak{a}$ в формулах $\forall x\,\mathfrak{a}$ и $\exists x\,\mathfrak{a}$ *называется областью действия соответствующего квантора по* x. Всякое вхождение буквы x в область действия квантора по x называется *связанным вхождением* буквы x. Первое вхождение буквы x в формулы $\forall x\,\mathfrak{a}$ и $\exists x\,\mathfrak{b}$ считается также связанным вхождением.

Если же некоторое вхождение буквы x в какую-то формулу не находится в области действия квантора по x, то такое вхождение этой буквы называется *свободным вхождением* в данную формулу. Буква x, имеющая свободные вхождения в формулу $\mathfrak{b}$, называется *свободной предметной переменной* в формуле $\mathfrak{b}$. Если же буква x имеет лишь связанные вхождения в формулу $\mathfrak{b}$, то x называется *связанной предметной переменной* в формуле $\mathfrak{b}$.

Отметим, что если буква x не входит в формулу $\mathfrak{a}$, то формулы $\forall x\,\mathfrak{a}$ и $\exists x\,\mathfrak{a}$ имеют тот же содержательный смысл, что и формула $\mathfrak{a}$, так что в этом случае все эти три формулы будем отождествлять.

Совокупность всевозможных формул, определенных выше, будем называть *языком алгебры предикатов.* Отметим, что среди формул языка алгебры предикатов есть все формулы алгебры высказываний, так что язык алгебры предикатов включает в себя язык алгебры высказываний. Не трудно заметить, что язык алгебры предикатов гораздо богаче языка алгебры высказываний.

2.2. Интерпретации языка алгебры предикатов. Пусть $\mathfrak{a}$ — формула и $\mathfrak{M}$ — некоторое множество. Если все конкретные предметы, участвующие в записи формулы $\mathfrak{a}$, принадлежат множеству $\mathfrak{M}$ и все конкретные предикаты, участвующие в записи формулы $\mathfrak{a}$ можно доопределить (или ограничить) до предикатов на множестве $\mathfrak{M}$, то $\mathfrak{M}$ называется *допустимым множеством* для формулы $\mathfrak{a}$. В противном случае множество $\mathfrak{M}$ называется *недопустимым множеством* для формулы $\mathfrak{a}$.

Пример 1. Рассмотрим формулу $\mathfrak{a} = \forall x\,\forall y\,\forall z\,(x = y\cdot z + 1)$, где 1 — натуральное число, а $+, \cdot$ — сложение и умножение натуральных чисел. Очевидно, что эту формулу можно рассматривать

на любом множестве чисел, содержащем 1. Таким образом, всякое числовое множество, содержащее 1, является допустимым для данной формулы $\mathfrak{a}$. Однако всякое множество матриц, например, уже не является для $\mathfrak{a}$ допустимым.

Отметим, что если в записи формулы $\mathfrak{a}$ не участвуют конкретные предметы каких-то множеств и конкретные предикаты, то всякое множество является допустимым для этой формулы $\mathfrak{a}$.

Пусть $\mathfrak{a}$ — некоторая формула, $\mathfrak{M}$ — некоторое множество, допустимое для $\mathfrak{a}$. Сопоставим каждому переменному предикату, входящему в запись формулы $\mathfrak{a}$, некоторый конкретный предикат на множестве $\mathfrak{a}$ от тех же предметных переменных. Полученная формула $\mathfrak{a}'$ уже не содержит предикатных переменных, а лишь, быть может, предметные переменные. Формула $\mathfrak{a}'$ называется *интерпретацией* формулы $\mathfrak{a}$ на множестве $\mathfrak{M}$, которое называется *областью интерпретации.*

Отметим, что если интерпретация $\mathfrak{a}'$ формулы $\mathfrak{a}$ не содержит свободных предметных переменных, то $\mathfrak{a}'$ представляет собой какое-то конкретное высказывание об элементах множества $\mathfrak{a}$, истинное или ложное. Если же $\mathfrak{a}'$ содержит свободные предметные переменные, то $\mathfrak{a}'$ представляет собой некоторый предикат, заданный на области интерпретации $\mathfrak{M}$.

Пример 2. Рассмотрим формулу

$$\mathfrak{a} = \forall x\,(P(x,y) \vee Q(x,y)).$$

Очевидно, что любое множество является допустимым для $\mathfrak{a}$, так как $\mathfrak{a}$ не содержит в своей записи конкретных предметов и конкретных предикатов.

1. Пусть N — множество всех натуральных чисел, $P(x,y) =$ "$x \vdots y$", $Q(x,y) =$ "$x < y$". Тогда интерпретация $\mathfrak{a}'$ примет вид

$$\mathfrak{a}' = \forall x\,((x \vdots y) \vee (x < y)).$$

Очевидно, что $\mathfrak{a}' = \mathfrak{a}'(y)$ представляет собой одноместный предикат от переменной y, которая является свободной в $\mathfrak{a}'$. Переменная x является связанной предметной переменной. Отметим, что $\mathfrak{a}'(1) = \forall x\,((x \vdots 1) \vee (x < 1))$ — истинное высказывание. С другой стороны $\mathfrak{a}'(2) = \forall x\,((x \vdots 2) \vee \vee (x < 2))$ — ложное высказывание.

2. Приведем еще одну интерпретацию формулы $\mathfrak{a}$. Пусть $\mathfrak{M}$ — множество учащихся некоторой школы, $P(x,y) =$ "x и y учатся в одном классе", $Q(x,y) =$ "x и y посещают одну и ту же спортивную секцию". Тогда интерпретация $\mathfrak{a}'$ примет вид:

$$\mathfrak{a}' = \forall x\,(x \text{ и } y \text{ в одном классе или } x \text{ и } y \text{ посещают общую секцию}).$$

Легко понять, что если рассматриваемая школа достаточно велика, то интерпретация $\mathfrak{a}' = \mathfrak{a}'(y)$ ложна для любого значения y, так как, по-видимому, для любого ученика x найдется такой ученик y, что x и y в разных классах и общей секции не посещают.

2.3. Классификация формул. Модели. Пусть $\mathfrak{a}$ — некоторая формула, а $\mathfrak{a}'$ — ее интерпретация на некотором множестве $\mathfrak{M}$. (Отметим, что вообще говоря, на одном и том же множестве может существовать более одной интерпретации. Более того, как правило, их существует достаточно много.) Так как $\mathfrak{a}'$ есть некоторый предикат на $\mathfrak{M}$, то для $\mathfrak{a}'$ определены все те понятия, которые определены для предикатов, в частности понятие логической возможности, см. п. VI.1.3.

Формула $\mathfrak{a}$ называется *выполнимой в данной интерпретации* $\mathfrak{a}'$, если для $\mathfrak{a}'$ существует хотя бы одна логическая возможность на $\mathfrak{M}$, в которой $\mathfrak{a}' = 1$. В противном случае формула $\mathfrak{a}$ называется *ложной* или *невыполнимой в данной интерпретации.*

Формула $\mathfrak{a}$ называется *выполнимой,* если она выполнима хотя бы в одной интерпретации. В противном случае формула $\mathfrak{a}$ называется *ложной* или *противоречием.*

Формула $\mathfrak{a}$ называется *истинной в данной интерпретации* $\mathfrak{a}'$, если она истинна в любой логической возможности на $\mathfrak{M}$.

Формула $\mathfrak{a}$ называется *общезначимой*, если любое множество является допустимым для $\mathfrak{a}$ и $\mathfrak{a}$ истинна в любой интерпретации.

Множество $\mathfrak{M}$ называется *моделью для множества формул* Γ, если существует интерпретация формул из Γ на $\mathfrak{M}$, в которой все эти формулы истинны.

Отметим, что формула $\forall x\,(P(x) \vee \neg P(x))$ является общезначимой, а формула $\forall x\,(P(x)$ & & $\neg P(x))$ — ложной или противоречием.

Пример 1. Рассмотрим множество формул Γ:

$$\Gamma = \{\forall x\,P(x,x), (P(x,y)\ \&\ P(y,x)) \to (x=y), (P(x,y)\ \&\ P(y,z)) \to P(x,z)\}$$

и следующую интерпретацию этих формул на N. Пусть $P(x,y) =$ "$x \leq y$". Легко проверить, что в такой интерпретации все формулы из Γ истинны на N. Следовательно $\langle N, \leq\rangle$ является моделью системы формул Γ.

2.4. Новые термины. Элементарные формулы. Формулы. Переменные и постоянные предикаты. Предикатные переменные. Предметные переменные. Конкретные предметы. Кванторы. Область действия квантора. Свободные и связанные вхождения предметной переменной. Свободные и связанные предметные переменные. Язык алгебры предикатов. Допустимые множества для данной формулы. Интерпретация формулы на данном множестве. Область интерпретации. Формулы выполнимые и невыполнимые (ложные) в данной интерпретации. Выполнимые формулы. Противоречия (невыполнимые формулы). Формулы, истинные в данной интерпретации. Общезначимые формулы. Модель для множества формул Γ.

2.5. Контрольные вопросы.

1. Какие из выражений являются элементарными формулами:
   A, A_1, A_1^2, A', $\neg A'$, Φ, Ω, $P(x,y)$, $Q^1(x,y,t)$, $R(A,B,C)$.
2. Какие из выражений являются формулами: $\forall P\,P(x,y)$, $\exists x\,(Q(x) \to \neg P(y))$, $P(x) \to$ $\to (q(y,z)\ \&\ S(t))$, $\forall x\,\exists x\,P(x,y)$, $\exists z\,P_1(x,y)$.
3. В следующих ниже формулах укажите свободные и связанные вхождения каждой буквы. Какие из букв являются свободными переменными? Укажите область действия каждого из кванторов.
   (a) $\forall x\,(P(x,y,z) \to \neg\forall z\,Q(z,x))$;
   (b) $(\forall x\,\exists y\,R(x,y,z)\ \&\ \exists z\,S(x,y,z)) \to P(x,y,z)$;
   (c) $\forall x\,\exists y\,(P(x,y,z) \vee \neg P(x,y,z)) \to \exists z\,Q(x,y,z)$.
4. Может ли одна и та же буква иметь и свободные и связанные вхождения в формулу?
5. Может ли одна и та же буква быть одновременно свободной и связанной предметной переменной (в одной и той же формуле)?
6. Можно ли считать, что $\forall x\,P(z,t)$ и $P(z,t)$ суть одна и та же формула?
7. Поясните, почему язык алгебры высказываний является подъязыком алгебры предикатов.
8. Какие множества являются допустимыми для следующих формул:
   (a) $\exists x\,(P(x) \vee x^2 - 5x + 6 = 0)$;
   (b) $\forall x\,\exists y\,(x \leq y)$;
   (c) $\forall a\,\forall b\,\exists x\,(ax = b)$;
   (d) $P(x) \to (Q(y) \to \forall\, xP(x))$.
9. Может ли одна и та же формула иметь интерпретации на различных множествах? Приведите примеры.
10. В каком случае любое множество является допустимым для данной формулы?

11. Приведите пример выполнимой формулы и покажите ее выполнимость.
12. Приведите пример невыполнимой формулы.
13. Приведите пример формулы, выполнимой в одной интерпретации и невыполнимой в другой.
14. Приведите пример формулы, истинной в одной интерпретации и не являющейся истинной в другой.
15. Укажите модели для следующего множества формул:

$$\Gamma_1 = \{\forall x\,\forall y\forall z\,(xy = z), ((xy = t\ \&\ xy = t_1) \to t = t_1),\\ x(yz) = (xy)z, \forall x\,\forall y\,\exists z\,\exists t\,(xz = y\ \&\ tx = y)\}.$$

2.6. Упражнения. Докажите следующие утверждения.

1. $\mathfrak{a}$ ложна в данной интерпретации тогда и только тогда, когда $\neg\mathfrak{a}$ истинна в той же интерпретации.
2. Никакая формула не может быть одновременно истиной и ложной в одной и той же интерпретации.
3. Если в данной интерпретации истинны $\mathfrak{a}$ и $\mathfrak{a} \to \mathfrak{b}$, то истинна и $\mathfrak{b}$.
4. $\mathfrak{a} \to \mathfrak{b}$ ложна в данной интерпретации тогда и только тогда, когда $\mathfrak{a}$ в этой интерпретации истинна, а $\mathfrak{b}$ ложна.
5. Докажите, что формула $\forall x\,(P(x) \vee \neg P(x))$ общезначима.
6. Используя язык алгебры предикатов запишите в символической форме:
   (a) Определение предела последовательности;
   (b) Определение предела функции;
   (c) Определение простого числа;
   (d) Определение НОД и НОК двух чисел.

§ 3. Равносильные формулы алгебры предикатов

Равносильные формулы. Теорема о подстановках в равносильные формулы алгебры высказываний. Независимость формул от связанных переменных. Вынесение отрицания за кванторы. Вынесение кванторов за операции конъюнкции и дизъюнкции. Перестановка кванторов.

3.1. Равносильные формулы алгебры предикатов. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — некоторые формулы, а $\mathfrak{M}$ — множество, допустимое для этих формул. *Совместной* интерпретацией формул $\mathfrak{a}$ и $\mathfrak{b}$ на множестве $\mathfrak{M}$ называется всякая пара $\langle \mathfrak{a}', \mathfrak{b}' \rangle$ интерпретаций для $\mathfrak{a}$ и $\mathfrak{b}$, при которых переменные предикаты, входящие в $\mathfrak{a}$ и $\mathfrak{b}$ одновременно, одинаково интерпретируются на $\mathfrak{M}$.

Напомним, что интерпретации $\mathfrak{a}'$ и $\mathfrak{b}'$ являются предикатами на $\mathfrak{M}$ и потому имеет смысл говорить об общих логических возможностях для $\mathfrak{a}'$ и $\mathfrak{b}'$ на $\mathfrak{M}$.

Определение 1. *Две формулы $\mathfrak{a}$ и $\mathfrak{b}$ называются равносильными на множестве $\mathfrak{M}$ тогда и только тогда, когда $\mathfrak{M}$ является допустимым для $\mathfrak{a}$ и $\mathfrak{b}$ и в любой совместной интерпретации $\mathfrak{a}'$, $\mathfrak{b}'$ предикаты $\mathfrak{a}'$ и $\mathfrak{b}'$ принимают одинаковые значения истинности во всех общих логических возможностях для $\mathfrak{a}'$ и $\mathfrak{b}'$ на $\mathfrak{M}$ либо когда $\mathfrak{M}$ не является допустимым ни для $\mathfrak{a}$, ни для $\mathfrak{b}$. Обозначается:* $\mathfrak{a} \overset{\mathfrak{M}}{\equiv} \mathfrak{b}$.

Из определения непосредственно следует, что если множество $\mathfrak{M}$ является допустимым для одной из формул $\mathfrak{a}$ и $\mathfrak{b}$ и не является допустимым для другой, то $\mathfrak{a}$ и $\mathfrak{b}$ на $\mathfrak{M}$ неравносильны.

Определение 2. *Две формулы $\mathfrak{a}$ и $\mathfrak{b}$ называются равносильными, если они равносильны на любом множестве.*

Следующая ниже теорема связывает понятия равносильности и общезначимости.

Теорема 1. *Пусть для формул $\mathfrak{a}$ и $\mathfrak{b}$ любое множество является допустимым. Тогда:*

$$\mathfrak{a} \equiv \mathfrak{b} \Longleftrightarrow \mathfrak{a} \sim \mathfrak{b} \text{ — общезначима.}$$

Доказательство. Пусть $\mathfrak{M}$ — произвольное множество, $\mathfrak{a}' \sim \mathfrak{b}'$ — произвольная интерпретация формулы $\mathfrak{a} \sim \mathfrak{b}$ на $\mathfrak{M}$. Эта интерпретация, очевидно, будет совместной интерпретацией $\mathfrak{a}'$, $\mathfrak{b}'$ формул $\mathfrak{a}$ и $\mathfrak{b}$ на $\mathfrak{M}$. Зафиксируем произвольную логическую возможность для $\mathfrak{a}' \sim \mathfrak{b}'$. Она будет общей логической возможностью для $\mathfrak{a}'$, $\mathfrak{b}'$. Очевидно, что в этой логической возможности $\mathfrak{a}'$ и $\mathfrak{b}'$ принимают одинаковые значения тогда и только тогда, когда $\mathfrak{a}' \sim \mathfrak{b}'$ принимает значение, равное 1. В силу произвольности выбранного множества $\mathfrak{M}$, интерпретации и логической возможности получаем нужное. ■

3.2. Теорема о подстановках в равносильные формулы алгебры высказываний.

Теорема 1. *Если в равносильные формулы алгебры высказываний подставить вместо высказывательных переменных формулы алгебры предикатов, для которых любое множество допустимо, то полученные формулы алгебры предикатов будут также равносильны.*

Доказательство.

Пусть $\mathfrak{a}(A_1, \ldots, A_n) \equiv \mathfrak{b}(B_1, \ldots, B_m)$, где $A_1, \ldots, A_n$ и $B_1, \ldots, B_m$ — высказывательные переменные, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ и $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$ — формулы алгебры предикатов, для которых любое множество допустимо, $\mathfrak{M}$ — произвольно фиксированное множество и $\mathfrak{a}_0 = \mathfrak{a}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$, $\mathfrak{b}_0 = \mathfrak{b}(\mathfrak{b}_1, \ldots, \mathfrak{b}_m)$. Необходимо показать, что $\mathfrak{a}_0 \overset{\mathfrak{M}}{\equiv} \mathfrak{b}_0$.

Зафиксируем совместную интерпретацию $\mathfrak{a}'_0$, $\mathfrak{b}'_0$ для формул $\mathfrak{a}_0$, $\mathfrak{b}_0$ на множестве $\mathfrak{M}$. При этом $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$ также получат некоторую интерпретацию $\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n$, $\mathfrak{b}'_1, \ldots, \mathfrak{b}'_m$ на множестве $\mathfrak{M}$, причем $\mathfrak{a}'_0 = \mathfrak{a}(\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n)$, $\mathfrak{b}'_0 = \mathfrak{b}(\mathfrak{b}'_1, \ldots, \mathfrak{b}'_m)$.

Зафиксируем для предикатов $\mathfrak{a}'_0$ и $\mathfrak{b}'_0$ некоторую общую логическую возможность на $\mathfrak{M}$. Тогда в этой логической возможности каждый из предикатов $\mathfrak{a}'_1, \ldots, \mathfrak{a}'_n$, $\mathfrak{b}'_1, \ldots, \mathfrak{b}'_m$ получит соответственно значение $\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_m \in \{0, 1\}$. Но $\mathfrak{a}(\alpha_1, \ldots, \alpha_n)$ равно значению $\mathfrak{a}(A_1, \ldots, A_n)$ в логической возможности $(\alpha_1, \ldots, \alpha_n)$, а $\mathfrak{b}(\beta_1, \ldots, \beta_m)$ равно значению $\mathfrak{b}(B_1, \ldots, B_m)$ в логической

возможности $(\beta_1, \ldots, \beta_m)$. А так как $(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_m)$ является общей логической возможностью для формул $\mathfrak{a}(A_1, \ldots, A_n)$ и $\mathfrak{b}(B_1, \ldots, B_m)$, то значения $\mathfrak{a}(A_1, \ldots, A_n)$ и $\mathfrak{b}(B_1, \ldots, B_m)$ совпадают. Отсюда следует совпадение значений $\mathfrak{a}'_0$ и $\mathfrak{b}'_0$ в выбранной для них общей логической возможности. В силу произвольности логической возможности, интерпретации и множества $\mathfrak{M}$ получаем, что $\mathfrak{a}_0 \equiv \mathfrak{b}_0$. ■

3.3. Независимость формул от связанных переменных.

Теорема 1. *Пусть x — некоторая свободная предметная переменная в формуле $\mathfrak{a} = \mathfrak{a}(x)$, а буква y не входит в запись формулы $\mathfrak{a}$. Тогда*

$$\forall x\, \mathfrak{a}(x) \equiv \forall y\, \mathfrak{a}(y),$$
$$\exists x\, \mathfrak{a}(x) \equiv \exists y\, \mathfrak{a}(y).$$

Доказательство непосредственно следует из определения кванторных операций.

3.4. Вынесение отрицания за кванторы.

Теорема 1. *Пусть x — некоторая свободная предметная переменная в формуле $\mathfrak{a} = \mathfrak{a}(x)$. Тогда*

$$\neg\forall x\, \mathfrak{a}(x) \equiv \exists x\, \neg\mathfrak{a}(x),$$
$$\neg\exists x\, \mathfrak{a}(x) \equiv \forall x\, \neg\mathfrak{a}(x).$$

Доказательство. Пусть $\mathfrak{M}$ — произвольно фиксированное множество, допустимое для рассматриваемых формул. Зафиксируем некоторую совместную интерпретацию этих формул на $\mathfrak{M}$ и некоторую логическую возможность в этой интерпретации. Тогда в этой логической возможности имеем: $\neg\forall x\, \mathfrak{a}'(x) = 1 \Longleftrightarrow \forall x\, \mathfrak{a}'(x) = 0, \Longleftrightarrow$ не для любого $a \in \mathfrak{M}$: $\mathfrak{a}'(a) = 1 \Longleftrightarrow$ существует $b \in \mathfrak{M}$: $\mathfrak{a}'(b) = 0 \Longleftrightarrow$ существует $b \in \mathfrak{M}$: $\neg\mathfrak{a}'(b) = 1 \Longleftrightarrow \exists x\, \neg\mathfrak{a}'(x) = 1$. В силу произвольности множества $\mathfrak{M}$, интерпретации и логической возможности получаем, что $\neg\forall x\, \mathfrak{a}(x) \equiv \exists x\, \neg\mathfrak{a}(x)$.

Вторая формула доказывается аналогично. ■

3.5. Вынесение кванторов за операции конъюнкции и дизъюнкции.

Теорема 1. *Пусть $\mathfrak{a}(x)$ и $\mathfrak{b}(x)$ — некоторые формулы, x — свободная предметная переменная в них. $\mathfrak{d}$ — формула, не содержащая вхождений буквы x. Тогда истинны следующие равносильности:*

$$\forall x\, (\mathfrak{a}(x)\ \&\ \mathfrak{b}(x)) \equiv \forall x\, \mathfrak{a}(x)\ \&\ \forall x\, \mathfrak{b}(x), \tag{1}$$
$$\exists x\, (\mathfrak{a}(x)\ \&\ \mathfrak{d}) \equiv \exists x\, \mathfrak{a}(x)\ \&\ \mathfrak{d}, \tag{2}$$
$$\exists x\, (\mathfrak{a}(x) \vee \mathfrak{b}(x)) \equiv \exists x\, \mathfrak{a}(x) \vee \exists x\, \mathfrak{b}(x), \tag{3}$$
$$\forall x\, (\mathfrak{a}(x) \vee \mathfrak{d}) \equiv \forall x\, \mathfrak{a}(x) \vee \mathfrak{d}. \tag{4}$$

Доказательство. Зафиксируем произвольное допустимое множество $\mathfrak{M}$ и совместную интерпретацию формул, составляющих равносильность. Далее, зафиксируем общую логическую возможность в этой интерпретации. Тогда имеем:

(1) $\forall x(\mathfrak{a}'(x)\ \&\ \mathfrak{b}'(x)) = 1 \Longleftrightarrow$ для любого элемента $a \in \mathfrak{M}$: $\mathfrak{a}'(a)\ \&\ \mathfrak{b}'(a) = 1 \Longleftrightarrow$ для любого элемента $a \in \mathfrak{M}$: $\mathfrak{a}'(a) = 1$ и для любого элемента $a \in \mathfrak{M}$: $\mathfrak{b}'(a) = 1 \Longleftrightarrow \forall x\, \mathfrak{a}'(x) = 1$ и $\forall x\, \mathfrak{b}'(x) = 1$ $\Longleftrightarrow \forall x\, \mathfrak{a}'(x)\ \&\ \forall x\, \mathfrak{b}'(x) = 1$.

В силу произвольности $\mathfrak{M}$, интерпретации и логической возможности заключаем, что формула (1) доказана.

(2) $\exists x\, (\mathfrak{a}'(x)\ \&\ \mathfrak{d}') = 1 \Longleftrightarrow$ существует элемент $a \in \mathfrak{M}$: $\mathfrak{a}'(a)\ \&\ \mathfrak{d}' = 1 \Longleftrightarrow$ существует $a \in \mathfrak{M}$ такой, что $\mathfrak{a}'(a) = 1$ и $\mathfrak{d}' = 1 \Longleftrightarrow \exists x\, \mathfrak{a}'(x)\ \&\ \mathfrak{d}' = 1$.

В силу произвольности $\mathfrak{M}$, интерпретации и логической возможности заключаем, что формула (2) доказана.

(3), (4) доказывается аналогично. ■

3.6. Перестановка кванторов.

Теорема 1. *Для любой формулы* $\mathfrak{a}$ *справедливы утверждения:*

$$\text{(a) } \forall x\,\forall y\,\mathfrak{a} \equiv \forall y\,\forall x\,\mathfrak{a},$$
$$\text{(b) } \exists x\,\exists y\,\mathfrak{a} \equiv \exists y\,\exists x\,\mathfrak{a}.$$

Доказательство непосредственно следует из определения кванторных операций.

Таким образом из теоремы следует, что однотипные кванторы перестановочны. Следующий ниже пример показывает, что разнотипные кванторы неперестановочны.

Пример 1. Рассмотрим две формулы $\forall x\,\exists y\,P(x,y)$ и $\exists y\,\forall x\,P(x,y)$ на N. Проинтерпретируем переменный предикат $P(x,y)$ на N так: $P(x,y) =$ "$x \le y$". Тогда исходные формулы в такой интерпретации обратятся в высказывания $\forall x\,\exists y\,(x \le y)$ и $\exists y\,\forall x\,(x \le y)$, из которых первое истинно, а второе — ложно. Это означает, что на N формулы $\forall x\,\exists y\,P(x,y)$ и $\exists x\,\forall y\,P(x,y)$ неравносильны, следовательно эти формулы неравносильны.

3.7. Новые термины. Совместная интерпретация двух формул. Формулы, равносильные на множестве. Равносильные формулы.

3.8. Контрольные вопросы.

1. Приведите примеры формул, равносильных на одном множестве и неравносильных на другом.
2. Справедливы ли законы де Моргана для формул алгебры предикатов? Почему?

   Указание. Используйте теорему 3.2.1.
3. Равносильны ли формулы:
   (a) $\forall x\,\exists y\,\mathfrak{a}(x,y)$ и $\forall z\,\exists y\,\mathfrak{a}(z,y)$;
   (b) $\forall x\,\exists y\,\mathfrak{a}(x,y)$ и $\forall z\,\exists y\,\mathfrak{a}(y,z)$;
   (c) $\forall x\,\exists y\,\mathfrak{a}(x,y)$ и $\forall y\,\exists x\,\mathfrak{a}(x,y)$;
   (d) $\forall x\,\exists y\,\mathfrak{a}(x,y)$ и $\forall y\,\exists x\,\mathfrak{a}(y,x)$;

3.9. Упражнения.

1. Докажите, что если в теореме 3.1.1 отбросить условие допустимости любого множества для формул $\mathfrak{a}$ и $\mathfrak{b}$, то:
   (a) из общезначимости формулы $\mathfrak{a} \sim \mathfrak{b}$ следует равносильность $\mathfrak{a} \equiv \mathfrak{b}$.
   (b) из равносильности $\mathfrak{a} \equiv \mathfrak{b}$ не следует общезначимость формулы $\mathfrak{a} \sim \mathfrak{b}$.
2. Пользуясь теоремой 3.2.1, докажите в алгебре предикатов истинность следующих равносильностей:
   (a) $\mathfrak{a} \sim \mathfrak{b} \equiv (\mathfrak{a} \to \mathfrak{b})\ \&\ (\mathfrak{b} \to \mathfrak{a})$ — правило исключения эквиваленции;
   (b) $\mathfrak{a} \to \mathfrak{b} \equiv \neg\mathfrak{a} \vee \mathfrak{b}$ — правило исключения импликации;
   (c) $\mathfrak{a} \vee \mathfrak{b} \equiv \neg(\neg\mathfrak{a}\ \&\ \neg\mathfrak{b})$ — правило исключения дизъюнкции.
3. Пользуясь известными свойствами равносильных формул, доказать истинность следующих равносильностей для формул $\mathfrak{a}$, $\mathfrak{b}$ и $\mathfrak{d}$, где $\mathfrak{d}$ не содержит свободных вхождений буквы x:
   (a) $\forall x\,(\mathfrak{a}(x) \to \mathfrak{d}) \equiv \exists x\,\mathfrak{a}(x) \to \mathfrak{d}$,
   (b) $\exists x\,(\mathfrak{a}(x) \to \mathfrak{d}) \equiv \forall x\,\mathfrak{a}(x) \to \mathfrak{d}$,
   (c) $\forall x\,(\mathfrak{d} \to \mathfrak{a}(x)) \equiv \mathfrak{d} \to \forall x\,\mathfrak{a}(x)$,
   (d) $\exists x\,(\mathfrak{d} \to \mathfrak{a}(x)) \equiv \mathfrak{d} \to \exists x\,\mathfrak{a}(x)$.

В качестве образца приведем пример решения пункта (a):

$$\forall x\,(\mathfrak{a}(x) \to \mathfrak{d}) \overset{\text{Упр. 2(b)}}{\equiv} \forall x\,(\neg\mathfrak{a}(x) \vee \mathfrak{d}) \overset{\text{теор. 3.5.1}}{\equiv}$$
$$\overset{\text{теор. 3.5.1}}{\equiv} \forall x\,\neg\mathfrak{a}(x) \vee \mathfrak{d} \overset{\text{теор. 3.4.1}}{\equiv} \neg\exists x\,\mathfrak{a}(x) \vee \mathfrak{d} \overset{\text{Упр. 2(b)}}{\equiv} \exists x\,\mathfrak{a}(x) \to \mathfrak{d}.$$

4. Пусть $\mathfrak{a}(x)$ — некоторая формула алгебры предикатов, x — свободная предметная переменная в $\mathfrak{a}(x)$. Тогда истинны следующие равносильности:

   (a) $\forall x\,\mathfrak{a}(x) \equiv \neg\exists x\,\neg\mathfrak{a}(x)$;

   (b) $\exists x\,\mathfrak{a}(x) \equiv \neg\forall x\,\neg\mathfrak{a}(x)$;

   (c) $\forall x\,\mathfrak{a}(x) \to \mathfrak{a}(y) \equiv \exists x\,(\mathfrak{a}(x) \to \mathfrak{a}(y))$;

   (d) $\mathfrak{a}(y) \to \exists x\,\mathfrak{a}(x) \equiv \exists x\,(\mathfrak{a}(y) \to \mathfrak{a}(x))$.

§ 4. Предваренная нормальная форма

Приведенная форма для формул алгебры предикатов. Предваренная нормальная форма.

Цель данного параграфа — доказать, что всякую формулу алгебры предикатов можно привести к такому виду, в котором она воспринимается (с точки зрения ее содержательного смысла) гораздо легче.

4.1. Приведенная форма для формул алгебры предикатов.

Определение 1. *Формула* $\mathfrak{a}$ *называется приведенной формой, если* $\mathfrak{a}$ *не содержит операций импликации и эквиваленции и знаки отрицания относятся лишь к элементарным формулам.*

Пример 1. Формулы $(\forall x\, P(x,y) \vee \neg Q(z)) \to A$, $\neg(B \,\&\, \neg P(x))$, $\neg\forall x\, Q(y)$ не являются приведенными формами, а формулы $(\exists x\, \neg P(x,y) \,\&\, Q(z)) \vee A$, $\neg S \vee P(x)$, $\exists x\, \neg Q(x)$ являются приведенными формами.

Теорема 1. *Всякая формула алгебры предикатов равносильна некоторой приведенной форме.*

Доказательство. Пусть $\mathfrak{a}$ — произвольная формула алгебры предикатов. В силу упр. 2 предыдущего параграфа всякая формула равносильна такой формуле, в которой нет операций $\to$ и $\sim$.

Проведем доказательство индукцией по количеству n операций (связок) в формуле $\mathfrak{a}$.

Если $n = 0$, то есть $\mathfrak{a}$ не содержит связок, то $\mathfrak{a}$ есть элементарная формула и, следовательно, $\mathfrak{a}$ является приведенной формой.

Пусть $n > 0$ и для всякого k, $0 \le k < n$, формулы, содержащие k логических операций, равносильны приведенной форме. По определению формула $\mathfrak{a}$ имеет один из следующих видов:

$$1)\ \mathfrak{a} = \neg\mathfrak{b};$$
$$2)\ \mathfrak{a} = \mathfrak{b} \,\&\, \mathfrak{d};$$
$$3)\ \mathfrak{a} = \mathfrak{b} \vee \mathfrak{d};$$
$$4)\ \mathfrak{a} = \forall x\, \mathfrak{b};$$
$$5)\ \mathfrak{a} = \exists x\, \mathfrak{b}.$$

Причем, формулы $\mathfrak{b}$ и $\mathfrak{d}$ по индуктивному предположению равносильны приведенным формам:

$$\mathfrak{b} \equiv \mathfrak{b}^*$$
$$\mathfrak{d} \equiv \mathfrak{d}^*$$

Тогда:
2) $\mathfrak{a} \equiv \mathfrak{b}^* \,\&\, \mathfrak{d}^*$ — приведенная форма;
3) $\mathfrak{a} \equiv \mathfrak{b}^* \vee \mathfrak{d}^*$ — приведенная форма;
4) $\mathfrak{a} \equiv \forall x\, \mathfrak{b}^*$ — приведенная форма;
5) $\mathfrak{a} \equiv \exists x\, \mathfrak{b}^*$ — приведенная форма.

Таким образом осталось рассмотреть случай 1).

1) $\mathfrak{a} \equiv \neg\mathfrak{b}^*$, где $\mathfrak{b}^*$ — приведенная форма. Строго говоря, этот случай следует доказывать индукцией по количеству логических связок в $\mathfrak{b}^*$. Однако мы ограничимся лишь апелляцией к пониманию того, почему это так.

$\mathfrak{b}^*$ — приведенная форма. Пользуясь законами де Моргана и теоремой 3.4.1 отрицание в формуле $\neg\mathfrak{b}^*$ последовательно можно отнести к элементарным формулам, составляющим формулу $\mathfrak{b}^*$. Таким образом, теорему можно считать доказанной. ■

4.2. Предваренная нормальная форма.

Определение 1. *Формула* $\mathfrak{a}$ *называется предваренной нормальной формой, если* $\mathfrak{a}$ *имеет вид:*

$$\mathfrak{a} = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b},$$

где $Q_1, \ldots, Q_n \in \{\forall, \exists\}$, *а формула* $\mathfrak{b}$ *является приведенной формой, не содержащей кванторов.*

Пример 1. Формулы: $\forall x\, P(x)$, $\exists x\, \forall y\, \exists z\, (\neg P(x,y) \vee Q(z))$, $\forall x\, \forall y\, ((P(x,y)\ \&\ Q(z)) \vee \neg P(x,y))$ — предваренные нормальные формы, а формулы: $\neg \forall x\, P(x)$, $\exists x\, \forall y\, \exists z\, \neg (P(x,y) \vee A)$, $\forall x\, \exists y\, (\forall z\, P(z) \vee \vee \neg Q(x,y))$ не являются предваренными нормальными формами. Поясните, почему.

Теорема 1. *Всякая формула $\mathfrak{a}$ алгебры предикатов равносильна некоторой предваренной нормальной форме.*

Доказательство. Как и в предыдущей теореме можно считать, что $\mathfrak{a}$ не содержит операций $\to$ и $\sim$.

Так как всякая формула равносильна приведенной форме, см. теорема 4.1.1, то достаточно показать, что формула $\mathfrak{a}$ равносильна формуле

$$Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b}, \tag{1}$$

где $\mathfrak{b}$ — бесквантворная формула.

Индукция по количеству n логических операций в формуле $\mathfrak{a}$.

Если $n = 0$, то $\mathfrak{a}$ является элементарной формулой и, следовательно, $\mathfrak{a}$ есть предваренная нормальная форма.

Пусть теперь $n > 0$ и для всякого k, $0 \le k < N$ формулы с количеством логических операций k равносильны формуле вида (1).

По определению формулы, $\mathfrak{a}$ имеет вид:

$$\begin{array}{l} 1)\ \mathfrak{a} = \neg \mathfrak{b}; \\ 2)\ \mathfrak{a} = \mathfrak{b}\ \&\ \mathfrak{d}; \\ 3)\ \mathfrak{a} = \mathfrak{b} \vee \mathfrak{d}; \\ 4)\ \mathfrak{a} = \forall x\, \mathfrak{b}; \\ 5)\ \mathfrak{a} = \exists x\, \mathfrak{b}. \end{array}$$

Причем можно считать, что формулы $\mathfrak{b}$ и $\mathfrak{d}$ имеют вид (1). Пусть:

$$\begin{array}{l} \mathfrak{b} = Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b}_1, \\ \mathfrak{d} = R_1 y_1\, R_2 y_2 \ldots R_m y_m\, \mathfrak{d}_1, \end{array}$$

где $\mathfrak{b}_1$ и $\mathfrak{d}_1$ — безквантворные формулы, $Q_1, \ldots, Q_n, R_1, \ldots, R_m \in \{\forall, \exists\}$.

На основании теоремы 3.3.1 можно считать, что буквы $x_1, \ldots, x_n$ не входят в запись формулы $\mathfrak{d}$, а буквы $y_1, \ldots, y_m$ не входят в запись формулы $\mathfrak{b}$.

1) $\mathfrak{a} = \neg \mathfrak{b}$. Пользуемся теоремой 3.4.1.

$$\mathfrak{a} = \neg \mathfrak{b} = \neg Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b}_1 \equiv Q_1' x_1\, (\neg Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b}_1) \equiv \ldots \equiv Q_1' x_1 \ldots Q_n' x_n \neg \mathfrak{b}_1$$

— имеет вид (1). Здесь

$$Q_i' = \begin{cases} \forall, & \text{если } Q_i = \exists, \\ \exists, & \text{если } Q_i = \forall. \end{cases}$$

2) $\mathfrak{a} = \mathfrak{b}\ \&\ \mathfrak{d}$. Воспользуемся теоремой 3.5.1 п. (1), (2).

$$\begin{array}{l} \mathfrak{a} = \mathfrak{b}\ \&\ \mathfrak{d} = Q_1 x_1\, Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b}_1\ \&\ R_1 y_1\, R_2 y_2 \ldots R_m y_m\, \mathfrak{d}_1 \equiv \\ \equiv Q_1 x_1\, (Q_2 x_2 \ldots Q_n x_n\, \mathfrak{b}_1\ \&\ R_1 y_1\, R_2 y_2 \ldots R_m y_m\, \mathfrak{d}_1) \equiv \ldots \\ \ldots \equiv Q_1 x_1 \ldots Q_n x_n\, (\mathfrak{b}_1\ \&\ R_1 y_1\, R_2 y_2 \ldots R_m y_m\, \mathfrak{d}_1) \equiv \\ \equiv Q_1 x_1 \ldots Q_n x_n\, R_1 y_1\, (\mathfrak{b}_1\ \&\ R_2 y_2 \ldots R_m y_m\, \mathfrak{d}_1) \equiv \ldots \\ \ldots \equiv Q_1 x_1 \ldots Q_n x_n\, R_1 y_1 \ldots R_m y_m\, (\mathfrak{b}_1\ \&\ \mathfrak{d}_1) \end{array}$$

— имеет вид (1).

3) $\mathfrak{a} = \mathfrak{b} \vee \mathfrak{d}$. Воспользовавшись теоремой 3.5.1 п. (3), (4) и проводя равносильные преобразования, подобные преобразованиям предыдущего пункта, получим нужное.

4) $\mathfrak{a} = \forall x\, \mathfrak{b} = \forall x\, Q_1 x_1 \ldots Q_n x_n\, \mathfrak{b}_1$ — имеет вид (1).

5) Точно также, как и в 4). ■

Пример 2. Привести к предваренной нормальной форме формулу

$$\neg(\forall x\,\exists y\,P(x,y) \to \exists x\,Q(x))$$

Решение:

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

4.3. Новые термины. Приведенная форма. Предваренная нормальная форма.

4.4. Контрольные вопросы.

1. Какие из формул являются приведенными формами:
   (a) $(P(x) \to \forall x\,Q(x,y)) \vee A$;
   (b) $\forall x\,P(x)\ \&\ \neg(A \vee B)$;
   (c) $\forall x\,(\neg S(x,y) \vee \forall y\,Q(x,y))$;
   (d) $\forall x\,(\neg S(x,y) \vee \neg\forall y\,Q(x,y))$.
2. Какие из формул предыдущего примера являются предваренными нормальными формами?
3. Какие из формул являются предваренными нормальными формами:
   (a) $\forall x\,\exists y\,\exists z\,(P(x,y,z) \vee \exists x\,(Qx,y))$;
   (b) $\forall x\,\exists y\,\exists z\,\exists t\,(P(x,y,z) \vee \exists x\,(Qx,t))$;
   (c) $\exists x\,\forall y\,\exists z\,(\neg P(x,y,z) \to \neg\exists x\,(Qx,y))$.

4.5. Упражнения.

1. Привести к предваренной нормальной форме формулы вопроса 1 п. VI.4.4.
2. Привести к предваренной нормальной форме формулы вопроса 3 п. VI.4.4.
3. Проведите подробные рассуждения в доказательстве части 3) теоремы 4.2.1.
4. Привести к предваренной нормальной форме:
   (a) $\forall x\,(P(x) \to Q(x,y)) \to (\exists y\,P(y) \to \exists z\,Q(x,y,z))$;
   (b) $\exists x\,P(x,y) \to (Q(x) \to \neg\exists y\,P(x,z))$;

§ 5. Теории первого порядка

Термы и формулы теорий первого порядка. Теории 1-го порядка. Аксиомы и правила вывода теорий 1-го порядка. Модели. Непротиворечивость, полнота и неразрешимость исчислений предикатов первого порядка. Формальная арифметика. Теорема Гёделя о неполноте формальной арифметики.

В этом параграфе рассматриваются формальные теории первого порядка, которые, как и исчисление высказываний, служат примерами формальных аксиоматических теорий. Рассмотренная в предыдущих параграфах алгебра предикатов также формализуется в виде теории 1-го порядка, которая называется исчислением предикатов. С другой стороны, каждая из теорий 1-го порядка является расширением формализованного исчисления предикатов.

5.1. Термы и формулы теорий первого порядка. Алфавит произвольной теории первого порядка состоит из следующих символов.

1. $\{x_1, x_2, \ldots\}$ эти буквы обозначают предметные переменные теории.
2. $\{a_1, a_2, \ldots\}$ эти буквы обозначают предметные постоянные (константы) теории.
3. P_i^n — предикатные переменные.
4. f_i^n — функциональные переменные.
5. $\neg$, $\to$, $\forall$ — логические символы.
6.), (, ',' — вспомогательные символы.

В теории 1-го порядка символов, обозначающих предметные постоянные может быть конечное и даже пустое множество. Предикатных переменных может быть конечное, но не пустое множество. Множество функциональных переменных может быть и пустым.

Определим терм теории 1-го порядка следующим образом.

Определение 1.

1. *Каждая предметная переменная и каждая предметная постоянная являются термом (элементарным).*
2. *Если $t_1, t_2, \ldots, t_n$ являются термами, то $f_i^n(t_1, t_2, \ldots, t_n)$ также является термом, где f_i^n — функциональный символ теории, n — верхний индекс, указывающий местность этого символа, а нижний индекс i разделяет различные функциональные символы.*
3. *Других термов нет.*

Пример 1. Пусть f_1^2 и f_2^2 — функциональные символы некоторой теории 1-го порядка, тогда выражения $f_1^2(x_1, x_2)$, $f_1^2(x_1, x_1)$, $f_2^2(x_2, x_1)$, $f_2^2(f_1^2(a_1, x_1), f_2^2(x_2, x_1))$ являются термами при условии, что x_1, x_2 — предметные переменные, а a_1 — предметная постоянная этой теории.

Часто из соображений удобства используют не префиксную запись, а инфиксную. При этом обычно заменяют функциональные символы на более привычные. Например, если символу f_1^2 поставить в соответствие символ $\cdot$, а символу f_2^2 — символ $+$, то, используя инфиксную запись, термы этого примера могут быть записаны в виде $x_1 \cdot x_2$, $x_1 \cdot x_1$, $x_2 + x_1$, $(a_1 \cdot x_1) + (x_2 + x_1)$ соответственно. В последнем случае скобки указывают порядок выполнения операций (действий функциональных символов).

Определим формулу теории 1-го порядка следующим образом.

Определение 2.

1. *Если P_i^n — предикатный символ теории, $t_1, \ldots, t_n$ — термы, то выражение $P_i^n(t_1, \ldots, t_n)$ является формулой (элементарной).*

2. *Если* $\mathfrak{a}$ *и* $\mathfrak{b}$ *— формулы теории 1-го порядка, то следующие выражения* $\neg\mathfrak{a}$, $(\mathfrak{a}\to\mathfrak{b})$, $\forall x_i\mathfrak{a}$ *также являются формулами данной теории.*

3. *Других формул нет.*

Заметим, что понятие о свободных и связанных переменных, соглашения о расстановке скобок в формулах теорий 1-го порядка предполагаются такими же как и в алгебре предикатов. Кроме того видно, что формулы теорий 1-го порядка не содержат квантор $\exists$. Без него можно обойтись, считая $\exists x_i\mathfrak{a}$ сокращением записи формулы $\neg\forall x_i\neg\mathfrak{a}$ (точно также в исчислении высказываний обходятся без символов $\&$, $\vee$ и $\sim$).

5.2. Терм, свободный для переменной в формуле.

Определение 1. *Терм* t *называется свободным для переменной* x *в формуле* $\mathfrak{a}$, *если никакое свободное вхождение* x *в* $\mathfrak{a}$ *не лежит в области действия кванторов по какой-либо переменной, входящей в запись терма* t.

Пример 1. Пусть $\mathfrak{a}=\forall x_1\forall x_2P_1^3(x_1,x_2,x_3)$ и $t=f_1^3(x_1,x_2,x_3)$, тогда терм t не является свободным для переменной x_3 в формуле $\mathfrak{a}$, так как свободное вхождение x_3 в формулу $\mathfrak{a}$ находится в области действия, например, переменной x_2, входящей в запись терма t. Терм t является свободным для переменных x_1 и x_2, так как они вообще не имеют свободных вхождений в формуле $\mathfrak{a}$.

Пример 2. Пусть $\mathfrak{a}=\forall x_1P_1^2(x_1,x_2)$ и $t=f_1^1(x_1)$, тогда терм t является свободным для переменной x_1 в формуле $\mathfrak{a}$, так как она не имеет свободных вхождений в формуле $\mathfrak{a}$. Терм t не является свободным для переменной x_2, так как свободное вхождение x_2 в формулу $\mathfrak{a}$ находится в области действия квантора по переменной x_1, входящей в запись терма t.

Пример 3. Если x не имеет свободных вхождений в $\mathfrak{a}$, то любой терм t является свободным для x в формуле $\mathfrak{a}$.

Пример 4. Всякий терм, не содержащий предметных переменных (то есть содержащий только предметные постоянные), свободен для любой переменной в любой формуле.

Пример 5. Если никакая переменная терма t не является связанной в формуле $\mathfrak{a}$, то t свободен для любой переменной в формуле $\mathfrak{a}$.

Пример 6. Терм $t=x$ свободен для переменной x в любой формуле.

5.3. Аксиомы и правила вывода теорий первого порядка. В теориях первого порядка все аксиомы делятся на логические и собственные (или специальные). Теория первого порядка, не содержащая собственных аксиом называется *исчислением предикатов* и формализует алгебру предикатов, с соответствующим набором предикатных символов и предметных постоянных.

Схемы логических аксиом в любой теории первого порядка одни и те же.

Логические аксиомы. Для любых формул $\mathfrak{a}$. $\mathfrak{b}$, $\mathfrak{c}$ теории 1-го порядка следующие ниже формулы являются аксиомами.

A1. $\mathfrak{a}\to(\mathfrak{b}\to\mathfrak{a})$;

A2. $(\mathfrak{a}\to(\mathfrak{b}\to\mathfrak{c}))\to((\mathfrak{a}\to\mathfrak{b})\to(\mathfrak{a}\to\mathfrak{c}))$;

A3. $(\neg\mathfrak{b}\to\neg\mathfrak{a})\to((\neg\mathfrak{b}\to\mathfrak{a})\to\mathfrak{b})$;

A4. $\forall x_i\mathfrak{a}(x_i)\to\mathfrak{a}(t)$, где t есть терм, свободный для x_i в формуле $\mathfrak{a}(x_i)$;

A5. $\forall x_i(\mathfrak{a}\to\mathfrak{b})\to(\mathfrak{a}\to\forall x_i\mathfrak{b})$, где формула $\mathfrak{a}$ не содержит свободных вхождений x_i.

Собственные аксиомы зависят от теории 1-го порядка и меняются от теории к теории.

Правила вывода. Любая теория 1-го порядка содержит два правила вывода, формулируемых для произвольных формул $\mathfrak{a}$ и $\mathfrak{b}$ этой теории.

1. $\mathfrak{a}, \mathfrak{a} \to \mathfrak{b} \vdash \mathfrak{b}$ — правило MP (Modus Ponens).

2. $\mathfrak{a} \vdash \forall x_i \mathfrak{a}$ — правило Gen (обобщения).

Заметим, что любая теория 1-го порядка содержит исчисление высказываний в качестве подтеории. Поэтому многие свойства и утверждения верные для исчисления высказываний остаются по форме такими же и в теориях 1-го порядка. Однако, некоторые свойства оказываются неверными или требуют уточнений. Например, теорема дедукции также имеет место в теориях 1-го порядка, однако со значительными дополнительными условиями в формулировке; исчисление высказываний непротиворечиво и такими же являются исчисления предикатов 1-го порядка (см. далее); исчисление высказываний есть разрешимая теория, а любая теория первого порядка неразрешима (см. далее) и т. д.

Пример 1. Непустое множество с заданной на нем бинарной ассоциативной операцией называется *полугруппой*. Постоим теорию первого порядка, формализующую теорию полугрупп. Итак, формальная теория полугрупп:

1. Предметных постоянных не содержит.

2. Содержит одну предикатную переменную P_1^2, которая обозначает предикат равенства. Далее, в записи формул этой теории вместо $P_1^2(x_1, x_2)$ будем писать $x_1 = x_2$.

3. Содержит один функциональный символ f_1^2, обозначающий операцию в полугруппе. Далее, вместо $f_1^2(x_1, x_2)$ будем использовать более привычное обозначение $x_1 \cdot x_2$.

Собственные аксиомы теории полугрупп (схемы логических аксиом во всех теориях 1-го порядка одинаковы):

1. $\forall x_1 (x_1 = x_1)$. Эта аксиома устанавливает рефлексивность равенства.

2. $\forall x_1 \forall x_2 (x_1 = x_2 \to x_2 = x_1)$. Эта аксиома устанавливает симметричность равенства.

3. $\forall x_1 \forall x_2 \forall x_3 \big(x_1 = x_2 \to (x_2 = x_3 \to x_1 = x_3)\big)$. Эта аксиома устанавливает транзитивность равенства.

4. $\forall x_1 \forall x_2 \forall x_3 \big(x_1 = x_2 \to (x_3 \cdot x_1 = x_3 \cdot x_2 \ \& \ x_1 \cdot x_3 = x_2 \cdot x_3)\big)$. Эта аксиома устанавливает свойство подстановочности равенства. Отметим, что символ & трактуется так же как в исчислении высказываний.

5. $\forall x_1 \forall x_2 \forall x_3 \big(x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3\big)$. Эта аксиома устанавливает свойство ассоциативности операции.

Собственные аксиомы 1–3 формализуют интуитивно понятные свойства равенства и включаются в любую теорию 1-го порядка, содержащую предикат равенства.

Если в полугруппе выполняется формула $\forall x_1 \forall x_2 (x_1 \cdot x_2 = x_2 \cdot x_1)$, то она называется *коммутативной*. Добавляя эту формулу в качестве собственной аксиомы, получим теорию коммутативных полугрупп.

5.4. Области интерпретации и модели.

Определение 1. *Пусть $\mathfrak{a}$ — формула некоторой теории 1-го порядка τ, M — некоторое множество. Если для каждого предикатного и функционального символа на M заданы соответствующие конкретные предикаты и операции, а каждой предметной постоянной поставлен в соответствие некоторый элемент множества M, то M обратится в некоторую алгебраическую систему (множество с заданными на нем операциями и предикатами). Эта алгебраическая система называется областью интерпретации формулы $\mathfrak{a}$ теории τ.*

Определение 2. *Моделью теории 1-го порядка τ называется всякая область интерпретации в которой истинны все аксиомы (логические и собственные) теории τ.*

Пользуясь обычными понятиями выполнимости и истинности, легко показать, что для произвольных формул $\mathfrak{a}$ и $\mathfrak{b}$ теории 1-го порядка τ

1. Если на данной области интерпретации истинны формулы $\mathfrak{a}$ и $\mathfrak{a} \to \mathfrak{b}$, то истинна и формула $\mathfrak{b}$.

2. $\mathfrak{a}$ истинно на данной области интерпретации тогда и только тогда, когда истинно $\forall x_i \mathfrak{a}$.

Это означает, что всякая выводимая в τ формула будет истинной на модели этой теории. Обычно при построении теории 1-го порядка τ, формализующей некоторую содержательную теорию, собственные аксиомы выбираются так, чтобы множество логических следствий всех аксиом τ совпадало со множеством всех выводимых в τ формул.

Пример 1. Всякая полугруппа является моделью формальной теории полугрупп, построенной в примере 5.3.1.

Пример 2. Множество всех точек и прямых произвольной плоскости является моделью геометрии Евклида (планиметрии).

5.5. Непротиворечивость, полнота и неразрешимость исчислений предикатов первого порядка. Нижеследующую теорему называют теоремой Гёделя о полноте исчисления предикатов.

Теорема 1. *Во всяком исчислении предикатов 1-го порядка теоремами являются те и только те формулы, которые логически общезначимы.*

Данная теорема приводится без доказательства.

Теорема 2. *Всякое исчисление предикатов 1-го порядка непротиворечиво.*

Доказательство. Обозначим через $h(\mathfrak{a})$ формулу, которая получается из $\mathfrak{a}$ удалением всех кванторов и термов вместе с соответствующими скобками, запятыми, предметными переменными и предметными постоянными. Таким образом, $h(\mathfrak{a})$ является формулой алгебры высказываний.

Легко видно, что оператор h, примененный к логическим аксиомам произвольного исчисления предикатов дает тавтологии. Также проверяется, что если $h(\mathfrak{a})$ и $h(\mathfrak{a} \to \mathfrak{b})$ являются тавтологиями, то и $h(\mathfrak{b})$ также тавтология. Так как $h(\mathfrak{a}) = h(\forall x_i \mathfrak{a})$, то если $h(\mathfrak{a})$ — тавтология, то и $h(\forall x_i \mathfrak{a})$ также тавтология. Все это означает, что если $\mathfrak{a}$ есть выводимая в исчислении предикатов формула, то $h(\mathfrak{a})$ — тавтология. Значит, если бы в исчислении предикатов существовала бы формула $\mathfrak{b}$ такая, что $\vdash \mathfrak{b}$ и $\vdash \neg\mathfrak{b}$, то $h(\mathfrak{b})$ и $h(\neg\mathfrak{b}) = \neg h(\mathfrak{b})$ были бы тавтологиями, что невозможно. ■

Теорема 3. *Всякое исчисление предикатов первого порядка является неразрешимой теорией.*

Теорема также приводится без доказательства и из нее следует, что так как каждая теория 1-го порядка содержит некоторое исчисление предикатов в качестве подтеории, то любая теория 1-го порядка неразрешима, то есть не существует алгоритма, который позволял бы для каждой формулы этой теории определять является эта формула выводимой или нет.

5.6. Формальная арифметика. Наряду с геометрией арифметика наиболее непосредственно интуитивная область математики. Поэтому вполне естественно именно с арифметики начать попытку формализации и строгого обоснования математики. Первое, полуаксиоматическое построение арифметики было предложено Дедекиндом и Пеано независимо. Эти аксиомы известны под названием “системы аксиом Пеано”.

Аксиомы Пеано.

P1. 0 есть натуральное число.

P2. Для любого натурального числа x существует число x' непосредственно следующее за x.

P3. Для любого натурального числа x, $0 \neq x'$.

P4. Если для натуральных чисел x и y верно $x' = y'$, то $x = y$.

P5. Если Q есть свойство, которым, быть может, обладают одни и не обладают другие натуральные числа, и если

1) 0 обладает свойством Q;

2) для любого натурального числа x, если x обладает свойством Q, то и x' обладает Q;

то свойством Q обладают все натуральные числа.

Аксиому P5 называют *принцип индукции.* Этих аксиом, вместе с некоторыми фрагментом теории множеств достаточно для построения не только арифметики натуральных чисел, но и теории рациональных, вещественных и комплексных чисел (Ландау, 1930).

Однако, в этих аксиомах содержатся интуитивные понятия такие, например, как "свойство". Кроме того, отсутствуют правила вывода. Все это говорит о том, что эту систему нельзя считать строгой формализацией.

В этом пункте построим некоторую теорию 1-го порядка S, основанную на системе аксиом Пеано, которая окажется, по всей видимости, достаточной для вывода всех основных результатов элементарной арифметики. Теория S имеет: один предикатный символ P_1^2 — предикат равенства, который опять будем обозначать знаком $=$ и использовать инфиксную запись; одну предметную постоянную a_1, которую будем обозначать символом 0; три функциональных символа — одноместный f_1^1 и два двуместных f_1^2 и f_2^2, которые будем обозначать как t', $t + s$ и $t \cdot s$, где t и s — произвольные термы теории S.

Собственные аксиомы теории S.

S1. $x_1 = x_2 \to (x_1 = x_3 \to x_2 = x_3)$

S2. $x_1 = x_2 \to x_1' = x_2'$

S3. $0 \neq x_1'$

S4. $x_1' = x_2' \to x_1 = x_2$

S5. $x_1 + 0 = x_1$

S6. $x_1 + x_2' = (x_1 + x_2)'$

S7. $x_1 \cdot 0 = 0$

S8. $x_1 \cdot x_2' = (x_1 \cdot x_2) + x_1$

S9. $\mathfrak{a}(0) \to \big(\forall x(\mathfrak{a}(x) \to \mathfrak{a}(x')) \to \forall x\,\mathfrak{a}(x)\big)$, где $\mathfrak{a}(x) \in S$

Заметим, что аксиомы S1–S8 являются конкретными формулами, а S9 представляет собой схему аксиом, причем S9 (принцип математической индукции) не соответствует полностью аксиоме P5 системы Пеано, поскольку в P5 интуитивно предполагается континуум свойств натуральных чисел, а S9 может иметь дело лишь со счетным множеством свойств, определяемых формулами теории S.

Аксиомы S3 и S4 соответствуют аксиомам P3 и P4 системы аксиом Пеано. Аксиомы P1 и P2 обеспечивают существование нуля и операции "непосредственно следующий", которым в теории S соответствуют предметная константа a_1 и функциональный символ f_1^1. Аксиомы S1 и S2 обеспечивают необходимые свойства равенства, которые Пеано и Дедекиндом предполагались интуитивно очевидными. Аксиомы S5–S8 представляют собой рекурсивные равенства, служащие определениями операций сложения и умножения. Никаких постулатов, соответствующих этим аксиомам Дедекинд и Пеано не формулировали, потому что они допускали использование интуитивной теории множеств, в рамках которой можно вывести существование операций $\cdot$ и $+$.

С помощью правила вывода MP и аксиомы S9 можно, например, получить производное правило вывода теории S: $\mathfrak{a}(0), \forall x(\mathfrak{a}(x) \to \mathfrak{a}(x')) \vdash \forall x\,\mathfrak{a}(x)$, которое называется *правилом индукции.*

5.7. Примеры выводов в формальной арифметике S. Покажем, что в любой теории первого порядка имеет место следующее *правило индивидуализации.*

Теорема 1. *В любой теории 1-го порядка если терм t свободен для переменной x в формуле $\mathfrak{a}(x)$, то $\forall x\mathfrak{a}(x) \vdash \mathfrak{a}(t)$.*

Доказательство. Рассмотрим последовательность формул:

1. $\forall x\mathfrak{a}(x)$ — гипотеза,
2. $\forall x\mathfrak{a}(x) \to \mathfrak{a}(t)$ — аксиома A4,
3. $\mathfrak{a}(t)$ — MP 1,2

Эта последовательность является выводом формулы $\mathfrak{a}(t)$ из гипотезы $\forall x\mathfrak{a}(x)$. ■

Теорема 2. *В формальной арифметике S формула $t = r \to t' = r'$ является выводимой, где t и r — произвольные термы.*

Доказательство. Построим вывод этой формулы.

1. $x_1 = x_2 \to x_1' = x_2'$ — аксиома S2,
2. $\forall x_2(x_1 = x_2 \to x_1' = x_2')$ — правило Gen к п. 1,
3. $\forall x_1\forall x_2(x_1 = x_2 \to x_1' = x_2')$ — правило Gen к п. 2,
4. $\forall x_2(t = x_2 \to t' = x_2')$ — правило индивидуализации к п. 3,
5. $t = r \to t' = r'$ — правило индивидуализации к п. 4.

Поясните самостоятельно правомерность применения в этом выводе правила индивидуализации. ■

Эта теорема и аналогичные ей показывают почему аксиомы S1–S8 формальной арифметики являются конкретными формулами, а не схемами аксиом.

5.8. Теорема Гёделя о неполноте формальной арифметики S. В связи с обнаружением на рубеже XIX и XX веков различных парадоксов в основаниях математики были предприняты значительные усилия по их устранению и доказательству непротиворечивости классической математики. Один из путей в этом направлении разрабатывался немецким математиком Д. Гильбертом. Основанное им течение в обосновании математики получило название *формализма.* Большая роль в этих исследованиях отводилась формальной арифметике, так как доказательство непротиворечивости значительной части классической математики может быть сведена к проблеме непротиворечивости арифметики натуральных чисел. После некоторых частичных успехов гильбертовской школы в доказательстве непротиворечивости арифметики надежды на получение желаемого достижения были уничтожены результатом, полученным в 1931 году К. Гёделем. Он утверждает невозможность доказательства непротиворечивости формальной теории, включающей формальную арифметику, конструктивными методами, формализуемыми в самой теории.

Приведем формулировки соответствующих теорем.

Формула теории 1-го порядка называется *замкнутой,* если она не содержит свободных переменных.

Определение 1. *Если замкнутая формула $\mathfrak{a}$ теории 1-го порядка τ обладает следующим свойством: $\mathfrak{a}$ невыводимо в τ и $\neg\mathfrak{a}$ невыводимо в τ, то $\mathfrak{a}$ называется неразрешимым предложением теории τ.*

Следующую теорему доказал К. Гёдель в 1931 г.

Теорема 1. *Если формальная арифметика S непротиворечива, то в ней существует по крайней мере одно неразрешимой предложение.*

Возникает идея: если нельзя вывести ни это предложение, ни его отрицание, то, может быть, добавив его к аксиомам, получим теорию, не содержащую неразрешимых предложений? Однако, это тоже ничего не даст. Это следует из нижеследующей теоремы, также доказанной Гёделем, для формулировки которой дадим сначала следующее

Определение 2. *Формальная аксиоматическая теория называется эффективно аксиоматизируемой, если существует алгоритм, позволяющий для каждой формулы этой теории определять, является ли она ее аксиомой.*

Теорема 2. *Теорема Гёделя справедлива для каждого непротиворечивого эффективно аксиоматизируемого расширения теории S, то есть каждое такое расширение имеет неразрешимые предложения.*

Эта теорема означает, в частности, что формальное доказательство непротиворечивости арифметики, классического анализа или геометрии невозможно. Одно из важных значений теоремы состоит в том, что она показала невыполнимость программы Гильберта в ее полном виде, однако, возможные модификации этой программы подвергаются полезному обсуждению и до настоящего времени. Прошедшие годы и безусловные достижения математической логики сняли остроту этой проблемы настолько, что большинство математиков, работающих в других областях математики, не уделяют особого внимания тем дискуссиям, которые ведут и ныне специалисты про снованиям математики.

Основным итогом деятельности в области оснований математики можно считать становление математической логики как самостоятельной математической дисциплины, а принципиальным достижением математической логики — разработку современного аксиоматического метода.

5.9. Новые термины. Термы и формулы теорий 1-го порядка. Терм, свободный для переменной в формуле. Исчисление предикатов 1-го порядка. Логические и собственные (специальные) аксиомы. Области интерпретации и модели. Полугруппа. Система аксиом Пеано. Формальная арифметика. Правило индукции. Правило индивидуализации. Замкнутая формула теории 1-го порядка. Неразрешимое предложение теории 1-го порядка. Эффективно аксиоматизируемая теория 1-го порядка.

Глава VII

Основы теории алгоритмов

§ 1. Рекурсивные функции

Интуитивное понятие алгоритма. Отличительные признаки алгоритма. Вычислимые функции. Необходимость уточнения понятия алгоритма. Простейшие функции. Операторы суперпозиции (подстановки), примитивной рекурсии и минимизации. Примитивно рекурсивные и частично рекурсивные функции. Тезис Чёрча.

1.1. Интуитивное понятие алгоритма. Под *алгоритмом* понимают конечную последовательность предписаний (инструкций), точное исполнение которых приводит к решению поставленной задачи (достижению поставленной цели).

Отличительными признаками алгоритма являются следующие.

1. *Дискретность.* Алгоритм представляет собой систему пошаговых (дискретных) предписаний. Исполнение этих предписаний (шагов) осуществляется дискретно, то есть предполагается, что какое-то предписание (шаг) не может быть выполнено, например, наполовину или на одну треть. Каждый шаг является в каждый (дискретный) момент времени исполненным полностью, либо не исполненным совсем.

2. *Детерминированность.* Система получаемых (конструируемых) величин (объектов) после исполнения n-ого шага однозначно определяется системой величин (объектов), полученных (сконструированных) после исполнения каждого из предыдущих $(n-1)$ шагов.

3. *Элементарность шагов.* Закон (правило) получения системы величин (объектов) из предшествующих систем величин (объектов) должен быть достаточно простым.

4. *Направленность (определенность).* Если закон (правило) получения системы величин (объектов) из предшествующих систем не дает результата, то, должно быть указано, что следует считать результатом алгоритма в этом случае.

5. *Массовость.* Допустимой системой величин (объектов) является некоторое бесконечное множество.

Отметим, что в описании алгоритма и его свойств фигурирует масса терминов, точный смысл которых не установлен. Таким образом, понятие алгоритма, определенное выше, нельзя считать строгим. В дальнейшем введенное выше понятие алгоритма будем называть *интуитивным.*

Вычислительные процессы чисто механического характера стали возникать на самых ранних ступенях развития математики. Это, например, алгоритмы получения десятичной записи суммы (разности, произведения, частного) по десятичным записям слагаемых (уменьшаемого и вычитаемого, сомножителей, делимого и делителя); алгоритм нахождения НОД двух целых чисел (двух многочленов); алгоритмы геометрических построений с помощью заданных инструментов и так далее. Немало алгоритмов и в обыденной окружающей нас жизни. Всякий изложенный на приобретенном Вами пакете способ приготовления из данных полуфабрикатов некоего продукта, пригодного к употреблению в пищу, есть не что иное, как алгоритм. Всякая инструкция пользования тем или иным бытовым прибором (например, телефоном-автоматом) есть алгоритм и так далее.

Считая теперь понятие алгоритма интуитивно известным, определим понятие *вычислимой* функции. Определение этого понятия также следует считать нестрогим (интуитивным).

Числовой функцией (частичной числовой функцией) будем называть всякую функцию (частичную функцию) от n переменных, $n \in N$, заданную на множестве всех неотрицательных целых чисел N_0 со значениями в N_0. Таким образом, числовая функция (частичная числовая функция)

f — это отображение множества $\underbrace{N_0 \times \cdots \times N_0}_{n}$ (подмножества $\mathfrak{X}_f$ множества $\underbrace{N_0 \times \cdots \times N_0}_{n}$) в N_0. $\mathfrak{X}_f$ называется областью определения частичной числовой функции f. Область значений числовой функции (частичной числовой функции) f будем обозначать $\mathfrak{Y}_f$. Отметим, что числовая функция f есть частичная числовая функция, для которой $\mathfrak{X}_f = \underbrace{N_0 \times \cdots \times N_0}_{n}$.

Определение 1. *Частичная числовая функция называется вычислимой, если существует алгоритм, позволяющий вычислять ее значения для тех наборов значений аргументов, для которых она определена, и работающий вечно на наборах значений аргументов, для которых эта функция не определена.*

Как правило, отыскание того или иного алгоритма в математике можно свести к нахождению алгоритма, вычисляющего некоторую частичную числовую функцию или хотя бы доказательству принципиальной вычислимости этой функции.

1.2. Необходимость уточнения понятия алгоритма. Период до начала XX столетия можно считать периодом накопления конкретных алгоритмов в математике. Отметим, что интуитивное понятие алгоритма является достаточно ясным и потому среди математиков, как правило, не возникало разногласий по поводу того, является ли данная процедура алгоритмом или не является. Однако, уже в конце XIX века стало интуитивно ясно, что многие задачи об отыскании алгоритмов, по-видимому, не имеют решения. Однако, если для доказательства существования алгоритма достаточно его предъявить, то для доказательства отсутствия алгоритма необходимо иметь его строгое определение. Так как в математике понятие алгоритма тесно связано с понятием вычислимой функции, то впервые строгое определение было дано не самому понятию алгоритма, а понятию вычислимой функции. Говоря более точно, класс вычислимых функций был *формализован* или *аксиоматизирован*. Это было сделано впервые К. Гёделем и, почти одновременно, А. Чёрчем в 1935–1936 годах. При этом класс всех вычислимых функций был формализован точно также, как класс всех тавтологий алгебры высказываний в исчислении высказываний. А именно, были выделены некоторые *простейшие функции*, которые, очевидным образом, являются вычислимыми. Затем введены три правила получения из имеющихся функций новых. Эти правила, примененные к вычислимым функциям, дают в результате функции вычислимые. Такие правила названы *основными вычислимыми операторами*. Таким образом, класс формализованных указанным выше способом функций состоит из вычислимых функций. Возникает вопрос, а всякая ли вычислимая функция попадает в этот класс? Примера интуитивно вычислимой функции не попавшей в указанный класс, не построено. И, более того, дальнейшие исследования в этом направлении позволили выдвинуть гипотезу о том, что таких примеров не существует (тезис Чёрча).

1.3. Простейшие функции. Приступим к построению формализованного класса функций, каждая из которых является вычислимой. Функции из этого класса будем называть *рекурсивными*.

Следующие ниже функции будем называть *простейшими:*

$s(x) = x + 1$ — функция следования,

$o(x) = 0$ — нуль-функция,

$I_m^n(x_1, \ldots x_n) = x_m, 1 \le m \le n$ — проектирующая функция.

Легко понять, что каждая из простейших функций является вычислимой.

1.4. Оператор суперпозиции. Пусть задано n частичных функций от m переменных:

$$\begin{aligned} f_1 &= f_1(x_1, \ldots, x_m), \\ f_2 &= f_2(x_1, \ldots, x_m), \\ &\ldots\ldots\ldots\ldots\ldots, \\ f_n &= f_n(x_1, \ldots, x_m). \end{aligned}$$

и некоторая частичная n-местная функция $f = f(y_1, \ldots, y_n)$. Определим при помощи функций $f, f_1, \ldots, f_n$ новую m -местную частичную функцию $g(x_1, \ldots, x_m)$ следующим образом:

$$g(x_1, \ldots, x_m) = f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)).$$

Говорят, что функция g получена операцией *суперпозиции* или *подстановки* из функций $f, f_1, \ldots, f_n$.

Легко понять, что если функции $f, f_1, \ldots, f_n$ вычислимы, то и функция g также вычислима, то есть результат применения оператора суперпозиции к вычислимым функциям есть функция вычислимая.

Отметим, что в случае, когда $n = m = 1$, мы имеем известную суперпозицию двух одноместных функций (или функцию от функции, или сложную функцию).

Пример 1. n-местная нуль-функция $o(x_1, \ldots, x_n) = 0$ есть суперпозиция функций $o(x) = 0$ и $I_1^n(x_1, \ldots, x_n)$:

$$o(x_1, \ldots, x_n) = o(I_1^n(x_1, \ldots, x_n)).$$

Пример 2. Константная функция одной переменной $f(x) = a$, $a \in N$, есть суперпозиция функций $o(x) = 0$ и $s(x) = x + 1$:

$$\underbrace{s(s(\ldots s}_{a}(o(x)) \ldots) = a$$

1.5. Оператор примитивной рекурсии определим для всякого $n \in N_0$ следующим образом.

Пусть $n > 0$. Говорят, что $(n+1)$-местная частичная функция f получена из данной n-местной функции g и данной $(n+2)$-местной частичной функции h при помощи *оператора примитивной рекурсии*, если эта функция f определяется *схемой примитивной рекурсии*:

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n),$$
$$f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)).$$

Пусть $n = 0$. Говорят, что одноместная частичная функция f получена из данной константной одноместной функции g $(g(x) = a)$ и данной двуместной функции h при помощи оператора примитивной рекурсии, если она определяется схемой примитивной рекурсии:

$$f(0) = a = g(0),$$
$$f(y+1) = h(y, f(y)).$$

Легко понять, что функция f однозначно определяется схемой примитивной рекурсии и функциями g и h.

Предположим теперь, что функции g и h вычислимы. Вычислима ли при этих предположениях функция f?

Пусть $a_1, a_2, \ldots, a_n$, $m \in N_0$. Предположим, что при помощи схемы примитивной рекурсии получена последовательность чисел

$$b_0 = g(a_1, \ldots, a_n),$$
$$b_1 = h(a_1, \ldots, 0, b_0),$$
$$b_2 = h(a_1, \ldots, 1, b_1),$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$b_{m+1} = h(a_1, \ldots, m, b_m).$$

Тогда определено и значение $f(a_1, \ldots, a_n, m+1)$, равное b_{m+1}. Так как g и h вычислимы, то существуют алгоритмы T_g и T_h для g и h, вычисляющие их значения. Тогда b_0 может быть вычислено при помощи алгоритма T_g, b_1 — при помощи алгоритма $T_g T_h$ где $T_g T_h$ — последовательное выполнение алгоритмов T_g и T_h. Понятно, что b_2 может быть вычислено при помощи алгоритма $T_g T_h T_h$ и т. д. и, наконец, b_{m+1} — при помощи алгоритма $T_g \underbrace{T_h \ldots T_h}_{m+1}$. Если же хотя бы одно из чисел $b_0, \ldots, b_{m+1}$ не определено, то один из алгоритмов

$$T_g,\ T_gT_h,\ T_gT_hT_h,\ \ldots,\ T_g\underbrace{T_h\ldots T_h}_{m+1}$$

будет работать вечно. Таким образом, функция f также вычислима и нами показано, фактически, что применение оператора примитивной рекурсии к вычислимым функциям дает в результате функцию вычислимую.

Пример 1. Покажем, что функция $f(x,y)=x+y$ может быть получена из простейших при помощи суперпозиции и примитивной рекурсии. Положим:

$$g(x)=I_1^1(x),$$
$$h(x,y,z)=s(I_3^3(x,y,z)).$$

Тогда:

$$f(x,0)=g(x),$$
$$f(x,z+1)=h(x,z,f(x,z)).$$

Убедитесь в этом самостоятельно.

1.6. Оператор минимизации. Будем говорить, что n-местная, $n\in N$, частичная функция f получена из n-местной частичной функции g при помощи *оператора минимизации* и обозначать

$$f(x_1,\ldots,x_n)=\mu_y[g(x_1,\ldots,x_{n-1},y)=x_n],$$

если выполнено условие: $f(x_1,\ldots,x_n)$ определено и равно y тогда и только тогда, когда

$$g(x_1,\ldots,x_{n-1},0),g(x_1,\ldots,x_{n-1},1),\ldots,g(x_1,\ldots,x_{n-1},y-1)$$

определены и не равны x_n, а $g(x_1,\ldots,x_{n-1},y)=x_n$.

Легко понять, что всякая n-местная частичная функция g и определенный выше оператор минимизации определяют однозначно некоторую n-местную частичную функцию f.

Отметим, что если T — алгоритм, вычисляющий значения функции g, а буква H обозначает алгоритм сравнения двух натуральных чисел, то

$$(TH)(TH)(TH)\ldots$$

есть алгоритм, вычисляющий функцию f. Действительно, если значение функции $f(x_1,\ldots,x_n)$ определено и равно y, то после исполнения следующей части

$$\underbrace{(TH)(TH)\ldots,(TH)}_{y+1}$$

указанного выше алгоритма будет вычислено значение y. Если же $f(x_1,\ldots,x_n)$ не определено, то это значит, что либо $g(x_1,\ldots,x_{n-1},i)$ $(i\in N_0)$ не определено, либо значения $g(x_1,\ldots,y)$ определены для любого $y\in N_0$ и, вместе с тем, $g(x_1,\ldots,x_{n-1},y)\neq x_n$ для любого $y\in N_0$. Это значит, что в первом случае i-я компонента (TH) алгоритма

$$(TH)(TH)(TH)\ldots,$$

будет работать вечно, а во втором случае каждая компонента этого алгоритма на определенном шаге закончит свою работу, но так как сравнение двух натуральных чисел никогда не даст желаемого результата, то весь этот алгоритм будет работать вечно. Таким образом, нами доказано, что применение оператора минимизации к вычислимой функции даст функцию вычислимую.

Пример 1. Покажем, что

$$x-y=\mu_z[y+z=x].$$

Действительно, если $x\geq y$, то все числа $y+0,y+1,\ldots$ определены и одно из них равно x. Если $y+r=x$, то $r=x-y$. Если же $x<y$, то ни одно из чисел $y+0,y+1,\ldots$ не совпадает с x и потому

$$x-y=\mu_z[y+z=x]$$

не определена.

Для одноместной функции $g(x)$ функцию

$$f(x) = \mu_y[g(y) = x]$$

будем обозначать через $f^{-1}(x)$ и называть *обратной* для f (сравните с определениями обратной функции, известными Вам из курсов алгебры, анализа).

1.7. Частично рекурсивные функции. Тезис Чёрча.

Определение 1. *Числовая функция f называется примитивно рекурсивной, если она может быть получена из простейших функций $s(x), o(x), I_m^n(x_1, \ldots, x_n)$ конечным числом операций подстановки и примитивной рекурсии.*

Определение 2. *Частичная функция f называется частично рекурсивной, если она может быть получена из простейших функций $s(x), o(x), I_m^n(x_1, \ldots, x_n)$ конечным числом операций подстановки, примитивной рекурсии и минимизации.*

Отметим, что всякая частично рекурсивная функция является вычислимой функцией, так как нами показана вычислимость простейших функций и показано, что применение операторов подстановки, примитивной рекурсии и минимизации к вычислимым функциям дает функции вычислимые. В связи с этим возникает вопрос: "Всякая ли вычислимая функция является частично-рекурсивной?" До сих пор не построено примеров вычислимых функций, не являющихся частично рекурсивными. Чисто логико-математического доказательства того, что всякая вычислимая функция является частично рекурсивной, не может быть, так как понятие вычислимой функции — интуитивное понятие. А. Чёрч, анализируя идеи и результаты, относящиеся к теории рекурсивных функций и теории алгоритмов вообще, пришел к следующей естественнонаучной гипотезе, известной под названием

Тезис Чёрча. *Класс вычислимых частичных функций совпадает с классом частично рекурсивных функций.*

1.8. Новые термины. Свойства алгоритма: дискретность, детерминированность, элементарность шагов, направленность, массовость. Числовая функция. Частичная числовая функция. Вычислимые функции. Простейшие функции: функция следования, нуль-функция, проектирующие функции. Основные вычислимые операторы: суперпозиции (подстановки), примитивной рекурсии, минимизации. Примитивно рекурсивные функции. Частично рекурсивные функции. Тезис Чёрча.

1.9. Контрольные вопросы.

1. Перечислите отличительные признаки алгоритма. Поясните смысл каждого из них.
2. Перечислите известные Вам алгоритмы из школьной математики. Из курсов алгебры, анализа и геометрии.
3. Дайте определение функции, частичной функции, числовой функции, частичной числовой функции и вычислимой функции.
4. В связи с чем возникла необходимость уточнения понятия алгоритма?
5. Перечислите простейшие функции. Поясните, почему каждая из простейших функций является вычислимой?
6. Дайте определение оператора суперпозиции. Покажите, что этот оператор, примененный к вычислимым функциям, дает вычислимую функцию.
7. Какие функции можно получить из функции следования многократными применениями оператора суперпозиции?

8. Какие функции можно получить из нуль-функции многократными применениями оператора суперпозиции?

9. Какие функции можно получить из проектирующих функций многократными применениями оператора суперпозиции?

10. Дайте определение оператора примитивной рекурсии. Покажите, что применение оператора примитивной рекурсии к вычислимым функциям дает функцию вычислимую.

11. Дайте определение оператора минимизации. Покажите, что применение этого оператора к вычислимой функции дает вычислимую функцию.

12. Дайте определение обратной числовой функции, приведенное в данном параграфе. Найдите функцию, обратную для функции $f(x) = (x-1)(x-3)$

13. Дайте определение примитивно рекурсивной и частично рекурсивной функции.

14. Докажите, что всякая примитивно рекурсивная функция является частично рекурсивной, но не всякая частично рекурсивная функция является примитивно рекурсивной.

15. Докажите, что всякая примитивно рекурсивная функция всюду определена и что не любая частично рекурсивная функция обладает этим свойством.

16. Сформулируйте тезис Чёрча и поясните его смысл.

1.10. Упражнения.

1. Какие функции можно получить многократными применениями оператора суперпозиции к функции следования и нуль-функции? К функции следования и проектирующим функциям? К нуль-функции и проектирующим функциям?

2. Какие функции можно получить многократными применениями оператора суперпозиции к простейшим функциям?

3. Докажите, что функции: $f(x,y) = xy$, $f(x,y) = x^y$ и $f(x) = x!$ являются примитивно рекурсивными.

4. Какие функции получаются при помощи примитивной рекурсии из функций $g(x) = x$ и $h(x,y,z) = z^x$? $g(x) = x$ и $h(x,y,z) = x^z$?

5. Докажите, что: $x : y = \mu_z[yz = x]$. Означает ли это, что функция $f(x,y) = x : y$ является частично рекурсивной? Примитивно рекурсивной?

§ 2. Машины Тьюринга

Определение машины Тьюринга: внешний и внутренний алфавиты, программа. Машинные слова (конфигурации). Переработка машинных слов в машинах Тьюринга. Модель машины Тьюринга. Примеры вычислимых по Тьюрингу функций. Связь вычислимости по Тьюрингу с частичной рекурсивностью. Тезис Тьюринга.

Точное описание класса рекурсивных функций вместе с тезисом Чёрча дает одно из возможных решений об уточнении понятия алгоритма. Однако это решение не вполне прямое, так как понятие вычислимой функции является вторичным по отношению к понятию алгоритма. Спрашивается, нельзя ли уточнить непосредственно само понятие алгоритма и, уже затем, при его помощи определить точно класс вычислимых функций? Это было сделано Постом и Тьюрингом в 1936–1937 гг. независимо друг от друга и почти одновременно с работами Чёрча. Основная мысль Поста и Тьюринга заключалась в том, что алгоритмические процессы — это процессы, которые может совершать подходяще устроенная "машина". В соответствии с этой мыслью ими были описаны в точных математических терминах довольно узкие классы машин, но на этих машинах оказалось возможным осуществить или имитировать все алгоритмические процессы, которые когда-либо описывались математиками. Алгоритмы, осуществимые на упомянутых машинах, было предложено рассматривать как математических "представителей" вообще всех алгоритмов. Было доказано, что класс функций, вычислимых на этих машинах, в точности совпадает с классом всех рекурсивных функций. Тем самым было получено еще одно фундаментальное подтверждение тезиса Чёрча. В настоящее время все алгоритмы этого класса называются просто машинами Тьюринга.

2.1. Определение машины Тьюринга. Машиной Тьюринга T называется тройка множеств $T = \langle A, Q, P\rangle$, где:

$A = A(T) = \{a_0, a_1, \ldots, a_m\}$ — *внешний алфавит* машины T (обычно $a_0 = 0$, $a_1 = 1$);

$Q = Q(T) = \{q_0, q_1, \ldots, q_m\}$ — *алфавит внутренних состояний* или *внутренний алфавит* машины T;

$P = P(T) = \{T(i,j) \mid i = 1, \ldots, n; j = 0, 1, \ldots, m\}$ — *программа* машины T; где $T(i,j)$ — *команды* этой программы, причем, для каждой пары (i,j) существует одна единственная команда $T(i,j)$, которая имеет один из видов:

$$q_i a_j \to q_k a_l,$$
$$q_i a_j \to q_k R,$$
$$q_i a_j \to q_k L.$$

2.2. Машинные слова (конфигурации). *Машинным словом или конфигурацией* называется всякое слово вида $Cq_k a_l B$, где $0 \le k \le n$, $0 \le l \le m$, а C, B — некоторые слова (быть может, пустые) в алфавите A.

Для машинного слова $M = Cq_i a_j B$, $0 \le i \le n$, $0 \le j \le m$, машины Тьюринга T через M'_T обозначим слово, которое получится из слова M по следующим ниже правилам 1–2.

1. Для $i = 0$ $M'_T = M$.
2. Для $i > 0$.
   (a) Если $T(i,j) = (q_i a_j \to q_k a_l)$, то $M'_T = Cq_k a_l B$.
   (b) Если $T(i,j) = (q_i a_j \to q_k R)$, то:
      i. если B не пусто, то $M'_T = Ca_j q_k B$;
      ii. если B пусто, то $M'_T = Ca_j q_k a_0$.
   (c) Если $T(i,j) = (q_i a_j \to q_k L)$, то:
      i. если C не пусто и $C = C_1 a_s$, то $M'_T = C_1 q_k a_s a_j B$;
      ii. если C пусто, то $M'_T = q_k a_0 a_j B$.

Положим:

$$M_T^{(1)} = M'_T;$$
$$M_T^{(n+1)} = (M_T^{(n)})'.$$

Говорят, что машина T *перерабатывает* машинное слово M в M_1, если найдется такое натуральное число n, что $M_T^{(n)} = M_1$. В этом случае будем писать:

$$M \stackrel{T}{\Rightarrow} M_1$$

.

В случае $n = 1$ будем писать также

$$M \models M_1.$$

2.3. Модель машины Тьюринга. Приведенные в п. п. VII.2.1.–VII.2.2. абстрактные понятия проинтерпретируем на идеальной (не реализуемой) "машине".

Пусть имеем некоторое устройство, включающее в себя следующие компоненты: *конечную ленту, управляющую головку, механическое устройство, внешнюю и внутреннюю память, программу.*

Конечная лента разбита на конечное число одинаковых ячеек. Каждая ячейка в каждый момент времени находится в одном из состояний a_i, $i = 0, 1, \ldots, m$, то есть в каждый момент времени в каждой из ячеек записан один из символов алфавита $A = \{a_0, a_1, \ldots, a_m\}$ внешней памяти.

Как правило, символ a_0 считают пустым символом и в качестве a_0 обычно выбирается символ 0. В качестве символа a_1, как правило, выбирается символ 1. В соответствии с правилами, которые будут в дальнейшем приведены, к ленте могут "пристраиваться" ячейки слева или справа. Пристраиваются ячейки в пустом состоянии. Состояние ленты, состоящей из r ячеек, в каждый момент времени описывается словом $a_{j_1}a_{j_2}\ldots a_{j_r}$, где a_{j_s} — символ из A, записанный в s-ой ячейке ленты.

Внешняя память представлена алфавитом $A = \{a_0, a_1, \ldots, a_m\}$ и устройством, способным в соответствующий момент времени вписывать символы из A в ячейки ленты, стирая перед этим их предыдущее содержимое.

Внутренняя память — это алфавит $Q = \{q_0, \ldots, q_n\}$ внутренних состояний машины и устройство, способное менять одно внутреннее состояние машины на другое. В каждый конкретный момент времени машина может находиться в одном и только в одном внутреннем состоянии. Состояние q_0 — особое. Если машина попадает в состояние q_0, то она полностью прекращает свою работу, то есть останавливается. Поэтому q_0 называется также *стоп-символом*, а соответствующее состояние — *стоп-состоянием* или *заключительным состоянием.* q_1 принято называть *исходным* или *начальным* состоянием.

Управляющая головка управляет процессом преобразования машинных слов в машине Тьюринга. В каждый конкретный момент управляющая головка *обозревает (воспринимает)* одну и только одну ячейку ленты. Управляющая головка по соответствующим командам может передвигаться влево или вправо, менять содержимое воспринимаемой ячейки. Если по какой-то команде управляющей головке предписано передвижение влево (вправо) на одну ячейку, а обозреваемая в данный момент ячейка была крайней слева (справа), то механическим устройством (см. ниже) к ленте *"пристраивается слева"* (справа) дополнительная ячейка, в которой записан пустой символ внешнего алфавита.

Программу машины Тьюринга будем трактовать как совокупность команд, в соответствии с которыми осуществляется работа машины.

Механическое устройство пристраивает к ленте по соответствующим командам дополнительные ячейки и (или) передвигает управляющую головку.

2.4. Работа модели машины Тьюринга. Состояние машины Тьюринга определяется состоянием ленты, внутренним состоянием машины и номером обозреваемой ячейки, то есть состояние машины Тьюринга полностью определяется машинным словом $M = Cq_ia_jB$, где Ca_jB — состояние ленты, a_j — обозреваемая ячейка, q_i — внутреннее состояние машины.

Работа машины Тьюринга представляет собой *пошаговый* переход от одного состояния к другому. Один *шаг* или *такт* — это переход от машинного слова M к M'_T, см. п. VII.2.2. Этот переход осуществляется по нижеследующим правилам 1–2.

1. При $i = 0$, $M'_T = M$. Это означает, что если машина попала в состояние q_0, то она считается остановившейся. Если же в машине не происходит изменений в состоянии, отличном от q_0, то будем говорить, что машина *работает вечно.*

2. Пусть $i > 0$.

   (a) Если $T(i,j) = (q_i a_j \to q_k a_l)$. Внутреннее состояние машины q_i заменяется на q_k (возможно, $q_i = q_k$). Содержимое обозреваемой ячейки a_j заменяется на a_l (возможно, $a_j = a_l$).

   (b) Если $T(i,j) = (q_i a_j \to q_k R)$, то внутреннее состояние q_i заменяется на q_k и управляющая головка сдвигается вправо на одну ячейку, при этом, возможно, пристраивается справа одна ячейка в пустом состоянии.

   (c) Если $T(i,j) = (q_i a_j \to q_k L)$. Осуществляется все то, что в предыдущем пункте с заменой "право" на "лево".

Таким образом, с математической точки зрения машина Тьюринга — это определенный алгоритм для переработки машинных слов.

Пример 1. Пусть $T = \langle A, Q, P\rangle$, где: $A = \{0,1\}$, $Q = \{q_0, q_1, q_2\}$,

P: $q_1 0 \to q_2 R$, $q_1 1 \to q_1 R$,
$q_2 0 \to q_0 1$, $q_2 1 \to q_2 R$.

Имеем:
1) $q_1 110 \models 1 q_1 10 \models 11 q_1 0 \models 110 q_2 0 \models 110 q_0 1$.
2) $q_1 0110 \models 0 q_2 110 \models 01 q_2 10 \models 011 q_2 0 \models 011 q_0 1$.
Это означает, что: $q_1 110 \Rightarrow 110 q_0 1$ и $q_1 0110 \to 011 q_0 1$.
Легко понять, что:

$$q_1 01110 \Rightarrow 0111 q_0 1$$
$$q_1 011110 \Rightarrow 01111 q_0 1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$q_1 0 \underbrace{1\ldots1}_{n} 0 \Rightarrow 0 \underbrace{1\ldots1}_{n} q_0 1.$$

Пример 2. Пусть $T = \langle A, Q, P\rangle$, где $A = \{0,1\}$, $Q = \{q_0, q_1, q_2, q_3\}$,

P: $q_1 0 \to q_2 R$, $q_2 1 \to q_2 R$,
$q_1 1 \to q_1 R$, $q_3 0 \to q_3 L$,
$q_2 0 \to q_3 L$, $q_3 1 \to q_0 0$.

Имеем:
1) $q_1 00 \models 0 q_2 0 \models q_3 00 \models q_3 000 \models q_3 0000 \models \ldots$ Таким образом, в этом случае машина работает вечно.
2) $q_1 010 \models 0 q_2 10 \models 01 q_2 0 \models 0 q_3 10 \models 0 q_0 00$, то есть $q_1 010 \Rightarrow 0 q_0 00$.
Легко понять, что:

$$q_1 010 \Rightarrow 0 q_0 00$$
$$q_1 0110 \Rightarrow 01 q_0 00$$
$$q_1 01110 \Rightarrow 011 q_0 00$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$q_1 0 \underbrace{1\ldots1}_{n} 10 \Rightarrow 0 \underbrace{1\ldots1}_{n} q_0 00$$

Следует понимать, что машина Тьюринга является абстрактным математическим объектом и представляет собой просто определенный алгоритм для переработки слов в некотором алфавите.

2.5. Вычислимые по Тьюрингу функции. В дальнейшем будем пользоваться обозначением

$$a_i^x = \underbrace{a_i a_i \dots a_i}_{x}.$$

Определение 1. *Будем говорить, что машина Тьюринга T вычисляет n-местную частичную числовую функцию $f(x_1, x_2, \dots, x_n)$, если выполнены следующие условия:*

1. Если $f(x_1, x_2, \dots, x_n)$ определено, то

$$q_1 0 1^{x_1} 0 1^{x_2} 0 \dots 0 1^{x_n} 0 \overset{T}{\Rightarrow} C q_0 B,$$

где C, B — некоторые слова в алфавите $\{0, 1\}$, причем Cq_0B содержит $f(x_1, x_2, \dots, x_n)$ вхождений символа 1.

2. Если $f(x_1, x_2, \dots, x_n)$ не определено, то машина T, начиная работу со слова

$$M = q_1 0 1^{x_1} 0 1^{x_2} 0 \dots 0 1^{x_n} 0,$$

работает вечно.

Частичная числовая функция называется *вычислимой по Тьюрингу*, если существует машина Тьюринга T, вычисляющая эту функцию.

Отметим, что машина Тьюринга из примера 2.4.1 вычисляет функцию $f(x) = x + 1$, а из примера 2.4.2 — частичную функцию $f(x) = x - 1$.

Определение 2. *Будем говорить, что машина Тьюринга T правильно вычисляет n-местную частичную числовую функцию $f(x_1, x_2, \dots, x_n)$, если выполнены следующие условия:*

1. Если $f(x_1, x_2, \dots, x_n)$ определено, то

$$q_1 0 1^{x_1} 0 1^{x_2} 0 \dots 0 1^{x_n} 0 \overset{T}{\Rightarrow} q_0 1^{f(x_1, x_2, \dots, x_n)} 0 \dots 0$$

и при этом не достраивает ячеек слева.

2. Если $f(x_1, x_2, \dots, x_n)$ не определено, то машина T, начиная работу со слова

$$M = q_1 0 1^{x_1} 0 1^{x_2} 0 \dots 0 1^{x_n} 0,$$

работает вечно.

Пример 1. Пусть $T = \langle A, Q, P \rangle$, где: $A = \{0, 1\}$, $Q = \{q_0, q_1, q_2, q_3, q_4, q_5\}$,

P: $q_1 1 \to q_2 R$, $q_1 0 \to q_2 R$, $q_2 1 \to q_2 R$
$q_2 0 \to q_3 1$, $q_3 1 \to q_3 R$, $q_3 0 \to q_4 L$
$q_4 1 \to q_4 0$, $q_4 0 \to q_5 L$, $q_5 1 \to q_5 L$
$q_5 0 \to q_0 0$.

Убедитесь самостоятельно, что эта машина Тьюринга правильно вычисляет числовую функцию $f(x, y) = x + y$.

Частичная числовая функция называется *правильно вычислимой по Тьюрингу*, если существует машина Тьюринга T, вычисляющая эту функцию.

Мы видим, что понятие правильно вычислимой по Тьюрингу функции является более строгим, чем понятие вычислимой по Тьюрингу функции. Оно используется, как правило, для того, чтобы полученную для вычисления данной функции машину Тьюринга можно было корректно использовать в композиции с другими машинами для построения более сложных машин Тьюринга на основе более простых.

Приведем без доказательства теорему, связывающую понятия частично рекурсивной функции и машины Тьюринга.

Теорема 1. *Частичная числовая функция является частично рекурсивной тогда и только тогда, когда она вычислима по Тьюрингу.*

Данная теорема позволяет сделать вывод об эквивалентности определений понятия алгоритма в форме рекурсивной функции и в форме машины Тьюринга. Кроме того, она является косвенным подтверждением тезиса Чёрча и эквивалентного ему тезиса Тьюринга.

Тезис Тьюринга. Класс вычислимых частичных числовых функций совпадает с классом функций, вычислимых по Тьюрингу.

2.6. Новые термины. Машина Тьюринга. Внешний и внутренний алфавит. Внутреннее состояние машины. Заключительное или стоп-состояние. Программа и команды машины Тьюринга. Машинное слово (конфигурация). Переработка машинных слов в машине Тьюринга. Модель машины Тьюринга. Конечная лента. Управляющая головка. Механическое устройство. Такт (шаг) работы машины Тьюринга. Вечность работы. Вычислимые и правильно вычислимые по Тьюрингу функции. Тезис Тьюринга.

2.7. Контрольные вопросы.

1. Могут ли в машине Тьюринга быть две команды вида:
   (a) $q_i a_j \to q_k a_l$ и $q_i a_j \to q_s R$;
   (b) $q_i a_j \to q_k a_l$ и $q_i a_j \to q_s a_t$;
   (c) $q_i a_j \to q_k a_l$ и $q_i a_r \to q_s L$.
2. Могут ли в машине Тьюринга быть команды вида:
   (a) $q_i a_j \to q_i R$;
   (b) $q_i a_j \to q_k a_j$;
   (c) $q_i a_j \to q_i a_j$;
   (d) $q_i a_j \to q_i L$;
   (e) $q_0 a_j \to q_0 a_j$;
   (f) $q_0 a_j \to q_k R$.
3. Истинны ли высказывания для некоторой машины Тьюринга T и машинного слова M:
   (a) $M \Rightarrow M'_T$;
   (b) $M \models M'_T$;
   (c) $M \Rightarrow M_T^{(3)}$;
   (d) $M \models M_T^{(3)}$.
4. Дайте определение состояния ячейки, ленты, машины Тьюринга.
5. Дайте определение машинного слова.
6. Опишите понятие шага машины Тьюринга.
7. Можно ли процесс преобразования машинных слов назвать непрерывным? Почему?
8. Что значит термин “данная машина Тьюринга T вычисляет числовую функцию f”?
9. Дайте определение вычислимой и правильно вычислимой по Тьюрингу функции.
10. Обоснуйте эквивалентность тезисов Чёрча и Тьюринга.

2.8. Упражнения.

1. Подсчитайте максимально возможное количество команд в программе машины Тьюринга с алфавитами
$$A = \{a_0, a_1, \ldots, a_m\} \text{ и } Q = \{q_0, q_1, \ldots, q_n\}.$$

2. Программа машины T состоит из одной команды: $q_1 0 \to q_0 0$. Какие функции
$$f_1(x), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots x_n), \ldots$$
вычисляет эта машина?

3. Постройте машину Тьюринга, правильно вычисляющую функции $o(x) = 0$, $s(x) = x + 1$, $I_2^3(x_1, x_2, x_3) = x_2$.

4. Докажите вычислимость по Тьюрингу частичных числовых функций $f(x) = x - 2$, $g(x) = = x - y$.

§ 3. Нормальные алгоритмы Маркова

Марковские подстановки. Схема нормального алгоритма. Нормальные алгоритмы Маркова. Нормально вычислимые функции. Принцип нормализации Маркова. Эквивалентность определения алгоритма в форме нормальных алгоритмов Маркова определениям в форме рекурсивных функций и машины Тьюринга.

3.1. Марковские подстановки. Пусть $\mathfrak{X}$ — некоторый алфавит, $F_0(\mathfrak{X})$ — множество всех слов в алфавите $\mathfrak{X}$, включая и пустое слово, которое будем обозначать через $\mathbb{I}$.

Пусть $A, B \in F_0(\mathfrak{X})$. Будем говорить, что слово B является *подсловом* слова A, если для некоторых слов $B_1, B_2 \in F_0(\mathfrak{X})$ выполняется равенство:

$$A = B_1 B B_2.$$

Тройка $\langle B_1, B, B_2 \rangle$ называется *вхождением слова B в слово A.*

Пример 1. Пусть $\mathfrak{X}$ — русский алфавит (кириллица), $A =$ абракадабра, $B =$ бра. Видим, что B имеет два вхождения в A:
первое — $\langle$ а, бра, кадабра $\rangle$;
второе — $\langle$ абракада, бра, $\mathbb{I}\rangle$.

Пусть $\mathfrak{X}$ — произвольный фиксированный алфавит. Для тройки слов A, B, C из $F_0(\mathfrak{X})$ обозначим через

$$\mathrm{Sub}_B^C(A)$$

слово, полученное из A заменой первого вхождения слова B в A на слово C, если B является подсловом слова A. Если же B не является подсловом слова A, то будем считать, что выражение $\mathrm{Sub}_B^C(A)$ не определено.

Пример 2. $\mathrm{Sub}^{\mathbb{I}}_{\text{бра}}$(абракадабра) = акадабра,
$\mathrm{Sub}^{\text{л}}_{\text{бра}}$(абракадабра) = алкадабра,
$\mathrm{Sub}^{\text{бра}}_{\text{бра}}$(абракадабра) = абракадабра,
$\mathrm{Sub}^{\text{бра}}_{\text{бре}}$(абракадабра) не определено,
$\mathrm{Sub}^{\text{ж}}_{\mathbb{I}}$(абракадабра) = жабракадабра.

Отметим, что $\mathrm{Sub}_B^C(A)$ есть частичная трехместная операция на $F_0(\mathfrak{X})$. Если же слова B и C зафиксированы, то $\mathrm{Sub}_B^C(A)$, $A \in F_0(\mathfrak{X})$ есть *частичная одноместная* операция на $F_0(\mathfrak{X})$. Будем ее обозначать формулой вида:

$$B \to C$$

и называть *марковской подстановкой* на $F_0(\mathfrak{X})$, а само выражение $B \to C$ — *формулой* данной *марковской подстановки.*

При этом B будем называть *левой частью* (*посылкой*), а C — *правой частью* (*заключением*) данной марковской подстановки. Если $\mathrm{Sub}_B^C(A)$ не определено, то будем говорить, что формула $B \to C$ не применима к слову A.

Определение 1. *Схемой нормального алгоритма в алфавите $\mathfrak{X}$ называется последовательность вида:*

$$\begin{cases} B_1 & \to & C_1\alpha_1, \\ B_2 & \to & C_2\alpha_2, \\ \dots & \dots & \dots\dots \\ B_s & \to & C_s\alpha_s, \end{cases} \tag{1}$$

где $B_i \to C_i$, $i = 1, \dots, s$, — некоторые формулы марковских подстановок в $F_0(\mathfrak{X})$, а $\alpha_1, \dots, \alpha_s \in$ $\in \{\mathbb{I}, *\}$. При этом подстановку $B_i \to C_i\alpha_i$ будем называть *заключительной,* если $\alpha_i = *$.

3.2. Определение нормального алгоритма Маркова. Пусть дан некоторый алфавит $\mathfrak{X}$ и некоторая схема (1) нормального алгоритма в этом алфавите.

Нормальным алгоритмом Маркова (н. а. М.) в алфавите $\mathfrak{X}$, определенным схемой (1), называется описываемый процесс построения последовательности слов A_i, $i = 0, 1, \ldots$, исходя из данного слова A.

1. Если $i = 0$, то полагаем $A_0 = A$ и считаем, что процесс построения последовательности слов еще не завершен.

2. Пусть $i \geq 0$, слова $A_0, \ldots, A_i$ построены и процесс построения слов еще не завершился. Тогда:

   (a) если каждая из подстановок схемы (1) неприменима к слову A_i, то полагаем $A_{i+1} = A_i$, процесс построения слов считаем завершенным и слово A_{i+1} считаем результатом применения н. а. М. к слову A;

   (b) если среди подстановок схемы (1) есть применимые к слову A_i, то A_{i+1} есть слово, полученное из A_i применением первой применимой к нему подстановки из схемы (1); при этом, если эта подстановка была заключительной, то процесс построения слов считается завершенным и A_{i+1} считается результатом применения н. а. М. к слову A; если же примененная подстановка не являлась заключительной, то процесс построения последовательности слов считается незавершенным.

Таким образом, если н. а. М., примененный к слову A, завершается на слове B, то говорят, что н. а. М. *перерабатывает* слово A в слово B. Если же н. а. М., примененный к слову A, никогда не завершается, то говорят, что данный н. а. М. *неприменим* к слову A. В дальнейшем будем писать $A_i \Rightarrow A_{i+1}$.

3.3. Примеры нормальных алгоритмов Маркова. 1. Пусть $\mathfrak{X} = \{x_1, x_2, \ldots, x_n\}$. Рассмотрим схемы н. а. М.:

$$\begin{cases} x_1 \to \mathbb{I} \\ \mathbb{I} \to \mathbb{I}* \end{cases} \tag{2}$$

$$\begin{cases} \mathbb{I} \to \mathbb{I}* \\ x_1 \to \mathbb{I} \end{cases} \tag{2'}$$

$$\begin{cases} x_1 \to x_2 \\ \mathbb{I} \to \mathbb{I}* \end{cases} \tag{3}$$

$$\begin{cases} x_1 \to x_1* \\ \mathbb{I} \to \mathbb{I}* \end{cases} \tag{4}$$

$$\begin{cases} x_1 \to x_1x_1 \\ \mathbb{I} \to \mathbb{I}* \end{cases} \tag{5}$$

Отметим, что н. а. М. (2) всякое слово A, содержащее вхождения буквы x_1, перерабатывает в слово A', полученное из A вычеркиванием всех вхождений буквы x_1. Если же слово B не содержит вхождений буквы x_1, то н. а. М. (2) перерабатывает его в себя. Н. а. М. (2′) перерабатывает всякое слово в себя.

Н. а. М. (3) перерабатывает слова, не содержащие в своей записи буквы x_1, в себя, а содержащие — в слова, получающиеся из исходных заменой всех вхождений буквы x_1 на букву x_2.

Н. а. М. (4) всякое слово перерабатывает в себя.

Н. а. м. (5) всякое слово, не содержащее вхождений буквы x_1, перерабатывает в себя. К остальным словам он не применим. Действительно,

$$x_2x_1x_3x_1 \Rightarrow x_2x_1x_1x_3x_1 \Rightarrow x_2x_1x_1x_1x_3x_1 \Rightarrow x_2x_1x_1x_1x_1x_3x_1 \Rightarrow \ldots$$

2. Пусть $n, m \in N_0$, $m > 1$. Рассмотрим н. а. М. в алфавите $\{1\}$:

$$\begin{cases} \underbrace{11\ldots1}_{m} & \to & \mathbb{I} \\ \underbrace{11\ldots1}_{m-1} & \to & \mathbb{I}* \\ \underbrace{11\ldots1}_{m-2} & \to & \mathbb{I}* \\ & \ldots & \\ 1 & \to & \mathbb{I}* \\ \mathbb{I} & \to & 1* \end{cases}$$

Легко понять, что данный н. а. М. перерабатывает всякое слово $\underbrace{11\ldots1}_{n} = 1^n$ в 1, если $n \vdots m$, и в $\mathbb{I}$, если n не делится на m.

3.4. Нормально вычислимые функции.

Определение 1. *Частичная функция f, заданная на множестве слов в алфавите $\mathfrak{X}$ (словарная функция), называется нормально вычислимой, если найдется такое расширение $\overline{\mathfrak{X}}$ ($\overline{\mathfrak{X}} \supseteq \mathfrak{X}$) алфавита $\mathfrak{X}$ и такой н. а. М., который всякое слово A из области определения функции f перерабатывает в слово $f(A)$ и который неприменим к словам из $F(\mathfrak{X})$, не входящим в область определения функции f.*

На основе определения нормально вычислимой словарной функции можно дать определение нормально вычислимой частичной числовой функции, например, нижеследующим образом.

Определение 2. *Частичная числовая функция $f(x_1, \ldots, x_n)$ называется нормально вычислимой, если найдется такое расширение $\overline{\mathfrak{X}}$ алфавита $\mathfrak{X} = \{0, 1\}$ и такой н. а. М. P, который*

1) если $f(x_1, \ldots, x_n)$ определено, то

P слово $01^{x_1}0\ldots01^{x_n}0$ перерабатывает в слово $01^{f(x_1,\ldots,x_n)}0$ (по-прежнему $1^0 = \mathbb{I}$);

2) если же $f(x_1, \ldots, x_n)$ не определено, то н. а. М. P неприменим к слову $01^{x_1}0\ldots01^{x_n}0$.

Пример 1. В алфавите $\{1\}$ н. а. М. $\{\mathbb{I} \to 1*$ нормально вычисляет словарную функцию $f(1^x) = = 1^{x+1}$.

Пример 2. Числовая функция следования $s(x) = x + 1$ является нормально вычислимой, так как существует н. а. М., удовлетворяющий определению:

$$\begin{cases} 1 & \to & 11* \\ 0 & \to & 01* \end{cases}$$

Пример 3. Покажем, что функция $f(x, y) = x + y$ является нормально вычислимой. Рассмотрим н. а. М., определяемый схемой:

$$\begin{cases} 101 & \to & 11* \\ 001 & \to & 01*. \\ 100 & \to & 10*. \\ 000 & \to & 00*. \end{cases}$$

Очевидно, что

$$0\underbrace{11\ldots1}_{x}0\underbrace{11\ldots1}_{y}0 \Rightarrow 0\underbrace{11\ldots1}_{x+y}0$$

Это и означает, что рассмотренный н. а. М. нормально вычисляет функцию $f(x, y) = x + y$.

Пример 4. Легко убедиться в том, что схема н. а. М.:

$$
\begin{array}{lll}
0b \to 1* & a0 \to 0a & 0a \to 0b \\
1b \to 2* & a1 \to 1a & 1a \to 1b \\
2b \to 3* & a2 \to 2a & 2a \to 2b \\
3b \to 4* & a3 \to 3a & 3a \to 3b \\
4b \to 5* & a4 \to 4a & 4a \to 4b \\
5b \to 6* & a5 \to 5a & 5a \to 5b \\
6b \to 7* & a6 \to 6a & 6a \to 6b \\
7b \to 8* & a7 \to 7a & 7a \to 7b \\
8b \to 9* & a8 \to 8a & 8a \to 8b \\
9b \to b0 & a9 \to 9a & 9a \to 9b \\
b \to 1* & & \mathbb{I} \to a
\end{array}
$$

нормально вычисляет функцию $f(x) = x + 1$ в десятиричной системе счисления (в алфавите $\mathfrak{X} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$). Здесь в качестве расширения $\overline{\mathfrak{X}}$ алфавита $\mathfrak{X}$ рассматривается алфавит $\overline{\mathfrak{X}} = \mathfrak{X} \bigcup \{a, b\}$.

3.5. Принцип нормализации Маркова. Создателем теории нормальных алгоритмов является советский математик А. А. Марков (1903–1979). Им была выдвинута естественнонаучная гипотеза, подобная тезисам Чёрча и Тьюринга. Она получила название *принцип нормализации Маркова.*

Принцип нормализации Маркова. *Частичная числовая функция является вычислимой тогда и только тогда, когда она является нормально вычислимой.*

Отметим, что А. А. Марковым же доказано, что класс нормально вычислимых функций совпадает с классом частично рекурсивных функций (и, следовательно, с классом вычислимых по Тьюрингу функций). Из этого результата вытекает эквивалентность принципа нормализации Маркова тезисам Чёрча и Тьюринга. Это означает, что теории рекурсивных функций, машин Тьюринга и нормальных алгоритмов Маркова равносильны. В разное время в разных станах ученые независимо друг от друга, изучая интуитивное понятие алгоритма и алгоритмической вычислимости, создали теории, описывающие данное понятие, которые оказались равносильными. Если бы один из этих классов оказался шире какого-либо другого, то соответствующий тезис Чёрча, Тьюринга или Маркова был бы опровергнут. Например, если бы класс нормально вычислимых функций оказался шире класса рекурсивных функций, то существовала бы нормально вычислимая, но не рекурсивная функция. В силу ее нормальной вычислимости и принципа нормализации Маркова она была бы алгоритмически вычислима в интуитивном понимании алгоритма, и предположение об ее нерекурсивности опровергало бы тезис Чёрча. Однако эти классы функций совпадают, что служит еще одним косвенным подтверждением тезисов Чёрча, Тьюринга и принципа нормализации Маркова. Отметим, что существуют еще и другие варианты теорий алгоритмов, формализующих интуитивное понятие алгоритма, и для всех них также доказана их равносильность с рассмотренными теориями.

3.6. Новые термины. Подслова и вхождения слов в другие слова. Марковская подстановка, формула марковской подстановки. Применимые и неприменимые подстановки к данному слову. Заключительные подстановки. Схема нормального алгоритма. Нормальный алгоритм (Маркова), определяемый данной схемой. Переработка н. а. М. одного слова в другое. Применимый и неприменимый н. а. М. к данному слову. Нормально вычислимые функции. Принцип нормализации Маркова.

3.7. Контрольные вопросы.

1. Сколько вхождений имеет слово *aa* в слово *aaaa*?

2. Найдите: $\mathrm{Sub}^{\mathbb{I}}_{a}$(абракадабра), $\mathrm{Sub}^{\mathbb{I}}_{\text{аб}}(\mathrm{Sub}^{\mathbb{I}}_{\text{адабра}}$(абракадабра)), $\mathrm{Sub}^{\mathbb{I}}_{\text{ам}}$(ама), $\mathrm{Sub}^{\mathbb{I}}_{\text{р}}$(амбар), $\mathrm{Sub}^{\text{л}}_{\text{р}}$(амбар), $\mathrm{Sub}^{\text{уг}}_{\text{амб}}$(амбар), $\mathrm{Sub}^{\mathbb{I}}_{\text{раб}}$(амбар), $\mathrm{Sub}^{\mathbb{I}}_{\text{бар}}$(амбар).

3. Изменится ли н. а. М., если в определяющей его схеме две подстановки поменять местами?

4. Известно, что процесс построения последовательности слов в данном н. а. М. исходя из данного слова A никогда не завершается. Что можно сказать по этому поводу?

5. Ни одна из подстановок схемы, определяющей н. а. М. неприменима к слову A. Что является результатом применения н. а. М. к слову A?

3.8. Упражнения.

1. Постройте схемы для нормального вычисления частичных числовых функций: $o(x) = 0$; $f(x, y) = x$; $f(x, y) = y$; $f(x, y, z) = x$; $f(x, y, z) = z$; $f(x, y, z) = y$.

2. Докажите нормальную вычислимость функций: $f(x) = 2x$; $f(x) = x - 1$; $f(x) = x - 1$; $f(x) = x - 2$; $f(x) = x - 2$; $f(x) = x - y$.

3. Докажите, что суперпозиция нормально вычислимых функций нормально вычислима.

4. Докажите эквивалентность принципа нормализации Маркова тезисам Чёрча и Тьюринга.

§ 4. Алгоритмически неразрешимые проблемы

Алгоритмические проблемы. Невычислимые функции. Рекурсивные множества. Проблема общезначимости формул алгебры предикатов. Диофантовы уравнения.

Алгоритмическая проблема — это проблема, в которой требуется найти единый метод (алгоритм) для решения бесконечной серии однотипных задач. Такие проблемы возникали и решались в различных областях математики на протяжении всей ее истории. Примеры таких проблем рассматривались в § 1.

Уже отмечалось, что в начале XX века у математиков начали появляться подозрения, что некоторые алгоритмические проблемы не имеют решения. В связи с этим возникла необходимость дать точное определение самому понятию алгоритма. Мы познакомились с несколькими способами такого уточнения, и в этом параграфе приведем примеры алгоритмически неразрешимых проблем.

4.1. Невычислимые функции. Пусть $\mathfrak{K}_{\text{чр}}$, $\mathfrak{K}_{\text{вт}}$, $\mathfrak{K}_{\text{нв}}$ — классы частичных числовых функций: всех частично рекурсивных, всех вычислимых по Тьюрингу и всех нормально вычислимых соответственно. В соответствии с теоремой 2.5.1 и п. VII.3.4. все эти классы совпадают:

$$\mathfrak{K}_{\text{чр}} = \mathfrak{K}_{\text{вт}} = \mathfrak{K}_{\text{нв}}$$

Если $\mathfrak{K}_{\text{ив}}$ — класс всех интуитивно вычислимых частичных числовых функций, то в соответствии с тезисом Черча (тезисом Тьюринга, принципом нормализации Маркова) имеем:

$$\mathfrak{K}_{\text{ив}} = \mathfrak{K}_{\text{чр}} = \mathfrak{K}_{\text{вт}} = \mathfrak{K}_{\text{нв}}.$$

Условимся частичные числовые функции представлять "словарными" функциями в алфавите $\{0, 1\}$. Например, если

$$f(x_1, x_2, \ldots, x_n) = y,$$

то соответствующую словарную функцию, которую обозначим той же буквой f, определим так:

$$f(\underbrace{11\ldots1}_{x_1}0\underbrace{11\ldots1}_{x_2}0\ldots0\underbrace{11\ldots1}_{x_n}) = \underbrace{11\ldots1}_{y}.$$

Если f — нормально вычислимая функция, то есть $f \in \mathfrak{K}_{\text{нв}}$, то существует н. а. М., определяемый схемой

$$\begin{cases} B_1 & \to & C_1\alpha_1, \\ B_2 & \to & C_2\alpha_2, \\ \ldots & \ldots & \ldots\ldots \\ B_s & \to & C_s\alpha_s, \end{cases}$$

в некотором расширении $\{0, 1\} \bigcup \mathfrak{X}_f$ алфавита $\{0, 1\}$, где $\alpha_i \in \{*, \mathbb{I}\}$, который слово

$$\underbrace{11\ldots1}_{x_1}0\underbrace{11\ldots1}_{x_2}0\ldots0\underbrace{11\ldots1}_{x_n}$$

перерабатывает в слово

$$\underbrace{11\ldots1}_{y=f(x_1,\ldots,x_n)}.$$

Для каждой нормально вычислимой функции f схема н. а. М. содержит конечное число подстановок, каждая из которых содержит конечное число символов. Таким образом, множество $\mathfrak{X}_f$, конечно, для всякой нормально вычислимой функции. Так как обозначение символов $\mathfrak{X}_f$ не имеет значения (лишь бы они были отличны от уже используемых символов $0, 1, \to$, ",", $\star$), то взяв в качестве $\mathfrak{X}_f$ для всех f одно и то же счетное множество $\mathfrak{X} = \{x_1, x_2, \ldots\}$, всякий н. а. М., вычисляющий некоторую нормально вычислимую функцию, можно записать в виде слова (конечной последовательности символов) в алфавите:

$$I = \mathfrak{X} \bigcup \{0, 1, \to, \text{“,”}\ \star\},$$

который, очевидно, счетен. Это значит, что множество всех н. а. М., вычисляющих нормально вычислимые частичные числовые функции, является счетным.

Таким образом, класс $\mathfrak{K}_{\text{НВ}}$ нормально вычислимых частичных числовых функций счетен. Но множество всех частичных числовых функций имеет мощность континуума. Это означает, что существуют частичные числовые функции, не являющиеся нормально вычислимыми и, следовательно, не являющиеся рекурсивными и не являющиеся вычислимыми по Тьюрингу. Такие числовые функции назовем *невычислимыми.*

4.2. Пример невычислимой функции. Так как нормально вычислимых функций счетное множество, то перенумеруем все эти функции. Таким образом, всякая нормальная функция имеет некоторый номер. Пусть $\varphi_0, \varphi_1, \varphi_2, \ldots$ — все нормально вычислимые функции. Определим числовую функцию f следующим образом:

$$f(x) = \begin{cases} \varphi_x(x) + 1, & \text{если } \varphi_x(x) \text{ определено,} \\ 1, & \text{если } \varphi_x(x) \text{ не определено.} \end{cases}$$

Если предположить, что функция $f(x)$ нормально вычислима, то получим, что $f(x) = \varphi_k(x)$ для некоторого $k \in N_0$. Так как $f(x)$ всюду определена, то и $\varphi_k(x)$ определена всюду на N_0. Тогда

$$f(k) = \varphi_k(k).$$

Но по определению функции $f(x)$ имеем:

$$f(k) = \varphi_k(k) + 1.$$

Из двух последних равенств получаем противоречивое равенство:

$$\varphi_k(k) = \varphi_k(k) + 1.$$

Таким образом, определенная выше функция $f(x)$ не является нормально вычислимой, и потому не является вычислимой по Тьюрингу и частично рекурсивной, то есть для вычисления всех ее значений не существует алгоритма.

4.3. Рекурсивные множества.

Определение 1. *Пусть $A \subseteq N_0$. Числовая функция*

$$\chi_A = \begin{cases} 0, & \text{если } x \in A \\ 1, & \text{если } x \notin A \end{cases}$$

называется характеристической функцией множества A.

Пример 1.

1. Если $A = \varnothing$, то $\chi_\varnothing(x) = 1$.
2. Если $A = N_0$, то $\chi_{N_0}(x) = 0$.

Определение 2. *Числовое множество $A \subseteq N_0$ называется рекурсивным, если его характеристическая функция χ_A является рекурсивной.*

Множество, не являющееся рекурсивным называется *нерекурсивным.*

Пример 2.

1. Из примера 4.3.1 видно, что пустое множество и множество N_0 являются рекурсивными, так как их характеристические функции являются рекурсивными. В самом деле, $\chi_\varnothing(x) = 1 = s(o(x))$ и $\chi_{N_0}(x) = 0 = o(x)$, где $o(x)$ и $s(x)$ — простейшие функции.
2. Пусть $A = \{a_1, a_2, \ldots, a_n\}$ — произвольное конечное множество. Покажем, что оно является рекурсивным.

Легко понять, что его характеристическая функция есть

$$\chi_A(x) = \operatorname{Sg}|x-a_1| \cdot \operatorname{Sg}|x-a_2| \cdot \ldots \cdot \operatorname{Sg}|x-a_n|, \text{ где } \operatorname{Sg}(x) = \begin{cases} 1, & \text{если } x > 0 \\ 0, & \text{если } x = 0. \end{cases}$$

Действительно, если $x \in A$, то $x = a_k$, где $a_k \in A$. Следовательно, $\operatorname{Sg}|x-a_k| = 0$, а поэтому и $\chi_A(x) = 0$. Если же $x \notin A$, то $\operatorname{Sg}|x-a_i| = 1$ для всех $i = 1, \ldots, n$. Значит, в этом случае, $\chi_A(x) = 1$.

Покажем, что $\chi_A(x)$ является примитивно рекурсивной, а значит и рекурсивной. Видно, что функция $\chi_A(x)$ получена при помощи суперпозиций из функций xy, $\operatorname{Sg}(x)$ и $|x-y|$. Покажем теперь, что каждая из этих функций является примитивно рекурсивной.

а) Формулы

$$x \cdot 0 = 0 = o(x)$$
$$x(y+1) = xy + x = I_1^3(x, y, xy) + xy$$

показывают, что функция xy получена при помощи оператора примитивной рекурсии из примитивно рекурсивных функций (функция $x+y$ является примитивно рекурсивной, см. пример 1.5.1), а значит является примитивно рекурсивной.

б) Формулы

$$\operatorname{Sg}(0) = 0 = o(x)$$
$$\operatorname{Sg}(x+1) = 1 = s(o(x))$$

показывают, что функция $\operatorname{Sg}(x)$ получена при помощи оператора примитивной рекурсии из примитивно рекурсивных функций, а значит является примитивно рекурсивной.

в) Заметим, что $|x-y| = (x \dot{-} y) + (y \dot{-} x)$, где функция

$$x \dot{-} y = \begin{cases} x-y, & \text{если } x \geq y \\ 0, & \text{если } x < y \end{cases}$$

называется *усеченной разностью.*

Формулы

$$x \dot{-} 0 = x = I_1^1(x)$$
$$x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1 = I_3^3(x, y, x \dot{-} y) \dot{-} 1$$

показывают, что функция $x \dot{-} y$ получена при помощи оператора примитивной рекурсии из примитивно рекурсивных функций (докажите самостоятельно, что функция $x \dot{-} 1$ является примитивно рекурсивной), а значит является примитивно рекурсивной.

Проблемой вхождения для числового множества A называется задача отыскания алгоритма, который по стандартной записи (например, десятичной) произвольного натурального числа a позволяет узнать, принадлежит ли число a множеству A или нет, то есть позволяет вычислять значения характеристической функции множества A. В силу тезиса Чёрча существование такого алгоритма равносильно рекурсивности характеристической функции. Поэтому можно сказать, что рекурсивные множества — это множества с алгоритмически разрешимой проблемой вхождения.

Наконец отметим, что понятие рекурсивного множества можно распространить и на множества, не являющиеся числовыми. Для этого можно, например, перенумеровать элементы произвольного не более чем счетного множества M и рассматривать числовые множества индексов элементов M.

4.4. Общезначимые формулы алгебры предикатов. Для формул алгебры высказываний существует алгоритм, позволяющий определить является данная формула тавтологией или нет. Таким алгоритмом является построение таблицы истинности. Однако, этот алгоритм не применим для формул алгебры предикатов, так как такие формулы рассматриваются и на бесконечных множествах, для которых процесс построения таблиц истинности является бесконечным. Возникает вопрос: существует ли алгоритм, позволяющий для произвольной формулы алгебры предикатов установить за конечное число шагов является данная формула общезначимой или нет? Отрицательный ответ на этот вопрос дает теорема, полученная Чёрчем в 1936 году.

Теорема 1. *Совокупность всех общезначимых формул алгебры предикатов является нерекурсивным множеством.*

Однако, отсутствие алгоритма, позволяющего установить является ли произвольная формула алгебры предикатов общезначимой, еще не означает, что для каждой конкретной формулы этот вопрос нельзя решить. Более того, существуют алгоритмы, позволяющие определять общезначимость формулы для некоторых частных видов формул. Например, известно, что для формул алгебры предикатов, содержащих только одноместные предикатные переменные эта проблема имеет решение. Существуют и некоторые другие множества формул алгебры предикатов, которые являются рекурсивными, то есть для которых алгоритмическая проблема общезначимости разрешима.

4.5. Диофантовы уравнения. Пусть $F(x_1, x_2, \ldots, x_n)$ — многочлен от переменных x_1, $x_2, \ldots, x_n$ с целыми коэффициентами. Уравнение вида

$$F(x_1, x_2, \ldots, x_n) = 0,$$

называется *диофантовым*. На международном математическом конгрессе в Париже в 1901 году Д. Гильбертом была сформулирована одна из наиболее знаменитых алгоритмических проблем математики: "Найти алгоритм, позволяющий для любого диофантова уравнения определить его разрешимость или неразрешимость в целых числах". Эта проблема известна как 10-я проблема Гильберта.

Эта и многие другие алгоритмические проблемы стимулировали появление в 30-х годах нашего столетия и дальнейшее бурное развитие теории алгоритмов. 10-я же проблема Гильберта была отрицательно решена в 1970 году. Советским математиком Ю. В. Матиясевичем была доказана алгоритмическая неразрешимость в общем виде 10-ой проблемы Гильберта.

Еще раз отметим, что алгоритмическая неразрешимость означает лишь отсутствие единого способа для решения всех единичных задач данной серии, в то время как каждая индивидуальная задача серии вполне может быть решена своим индивидуальным способом. Более того, может существовать алгоритм для решения задач некоторого бесконечного подкласса данного класса задач. Например, для частного случая диофантова уравнения

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0, \text{ где } a_0, \ldots, a_n \in N_0 \qquad (1)$$

хорошо известно, что все его целые корни следует искать среди делителей свободного члена a_0. Таким образом, для класса диофантовых уравнений, состоящего из уравнений вида (1) существует алгоритм, позволяющий находить все целые решения каждого уравнения этого класса.

4.6. Новые термины. Невычислимая функция. Характеристическая функция данного множества. Рекурсивное множество. Проблема вхождения. Усеченная разность. Диофантово уравнение.

4.7. Контрольные вопросы.

1. Из каких общих соображений следует существование невычислимых функций?

2. Следует ли из рекурсивности данного числового множества существование алгоритма, позволяющего определить, является ли произвольное число элементом этого множества или нет?

3. Является ли рекурсивным множество всех четных чисел?

4. Опишите алгоритм нахождения всех целых корней многочлена от x с целыми коэффициентами.

4.8. Упражнения.

1. Докажите, что всех мыслимых машин Тьюринга, отличающихся между собой по существу своей работы, имеется более, чем счетное множество.

2. Рассмотрим множество всех одноместных словарных функций, заданных и принимающих значения в множестве всех слов одноэлементного алфавита $A = \{1\}$. Докажите, что среди этих функций имеется невычислимая по Тьюрингу функция.

Приложение А

Алфавиты

Готический алфавит

$\mathfrak{A}\ \mathfrak{a}$ — A	$\mathfrak{G}\ \mathfrak{g}$ — G	$\mathfrak{M}\ \mathfrak{m}$ — M	$\mathfrak{S}\ \mathfrak{s}$ — S	$\mathfrak{Y}\ \mathfrak{y}$ — Y
$\mathfrak{B}\ \mathfrak{b}$ — B	$\mathfrak{H}\ \mathfrak{h}$ — H	$\mathfrak{N}\ \mathfrak{n}$ — N	$\mathfrak{T}\ \mathfrak{t}$ — T	$\mathfrak{Z}\ \mathfrak{z}$ — Z
$\mathfrak{C}\ \mathfrak{c}$ — C	$\mathfrak{I}\ \mathfrak{i}$ — I	$\mathfrak{O}\ \mathfrak{o}$ — O	$\mathfrak{U}\ \mathfrak{u}$ — U	
$\mathfrak{D}\ \mathfrak{d}$ — D	$\mathfrak{J}\ \mathfrak{j}$ — J	$\mathfrak{P}\ \mathfrak{p}$ — P	$\mathfrak{V}\ \mathfrak{v}$ — V	
$\mathfrak{E}\ \mathfrak{e}$ — E	$\mathfrak{K}\ \mathfrak{k}$ — K	$\mathfrak{Q}\ \mathfrak{q}$ — Q	$\mathfrak{W}\ \mathfrak{w}$ — W	
$\mathfrak{F}\ \mathfrak{f}$ — F	$\mathfrak{L}\ \mathfrak{l}$ — L	$\mathfrak{R}\ \mathfrak{r}$ — R	$\mathfrak{X}\ \mathfrak{x}$ — X	

Греческий алфавит

$A\ \alpha$ — Альфа	$H\ \eta$ — Эта	$N\ \nu$ — Ню	$T\ \tau$ — Тау
$B\ \beta$ — Бета	$\Theta\ \theta$ — Тэта	$\Xi\ \xi$ — Кси	$\Upsilon\ \upsilon$ — Ипсилон
$\Gamma\ \gamma$ — Гамма	$I\ \iota$ — Йота	$O\ o$ — Омикрон	$\Phi\ \phi\ \varphi$ — Фи
$\Delta\ \delta$ — Дельта	$K\ \kappa$ — Каппа	$\Pi\ \pi\ \varpi$ — Пи	$X\ \chi$ — Хи
$E\ \varepsilon\ \epsilon$ — Эпсилон	$\Lambda\ \lambda$ — Ламбда	$P\ \rho\ \varrho$ — Ро	$\Psi\ \psi$ — Пси
$Z\ \zeta$ — Дзета	$M\ \mu$ — Мю	$\Sigma\ \sigma\ \varsigma$ — Сигма	$\Omega\ \omega$ — Омега

Приложение В

Предметный указатель