



*Томский межвузовский центр
дистанционного образования*

В.М. Зюзьков

ДИСКРЕТНАЯ МАТЕМАТИКА

Часть 1

Теория множеств и математическая логика

Учебное пособие

Томск - 1999

Министерство образования Российской Федерации

**ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)**

Кафедра компьютерных систем в управлении
и проектировании (КСУП)

В.М. Зюзьков

ДИСКРЕТНАЯ МАТЕМАТИКА

Часть 1

Теория множеств и математическая логика

Учебное пособие

1999

Зюзьков В.М.

Дискретная математика. Часть 1. Теория множеств и математическая логика: Учебное пособие. - Томск: Томский межвузовский центр дистанционного образования, 1999. - 71 с.

Учебное пособие содержит первую часть теоретического материала по дисциплине "Дискретная математика". Содержание пособия направлено на обучение формальному аппарату математики, логическому мышлению.

Предназначено для студентов, обучающихся на всех формах обучения с использованием дистанционных образовательных технологий.

© Зюзьков В.М., 1999

© Томский межвузовский центр
дистанционного образования, 1999

СОДЕРЖАНИЕ

1. Основы теории множеств	4
1.1. Начальные понятия теории множеств	4
1.2. Операции над множествами. Диаграммы Эйлера-Венна ...	6
1.3. Отношения	8
1.4. Функции	9
1.5. Эквивалентность	11
1.6. Порядок	14
2. Логика высказываний	15
2.1. Зачем вы изучаете математическую логику?	15
2.2. Высказывания	17
2.3. Логические связки	18
2.4. Формулы логики высказываний	20
2.5. Равносильность формул	23
2.6. Тождественно-истинные формулы	26
2.7. Правильные рассуждения	27
2.8. Нормальные формы формул	29
2.9. Разрешимость для логики высказываний	32
3. Булевы алгебры	34
3.1. Абстрактное определение булевой алгебры	34
3.2. Булевы функции. Теорема о нормальной булевой форме ...	37
3.3. Полные системы булевых функций	41
3.4. Переключательные элементы	42
4. Логика предикатов	47
4.1. Формулы логики предикатов	47
4.2. Равносильность формул в логике предикатов	52
4.3. Выполнимость и общезначимость в логике предикатов	54
5. Исчисления	55
5.1. Аксиоматические теории	55
5.2. Исчисление высказываний	55
5.3. Исчисление предикатов	57
5.4. Неполнота математики	58
6. Позиционные системы счисления	61
6.1. Определение и перевод целых чисел из одной системы счисления в другую	61
6.2. Представление отрицательных чисел	63
6.3. Нестандартные позиционные системы счисления	63
7. Решения логических задач	65
Рекомендуемая литература	71

1. ОСНОВЫ ТЕОРИИ МНОЖЕСТВ

1.1. Начальные понятия теории множеств

Под *множеством* S будем понимать любое собрание определенных и различимых между собою объектов, мыслимое как единое целое. Эти объекты называются *элементами* множества S .

В этом интуитивном определении, принадлежащем немецкому математику Георгу Кантору (1845-1918), существенным является то обстоятельство, что собрание предметов само рассматривается как один предмет, мыслится как единое целое. Что касается самих предметов, которые могут входить в множество, то относительно них существует значительная свобода. Это может быть множество студентов, присутствующих на лекции, множество целых чисел, множество точек плоскости, множество всех людей, живущих на Земле. Заметим, что канторовская формулировка позволяет рассматривать множества, элементы которых по той или иной причине нельзя точно указать (например, множество простых чисел, множество русских воинов, погибших в битве на Куликовом поле, и т. п.).

Символом \in обозначается *отношение принадлежности*. Запись $x \in S$ означает, что элемент x принадлежит множеству S . Если элемент x не принадлежит множеству S , то пишут $x \notin S$.

Г. Кантором сформулировано несколько интуитивных принципов, которые естественно считать выполняющимися для произвольных множеств.

Интуитивный принцип объемности. *Множества A и B считаются равными, если они состоят из одних и тех же элементов.*

Записывают $A=B$, если A и B равны, и $A \neq B$ - в противном случае.

Пример 1.1. Проиллюстрируем принцип объемности. Множество A всех положительных четных чисел равно множеству B положительных целых чисел, представимых в виде суммы двух положительных нечетных чисел. Действительно, если $x \in A$, то для некоторого целого положительного числа m $x = 2m$; тогда $x = (2m - 1) + 1$, т. е. $x \in B$. Если $x \in B$, то для некоторых целых положительных p и q $x = (2p - 1) + (2q - 1) = 2(p + q - 1)$, т. е. $x \in A$.

Множество, элементами которого являются объекты a_1, a_2, \dots, a_n и только они, обозначают $\{a_1, a_2, \dots, a_n\}$.

Пример 1.2. В силу принципа объемности $\{2, 4, 6\} = \{4, 2, 6\} = \{2, 4, 4, 6\}$; $\{\{1, 2\}\} \neq \{1, 2\}$, так как единственным элементом множества $\{\{1, 2\}\}$ является множество $\{1, 2\}$, а множество $\{1, 2\}$ состоит из двух элементов: чисел 1 и 2.

При рассмотрении способов задания множеств возникает проблема их эффективного описания. Ее решение обычно основано на интуитивном понятии "форма от x ". Под *формой от x* будем понимать конечную последовательность, состоящую из слов и символа x , такую, что если каждое вхождение x в эту последовательность заменить одним и тем же именем некоторого

предмета соответствующего рода, то в результате получится истинное или ложное предложение. Например формами от x являются следующие предложения; " 3 делит x ", " $x^2 + 2x + 1 > x$ ", " $x^2 = 4$ ", " x - родственник Иванова". Напротив, предложения " $\text{для всех } x \quad x^2 - 4 = (x - 2)(x + 2)$ " и " $\text{существует такое } x, \text{ что } x > 0$ " не являются формами от x .

Обозначим форму от x через $P(x)$.

Интуитивный принцип абстракции. Любая форма $P(x)$ определяет некоторое множество A , а именно множество тех и только тех предметов a , для которых $P(a)$ - истинное предложение.

Для множества A , определяемого формой $P(x)$, принято обозначение $A = \{x | P(x)\}$.

Пример 1.3.

1. $\{x | x - \text{положительное число, меньшее } 9\} = \{1, 2, 3, 4, 5, 6, 7, 8\}$.
2. $\{x | x - \text{четное число}\}$ - множество четных чисел.

Описанные выше понятия теории множеств с успехом могут быть использованы в началах анализа, алгебры, математической логики и т. д. Однако надо иметь в виду, что при более строгих рассмотрениях такое интуитивное восприятие может оказаться неудовлетворительным.

Парадокс Бертрانا Рассела (1872-1970). (О несовершенстве интуитивных представлений о множествах.) Можно указать такие множества, которые принадлежат самим себе как элементы, например, множество всех множеств, и такие множества, которые не являются элементами самих себя, например, множество $\{1, 2\}$, элементами которого являются числа 1 и 2. Рассмотрим теперь множество $A = \{X | X \notin X\}$. Тогда, если $A \notin A$, то, по определению, $A \in A$. С другой стороны, если $A \in A$, то A - одно из тех множеств X , которые не есть элементы самих себя, т. е. $A \notin A$. В любом случае A есть элемент A и A не есть элемент A .

Другая, более популярная форма этого парадокса известна как *парадокс бороды*. Владелец парикмахерской в одном селе повесил следующее объявление: "Брею тех и только тех жителей села, кто не бреется сам". Спрашивается, кто бреет бороды?

Этот парадокс свидетельствует о том, что широко используемая теория множеств в ее интуитивном, "наивном" изложении является противоречивой. Формализация теории множеств, связанная, в частности, с устранением парадоксов, способствовала развитию не только методов теории множеств, но и такой науки, как математическая логика.

Через \subseteq обозначим *отношение включения* между множествами, т. е. $A \subseteq B$, если каждый элемент множества A есть элемент множества B . Тогда говорят, что A есть *подмножество* множества B . Если $A \subseteq B$ и $A \neq B$, то говорят, что A есть *собственное подмножество* B , и пишут $A \subset B$.

Пример 1.4. Множество четных чисел есть подмножество множества целых чисел; множество рациональных чисел есть подмножество множества действительных чисел; $\{1, 2\} \subseteq \{1, 2, 3, 4\}$.

Заметим, что: а) $X \subseteq X$; б) если $X \subseteq Y$, $Y \subseteq Z$, то $X \subseteq Z$; в) если $X \subseteq Y$ и $Y \subseteq X$, то $X=Y$.

Не надо смешивать отношения принадлежности и включения. Хотя $1 \in \{1\}$, $\{1\} \subseteq \{\{1\}\}$, не верно, что $1 \in \{\{1\}\}$. так как единственным элементом множества $\{\{1\}\}$ является $\{1\}$.

Множество, не содержащее элементов, называется *пустым* и обозначается \emptyset . Пустое множество есть подмножество любого множества.

Множество всех подмножеств A называется *множеством-степенью* и обозначается $P(A)$.

Пример 1.5. Если $A = \{1, 2, 3\}$, то $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$.

В дальнейшем неоднократно будем пользоваться утверждением, что если множество A состоит из n элементов, то множество $P(A)$ состоит из 2^n элементов.

1. 2. Операции над множествами. Диаграммы Эйлера-Венна

Рассмотрим методы получения новых множеств из уже существующих.

Объединением множеств A и B называется множество $A \cup B$, все элементы которого являются элементами множества A или B :

$$A \cup B = \{x \mid x \in A \text{ или } x \in B\}.$$

Пересечением множеств A и B называется множество $A \cap B$, элементы которого являются элементами обоих множеств A и B :

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}.$$

Очевидно, что выполняются включения $A \cup B \subseteq A \subseteq A \cap B$ и $A \cup B \subseteq B \subseteq A \cap B$.

Относительным дополнением множества A до множества X называется множество $X \setminus A$ всех тех элементов множества X , которые не принадлежат множеству A :

$$X \setminus A = \{x \mid x \in X \text{ и } x \notin A\}.$$

Симметрической разностью множеств A и B называется множество

$$A \oplus B = (A \setminus B) \cup (B \setminus A).$$

Если все рассматриваемые в ходе данного рассуждения множества являются подмножествами некоторого множества U , то это множество U называется *универсальным* для данного рассуждения (контекста).

Абсолютным дополнением множества A называется множество \overline{A} всех тех элементов x , которые не принадлежат множеству A :

$$\overline{A} = U \setminus A.$$

Заметим, что $X \setminus A = X \cap \overline{A}$.

Для наглядного представления отношений между подмножествами какого-либо универсального множества используются диаграммы Эйлера-Венна. Само универсальное множество U изображают в виде прямоугольника, а его подмножества - в виде кругов, расположенных внутри прямоугольника (рис.1).

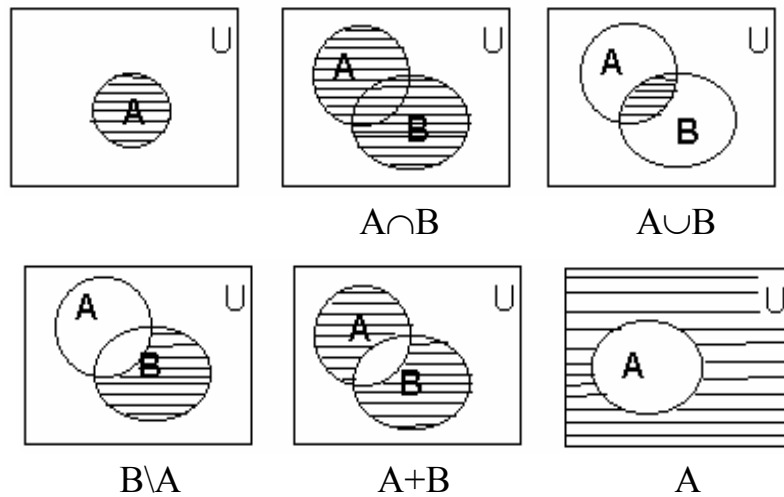


Рис. 1. Диаграммы Эйлера-Венна

Теорема 1.1. Для любых подмножеств A , B и C универсального множества U выполняются следующие тождества (основные тождества алгебры множеств):

- | | |
|--|---|
| 1. $A \cap B = B \cap A$ (коммутативность \cap) | 1'. $A \cup B = B \cup A$ (коммутативность \cup) |
| 2. $A \cap (B \cap C) = (A \cap B) \cap C$ (ассоциативность \cap) | 2'. $A \cup (B \cup C) = (A \cup B) \cup C$ (ассоциативность \cup) |
| 3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (дистрибутивность \cap относительно \cup) | 3'. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность \cup относительно \cap) |
| 4. $A \cap \emptyset = \emptyset$ | 4'. $A \cup U = A$ |
| 5. $A \cap \bar{A} = \emptyset$ | 5'. $A \cup \bar{A} = U$ |
| 6. $A \cap A = A$ | 6'. $A \cup A = A$ |
| 7. $\overline{A \cap B} = \bar{A} \cup \bar{B}$ (закон де Моргана) | 7'. $\overline{A \cup B} = \bar{A} \cap \bar{B}$ (закон де Моргана) |
| 9. $A \cap (A \cup B) = A$ (закон поглощения) | 9'. $A \cup (A \cap B) = A$ (закон поглощения) |

Докажем тождество 3. Сначала покажем, что $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Действительно, если $x \in A \cap (B \cup C)$, то $x \in A$ или $x \in B \cup C$. Если $x \in A$, то $x \in A \cap B$ и $x \in A \cap C$. Следовательно, $x \in (A \cap B) \cup (A \cap C)$. Если $x \in B \cup C$, то $x \in B$ и $x \in C$. Отсюда $x \in A \cap B$ и $x \in A \cap C$, а значит $x \in (A \cap B) \cup (A \cap C)$. Теперь покажем, что $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Если $x \in (A \cap B) \cup (A \cap C)$, то $x \in A \cap B$ и $x \in A \cap C$. Следовательно, $x \in A$ или $x \in B$ и $x \in C$, т.е. $x \in B \cup C$. Отсюда $x \in A \cap (B \cup C)$.

Докажем тождество 8. Пусть $x \in \overline{A \cap B}$. Тогда $x \in U$ и $x \notin A \cap B$. Следовательно, $x \notin A$ и $x \notin B$. Отсюда $x \in \overline{A}$ и $x \in \overline{B}$, а значит, $x \in A \cup B$. Итак, $A \cap B \subseteq A \cup B$. Пусть теперь, $x \in A \cup B$. Тогда $x \in A$ и $x \in B$. Следовательно, $x \in U$ и $x \notin A$ и $x \notin B$. Значит, $x \notin A \cap B$, т. е. $x \in \overline{A \cap B}$. Итак, $A \cup B \subseteq \overline{A \cap B}$.

Остальные тождества доказываются аналогично.

Теорема 1.2. Предложения о произвольных множествах A и B попарно эквивалентны:

1) $A \subseteq B$; 2) $A \cup B = A$; 3) $A \cap B = B$.

Докажем, что из первого предложения следует второе. Действительно, так как $A \cup B \subseteq A$, то достаточно показать, что в этом случае $A \subseteq A \cup B$. Но если $x \in A$, то $x \in B$, так как $A \subseteq B$, и, следовательно, $x \in A \cup B$.

Докажем, что из второго предложения следует третье. Так как $A \cup B = A$, то $A \cap B = (A \cup B) \cap B$. По закону поглощения (см. тождество 9) $B \cap (A \cup B) = B$. Отсюда, используя закон коммутативности, получаем $A \cap B = B$.

Докажем, что из третьего предложения следует первое. Так как $A \subseteq A \cap B$, а по условию третьего предложения $A \cap B = B$, то $A \subseteq B$.

1. 3. Отношения

Упорядоченная пара $\langle x, y \rangle$ интуитивно определяется как совокупность, состоящая из двух элементов x и y , расположенных в определенном порядке. Две пары $\langle x, y \rangle$ и $\langle u, v \rangle$ считаются равными тогда и только тогда, когда $x = u$ и $y = v$.

Упорядоченная n -ка элементов x_1, x_2, \dots, x_n обозначается $\langle x_1, x_2, \dots, x_n \rangle$ и, по определению, есть $\langle \langle x_1, x_2, \dots, x_{n-1} \rangle, x_n \rangle$.

Бинарным (или двуместным) отношением ρ называется множество упорядоченных пар. Если ρ есть некоторое отношение и пара $\langle x, y \rangle$ принадлежит этому отношению, то наряду с записью $\langle x, y \rangle \in \rho$ употребляется запись $x \rho y$. Элементы x и y называются *координатами* или *компонентами* отношения ρ . *n -арным отношением* называется множество упорядоченных n -ок.

Областью определения бинарного отношения ρ называется множество $D_\rho = \{x \mid \text{существует такое } y, \text{ что } x \rho y\}$.

Областью значений бинарного отношения ρ называется множество $R_\rho = \{y \mid \text{существует такое } x, \text{ что } x \rho y\}$.

Пример 1.6.

1. Множество $\{\langle 1, 2 \rangle, \langle 2, 4 \rangle, \langle 3, 3 \rangle, \langle 2, 1 \rangle\}$ - бинарное отношение.
2. Отношение равенства на множестве действительных чисел есть множество $\{\langle x, y \rangle \mid x \text{ и } y - \text{действительные числа и } x \text{ равно } y\}$. Для этого отношения

существует специальное обозначение $=$. Область определения D_p совпадает с областью значений R_p и является множеством действительных чисел.

3. Отношение "меньше чем" на множестве целых чисел есть множество $\{ \langle x, y \rangle \mid \text{для целых чисел } x \text{ и } y \text{ найдется положительное число } z \text{ такое, что } x + z = y \}$. Для этого отношения существует специальное обозначение $<$. Область определения D_p совпадает с областью значений R_p и является множеством целых чисел.

Прямым произведением множеств X и Y называется множество всех упорядоченных пар $\langle x, y \rangle$ таких, что $x \in X$ и $y \in Y$. Обозначается прямое произведение множеств X и Y через $X \times Y$.

Каждое отношение ρ есть подмножество прямого произведения некоторых множеств X и Y таких, что $D_\rho \subseteq X$ и $R_\rho \subseteq Y$. Если $X = Y$, то говорят, что ρ есть отношение на множестве X .

Прямым произведением множеств X_1, X_2, \dots, X_n называется множество всех упорядоченных n -ок $\langle x_1, x_2, \dots, x_n \rangle$ таких, что $x_i \in X_i$, $i = 1, 2, \dots, n$. Обозначается прямое произведение множеств X_1, X_2, \dots, X_n через $X_1 \times X_2 \times \dots \times X_n$. Если $X_1 = X_2 = \dots = X_n = X$, то пишут $X_1 \times X_2 \times \dots \times X_n = X^n$. Любое n -местное отношение есть подмножество прямого произведения некоторых множеств X_1, X_2, \dots, X_n .

Пример 1.7.

1. Пусть $X = \{1, 2, 3\}$, $Y = \{0, 1\}$. Тогда $X \times Y = \{ \langle 1, 0 \rangle, \langle 1, 1 \rangle, \langle 2, 0 \rangle, \langle 2, 1 \rangle, \langle 3, 0 \rangle, \langle 3, 1 \rangle \}$;
 $Y \times X = \{ \langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 0, 3 \rangle, \langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle \}$.

Мы указали, кроме того, такие множества X и Y , что $X \times Y \neq Y \times X$.

2. Пусть X - множество точек отрезка $[0, 1]$, а Y - множество точек отрезка $[1, 2]$. Тогда $X \times Y$ - множество точек квадрата $[0, 1] \times [1, 2]$ с вершинами в точках $(0, 1)$, $(0, 2)$, $(1, 1)$ и $(1, 2)$.

Для бинарных отношений обычным образом определены теоретико-множественные операции объединения, пересечения и т. д.

Обратным отношением для ρ называется отношение

$$\rho^{-1} = \{ \langle x, y \rangle \mid \langle y, x \rangle \in \rho \}.$$

Композицией отношений ρ_1 и ρ_2 называется отношение $\rho_2 \circ \rho_1 = \{ \langle x, z \rangle \mid \text{существует } y \text{ такое, что } \langle x, y \rangle \in \rho_1 \text{ и } \langle y, z \rangle \in \rho_2 \}$.

Для любых бинарных отношений выполняются следующие свойства:

1. $(\rho^{-1})^{-1} = \rho$;
2. $(\gamma \circ \varphi)^{-1} = \varphi^{-1} \circ \gamma^{-1}$.

Первое свойство очевидно. Для доказательства второго свойства покажем, что множества, записанные в левой и правой частях равенства, состоят из одних и тех же элементов. Действительно, $\langle x, y \rangle \in (\gamma \circ \varphi)^{-1} \Leftrightarrow \langle y, x \rangle \in \gamma \circ \varphi \Leftrightarrow \text{существует } z \text{ такое, что } \langle y, z \rangle \in \varphi \text{ и } \langle z, x \rangle \in \gamma \Leftrightarrow \text{существует } z \text{ такое, что}$

$\langle z, y \rangle \in \varphi^{-1}$ и $\langle x, z \rangle \in \gamma^{-1} \Leftrightarrow \langle x, y \rangle \in \varphi^{-1} \upharpoonright \gamma^{-1}$. (Символ \Leftrightarrow заменяет слова "тогда и только тогда, когда".)

1.4. Функции

Бинарное отношение f называется *функцией*, если из $\langle x, y \rangle \in f$ и $\langle x, z \rangle \in f$ следует $y = z$.

Поскольку функции являются бинарными отношениями, то к ним применим интуитивный принцип объемности, т. е. две функции f и g равны, если они состоят из одних и тех же элементов. Область определения функции обозначается D_f , а область её значений - R_f . Определяются они также как и для бинарных отношений. Часто приходится сталкиваться с трудностями при определении области значений функции. Поэтому, если $D_f = X$ и $R_f \subseteq Y$, то говорят, что функция f задана на множестве X со значениями во множестве Y и осуществляет *отображение* множества X во множество Y (или устанавливает *соответствие* между множествами X и Y). Это отображение обозначается таким образом: $f: X \rightarrow Y$.

Если f - функция, то вместо $\langle x, y \rangle \in f$ пишут $y = f(x)$ и говорят, что y - значение, соответствующее аргументу x , или y - образ элемента x при отображении f . При этом x называют прообразом элемента y .

Пример 1.8. Отношение $\{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle \square, 0 \rangle\}$ - функция: отношение $\{\langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 2, 4 \rangle\}$ не является функцией: отношение $\{\langle x, x^2 + 2x + 1 \rangle \mid x - \text{действительное число}\}$ - функция, которую обычно обозначают $y = x^2 + 2x + 1$.

Назовем f n -местной функцией из X в Y , если $f: X^n \rightarrow Y$. Тогда пишем $y = f(x_1, \dots, x_n)$ и говорим, что y - значение функции при значении аргументов x_1, \dots, x_n .

Пусть $f: X \rightarrow Y$. Функция (отображение) f называется *инъективной* (*инъективным*), если для любых x_1, x_2, y из $y = f(x_1)$ и $y = f(x_2)$ следует, что $x_1 = x_2$ (или, иначе, из $\langle x_1, y \rangle \in f$ и $\langle x_2, y \rangle \in f$ следует, что $x_1 = x_2$). Функция (отображение) f называется *сюръективной* (*сюръективным*), если для любого элемента $y \in Y$ существует элемент $x \in X$ такой, что $y = f(x)$. Функция (отображение) f называется *биективной* (*биективным*), если f одновременно инъективна и сюръективна. Если существует биективная функция $f: X \rightarrow Y$, то говорят, что f осуществляет взаимно-однозначное соответствие между множествами X и Y .

Пример 1.9. Рассмотрим три функции, отображающие множество действительных чисел \mathbb{R} во множество действительных чисел $f_i: \mathbb{R} \rightarrow \mathbb{R}$, $i = 1, 2, 3$:

- 1) функция $f_1(x) = e^x$ инъективна, но не сюръективна;
- 2) функция $f_2(x) = x^3 - x$ сюръективна, но не инъективна;
- 3) функция $f_3(x) = 2x + 1$ биективна.

Композиция двух функций f и g есть отношение $g \circ f = \{ \langle x, z \rangle \mid \text{существует } y \text{ такое, что } xfy \text{ и } ygz \}$.

Теорема 1.3. Композиция двух функций есть функция. При этом если $f: X \rightarrow Y$, $g: Y \rightarrow Z$, то $g \circ f: X \rightarrow Z$.

Действительно, если $\langle x, y \rangle \in g \circ f$ и $\langle x, z \rangle \in g \circ f$, то существует такое u , что xfu , ugu , и существует такое v , что xfv , vgz . Поскольку f - функция, то $u = v$; поскольку g - функция, то $u = z$ и, следовательно, $g \circ f$ - функция. Вторая часть утверждения очевидна.

Верно также и следующее утверждение.

Теорема 1.4. Композиция двух биективных функций есть биективная функция.

Тождественным отображением множества X в себя называется отображение $e_X: X \rightarrow X$ такое, что для любого $x \in X$ $e_X(x) = x$. Тогда, если $f: X \rightarrow Y$, то $e_X \circ f = f$, $f \circ e_Y = f$.

Пусть f^{-1} - отношение, обратное f . Выясним, при каких условиях отношение f^{-1} будет функцией. Его называют тогда *обратной функцией* или, если f осуществляет отображение множества X во множество Y , *обратным отображением*.

Теорема 1.5. Отображение $f: X \rightarrow Y$ имеет обратное отображение $f^{-1}: Y \rightarrow X$ тогда и только тогда, когда f - биекция.

Если f - биекция, то, поскольку f сюръективно, f^{-1} определено на множестве Y . Кроме того, f^{-1} - функция, так как если $\langle y, x_1 \rangle \in f^{-1}$ и $\langle y, x_2 \rangle \in f^{-1}$, то $\langle x_1, y \rangle \in f$ и $\langle x_2, y \rangle \in f$, а в силу инъективности f имеем $x_1 = x_2$.

Пусть теперь отображение f имеет обратное отображение f^{-1} , определенное на множестве Y со значениями во множестве X . Тогда f сюръективно, поскольку любой элемент $y \in Y$ имеет прообраз $x \in X$. При этом f инъективно, так как если $\langle x_1, y \rangle \in f$ и $\langle x_2, y \rangle \in f$, то $\langle y, x_1 \rangle \in f^{-1}$ и $\langle y, x_2 \rangle \in f^{-1}$, а поскольку f^{-1} - функция, то $x_1 = x_2$.

Заметим, что для того, чтобы обратное отношение f^{-1} было функцией, достаточно инъективности функции f .

Поскольку функция есть бинарное отношение, то выполняются следующие свойства инъективных функций f и g :

- 1) $(f^{-1})^{-1} = f$;
- 2) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Если $f: X \rightarrow Y$ - биекция, то

- 3) $f^{-1} \circ f = e_X$;
- 4) $f \circ f^{-1} = e_Y$.

1.5. Эквивалентность

Отношение ρ на множестве X называется *рефлексивным*, если для любого элемента $x \in X$ выполняется $x\rho x$.

Отношение ρ на множестве X называется *симметричным*, если для любых $x, y \in X$ из $x\rho y$ следует $y\rho x$.

Отношение ρ на множестве X называется *транзитивным*, если для любых $x, y, z \in X$ из $x\rho y$ и $y\rho z$ следует $x\rho z$.

Рефлексивное, симметричное и транзитивное отношение ρ на множестве X называется *отношением эквивалентности* на множестве X .

Пример 1.10.

1. Отношение равенства на множестве целых чисел есть отношение эквивалентности.
2. Отношение подобия на множестве треугольников есть отношение эквивалентности.
3. Отношение $x < y$ на множестве действительных чисел не рефлексивно, не симметрично, но транзитивно на этом множестве.
4. Отношение сравнимости по модулю натурального числа n на множестве целых чисел Z : $x \equiv y \pmod{n}$ тогда и только тогда, когда $x - y$ делится на n . Это отношение рефлексивно на Z , так как для любого $x \in Z$ $x - x = 0$, и, следовательно, делится на n . Это отношение симметрично, так как если $x - y$ делится на n , то $y - x$ делится на n . Это отношение транзитивно, так как если $x - y$ делится на n , то для некоторого целого t_1 имеем $x - y = t_1 n$, а если $y - z$ делится на n , то для некоторого целого t_2 имеем $y - z = t_2 n$. Отсюда $x - z = (t_1 + t_2)n$, т. е. $x - z$ делится на n .
5. Отношение принадлежности к одной студенческой группе на множестве студентов института - отношение эквивалентности.
6. На множестве $N \times N$, где N - множество натуральных чисел, определим отношение $\rho : \langle x, y \rangle \rho \langle u, v \rangle \Leftrightarrow xv = yu$. Это отношение рефлексивно: $\langle x, y \rangle \rho \langle x, y \rangle$, так как $x y = y x$; симметрично: если $\langle x, y \rangle \rho \langle u, v \rangle$, то $\langle u, v \rangle \rho \langle x, y \rangle$, так как из $xv = yu$ следует, что и $uy = vx$; транзитивно: если $\langle x, y \rangle \rho \langle u, v \rangle$, $\langle u, v \rangle \rho \langle w, z \rangle$, то $\langle x, y \rangle \rho \langle w, z \rangle$, так как, перемножая левые и правые части равенств $xv = yu$ и $uz = vw$ после сокращения получаем $xz = yw$.

Пусть ρ - отношение эквивалентности на множестве X .

Классом эквивалентности, порожденным элементом x , называется подмножество множества X , состоящее из тех элементов $y \in X$, для которых $x\rho y$. Класс эквивалентности, порожденный элементом x , обозначается $[x]$:

$$[x] = \{y \mid y \in X \text{ и } x\rho y\}.$$

Пример 1.11.

1. Отношение равенства на множестве целых чисел порождает следующие классы эквивалентности: для любого элемента $x \in \mathbf{Z}$ $[x] = \{x\}$, т. е. каждый класс эквивалентности состоит только из одного элемента - числа x .
2. Отношение сравнимости по модулю числа n на множестве целых чисел \mathbf{Z} порождает следующие классы эквивалентности: вместе с любым числом $a \in \mathbf{Z}$ в этом же классе эквивалентности содержатся все числа вида $a + kn$, где k - целое. Очевидно, что все числа $0, 1, 2, \dots, n-1$ порождают различные классы эквивалентности, которые обозначим $[0], [1], [2], \dots, [n-1]$. Они называются классами вычетов по модулю n . Все остальные классы эквивалентности для этого отношения совпадают с ними, так как любое число $a \in \mathbf{Z}$ можно представить в виде $a = qn + r$, где $0 \leq r < n$.
3. Для отношения принадлежности к одной студенческой группе классом эквивалентности является множество студентов одной группы.
4. Класс эквивалентности, порожденной парой $\langle x, y \rangle$ для отношения ρ из примера 1.10 (6) определяется соотношением

$$[\langle x, y \rangle] = \{ \langle u, v \rangle \mid x/y = u/v \}.$$

Каждый класс эквивалентности в этом случае определяет одно положительное рациональное число.

Теорема 1.6. Пусть ρ - отношение эквивалентности на множестве X . Тогда: 1) если $x \in X$, то $x \in [x]$; 2) если $x, y \in X$ и $x \rho y$, то $[x] = [y]$ (т. е. класс эквивалентности порождается любым своим элементом).

Для доказательства первой части утверждения достаточно воспользоваться рефлексивностью отношения ρ : $x \rho x$ и, следовательно, $x \in [x]$. Докажем вторую часть утверждения. Пусть $z \in [y]$, тогда $y \rho z$ и в силу транзитивности отношения ρ $x \rho z$, т. е. $z \in [x]$. Отсюда $[y] \subseteq [x]$. Аналогично, в силу симметричности ρ можно показать, что $[x] \subseteq [y]$, а значит $[y] = [x]$.

Разбиением множества X называется совокупность попарно непересекающихся множеств X таких, что каждый элемент множества X принадлежит одному и только одному из этих подмножеств.

Пример 1.12.

1. $X = \{1, 2, 3, 4, 5\}$. Тогда $\{\{1, 2\}, \{3, 5\}, 4\}$ - разбиение множества X .
2. Пусть X - множество студентов института. Тогда разбиением этого множества является, например, совокупность студенческих групп.

Теорема 1.7. Всякое разбиение множества X определяет на X отношение эквивалентности ρ : $x \rho y$ тогда и только тогда, когда x и y принадлежат одному подмножеству разбиения.

Рефлексивность и симметричность ρ очевидны. Пусть теперь $x \rho y$ и $y \rho z$. Тогда $x, y \in X_1$, $y, z \in X_2$, где X_1, X_2 - подмножества из разбиения X . Поскольку $y \in X_1$, $y \in X_2$, то $X_1 = X_2$. Следовательно, $x, z \in X_1$ и $x \rho z$.

Теорема 1.8. Всякое отношение эквивалентности ρ определяет разбиение множества X на классы эквивалентности относительно этого отношения.

Докажем, что совокупность классов эквивалентности определяет разбиение множества X . В силу теоремы 1.6 $x \in [x]$, а следовательно, каждый элемент множества X принадлежит некоторому классу эквивалентности. Из теоремы 1.6 вытекает также, что два класса эквивалентности либо не пересекаются, либо совпадают, так как если $z \in [x]$ и $z \in [y]$, то $x\rho z$, откуда $[x]=[z]$, и $y\rho z$, откуда $[y]=[z]$. Следовательно, $[x]=[y]$.

Совокупность классов эквивалентности элементов множества X по отношению эквивалентности ρ называется **фактор-множеством** множества X по отношению ρ и обозначается X/ρ .

1. 6. Порядок

Отношение ρ на множестве X называется *антисимметричным*, если для любых $x, y \in X$ из $x\rho y$ и $y\rho x$ следует $x = y$.

Рефлексивное, транзитивное и антисимметричное отношение называется отношением *частичного порядка* на множестве X и обозначается символом \sqsubseteq .

Пример 1. 13.

1. Отношение $x \leq y$ на множестве действительных чисел есть отношение частичного порядка.
2. Во множестве подмножеств некоторого универсального множества U отношение $A \subseteq B$ есть отношение частичного порядка.
3. Схема организации подчинения в учреждении есть отношение частичного порядка на множестве должностей.

Отношение частичного порядка на множестве X , для которого любые два элемента сравнимы, т. е. для любых $x, y \in X$ $x \sqsubseteq y$ или $y \sqsubseteq x$, называется отношением *линейного порядка*.

Пример 1.14. В примере 1.13 отношение, определенное в п. 1 есть отношение линейного порядка, а отношение, определенное в п. 2, таковым не является.

Заметим, что мы определили тип отношений, прообразом которых служит интуитивное понятие отношения порядка (предшествования, предпочтения).

Пусть на множестве X задано отношение частичного порядка ρ . Как можно задать отношение частичного порядка на множестве $X \times X$, т. е. как сравнивать пары элементов из множества X ? Один из возможных способов

состоит в следующем: на множестве $X \times X$ определяем отношение P условием $\langle a, b \rangle P \langle c, d \rangle \Leftrightarrow a \leq c$ и $b \leq d$. Отношение P есть отношение частичного порядка. Оно называется отношением Парето.

Множество X с заданным на нем частичным (линейным) порядком называется *частично (линейно) упорядоченным*.

2. ЛОГИКА ВЫСКАЗЫВАНИЙ

2.1. Зачем вы изучаете математическую логику?

Логика есть наука о законах и формах познающего мышления. Логика изучает мышление, но не всякое мышление, а лишь те мыслительные процессы, которые направлены на обнаружение и обоснование истины, на решение некоторой задачи, на поиск путей преодоления тех или иных трудностей, встающих перед нами как в профессиональной деятельности, так и в обыденной жизни.

Логику интересует лишь форма наших мыслей, но не их содержание. Разнообразие содержания укладывается в сравнительно небольшое число форм. Грубо говоря, логику интересуют сосуды - бутылки, ведра, бочки, - а не то, что в них налито.

В этом отношении логика сходна с грамматикой, которую мы изучали в школе. Грамматика тоже исследует и описывает формы языковых выражений, отвлекаясь от их содержания. Для иллюстрации этого обстоятельства известный лингвист Л. В. Щерба приводил пример следующего выдуманного им самим предложения: "Глокая куздра штеко будланула бокра и курдючит бокренка". Мы ничего не можем сказать о содержании этого предложения, но знание грамматики позволяет нам утверждать, что слово "куздра" здесь является подлежащим, "будланула" - сказуемым, "бокра" - дополнением и т. д. Мы можем говорить о роде, числе, падеже наших существительных, не имея ни малейшего представления о том, что обозначают соответствующие слова. Аналогичное знание о формах мысли дает нам логика.

При изучении логики мы вводим различные формальные языки. Дело в том, что формальные языки всегда проще, чем структура естественных языков. Иногда естественный язык может быть очень сложен.

Вот как, например, Марк Твен обыгрывает особенности словообразования в немецком языке:

"В одной немецкой газете, - уверяет он, - я сам читал такую весьма занятную историю:

Готтентоты (по-немецки: □хоттентотен□), как известно, ловят в пустынях кенгуру (по-немецки: □бейтельрате□ - сумчатая крыса). Они обычно сажают их в клетки (□коттэр□, снабженные решетчатыми крышками (□латтенгиттер□) для защиты от непогоды (□веттер□).

Благодаря замечательным правилам немецкой грамматики все это вместе - кенгуру и клетки - получают довольно удобное название:

□Латтенгиттерветтеркоттэрбейтельратте□.

Однажды в тех местах, в городе Шраттертроттэле, был схвачен негодяй, убивший готтентотку, мать двоих детей.

Такая женщина по-немецки должна быть названа □хоттентотенмуттер□, а ее убийца сейчас же получил в устах граждан имя □щраттертроттэльхоттентотенмуттэраттэнтэтэр□, ибо убийца - по-немецки □аттэнтэтэр□.

Преступника поймали и за неимением других помещений посадили в одну из клеток для кенгуру, о которых выше было сказано. Он бежал, но снова был изловлен. Счастливый своей удачей, негр-охотник быстро явился к старшине племени.

-Я поймал этого ... Бейтельратте? Кенгуру? - в волнении вскричал он.

-Кенгуру? Какого? - сердито спросил потревоженный начальник.

-Как какого? Этого самого! Латтенгиттерветтеркоттэрбейтельратте.

-Яснее! Таких у нас много... Непонятно, чему ты так радуешься?

-Ах ты, несчастье какое! - возмутился негр, положил на землю лук и стрелы, набрал в грудь воздуха и выпалил:

-Я поймал щраттертроттэльхоттентотенмуттэраттэнтэтэрлаттенгиттерветтеркоттэрбейтельратте! Вот кого!

Тут начальник подскочил, точно подброшенный пружиной:

-Так что же ты мне сразу не сказал этого так коротко и ясно, как сейчас?!"

Математическая логика - математический аппарат, направленный преимущественно к умозаключениям, применяемым в самой математике.

Математическая логика, возникшая почти 100 лет назад в связи с внутренними потребностями математики, нашла применение в теоретическом и практическом программировании и, судя по всему, взаимодействие этих двух наук в недалеком будущем сможет принести новые плоды.

Почему программисты обратились к математической логике, а логики заинтересовались программированием? Математическая логика, занимается построением формальных языков, предназначенных для представлений таких фундаментальных понятий, как функция, отношение, аксиома, доказательство, и изучение основанных на этих языках логических и логико-математических исчислений.

В недрах математической логики были найдены математически точные понятия алгоритма и вычислимой функции, развита семантика формальных языков и теорий, построены системы логического вывода - и все это, заметим было сделано в 30-40-х годах, в т. е. "докомпьютерную эру".

Программирование также имеет дело с формальными языками - языками программирования. Чтобы сделать эти языки удобными и естественными для человека полезно воспользоваться опытом математической логики. В результате появились принципиально новые языки функционального (Лисп, Clean) и логического (Пролог) программирования.

Для формализации семантики программы (это полезно при разработке трансляторов) необходим аппарат математической логики (уже использовались : λ -исчисление Черча, теория областей Дана Скотта).

Другие приложения математической логики в программировании:

- теория логического вывода;
- правильность программ относительно спецификаций;
- "доказательное" программирование - метод построения правильных программ;
- задачи представления и обработки знаний;
- параллельные вычисления;
- проблемы сложности вычислений;
- элементная логическая база компьютеров.

2.2. Высказывания

Под *высказыванием* принято понимать языковое предложение, о котором имеет смысл говорить, что оно истинно или ложно.

Высказываниями являются, например, следующие предложения: "дважды два - четыре", "5 - простое число", "Волга впадает в Черное море". Первые два предложения истинны, а третье - ложно. Предложения "Вашингтон - столица США", "Нью-Йорк - столица США", "царевич Дмитрий был убит по приказу Бориса Годунова" являются высказываниями, причем первое из них истинно, второе - ложное, а третье - неизвестно. Предложения " $x + y = 4$ " и "Который час?" высказываниями не являются. Предложения "Город стоит на берегу реки" и "Сегодня хорошая погода" тоже не следует относить к высказываниям ввиду их недостаточной точности.

В логике высказываний интересуются не содержанием, а *истинностью* или *ложностью* высказываний (т. е. их *истинностным значением*). Истинностные значения - *истина* и *ложь* - будем обозначать соответственно И и Л соответственно. Множество {И, Л} называется *множеством истинностных значений*.

Грамматическими средствами в разговорном языке из нескольких высказываний можно составить сложное (составное) высказывание. Например, с помощью союзов "и", "или" и отрицательной частицы "не" можно из простых высказываний "Москва стоит на берегу Невы" (ложного) "Санкт-Петербург стоит на берегу Невы" (истинного) составить следующие сложные высказывания: "Москва не стоит на берегу Невы", "Москва стоит на берегу Невы или Санкт-Петербург стоит на берегу Невы", "Москва стоит на берегу Невы и Санкт-Петербург стоит на берегу Невы". Первые два высказывания истинны, а последнее ложное.

2.3. Логические связи

Рассмотрим логические операции (связки) над высказываниями, при которых истинностные значения составных высказываний определяются только истинностными значениями составляющих высказываний, а не их смыслом.

Отрицанием высказывания P называется высказывание, истинное тогда и только тогда, когда высказывание P ложно. Отрицание P обозначается через $\neg P$ и читается как "не P ". Отрицание высказывания определяется также таблицей истинности (см. табл. 1).

В разговорной речи отрицание соответствует составлению из высказывания P нового высказывания, "неверно, что P ".

Таблица 1

P	$\neg P$
И	Л
Л	И

Конъюнкцией двух высказываний P и Q называется высказывание, истинное тогда и только тогда, когда истинны оба высказывания. Конъюнкция высказываний P и Q обозначается через $P \& Q$ и читается как " P и Q ". Конъюнкция определяется также таблицей истинности (см. табл. 2).

В разговорной речи конъюнкция соответствует соединению высказываний союзом "и".

Таблица 2

P	Q	$P \& Q$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	Л

Дизъюнкцией двух высказываний P и Q называется высказывание, ложное тогда и только тогда, когда оба высказывания ложны. Дизъюнкция высказываний P и Q обозначается через $P \vee Q$ и читается как " P или Q ". Дизъюнкция определяется также таблицей истинности (см. табл. 3).

В разговорной речи дизъюнкция соответствует соединению высказываний союзом "или" в "неразделительном смысле".

Таблица 3

P	Q	$P \vee Q$
И	И	И
И	Л	И
Л	И	И
Л	Л	Л

Из двух высказываний P и Q можно составить высказывание " P влечет Q " (или, иначе, "из P следует Q ", "если P , то Q "). Не математик может признать утверждение типа "если $2 \times 2 = 5$, то Москва - столица России" ложным, поскольку для него истинность высказывания " P влечет Q " означает, что P по смыслу должно влечь за собой Q . Но тогда связка "влечет" зависит от смысла самих этих высказываний. Однако практика показывает, что можно обороты типа " P влечет Q " и "из P следует Q " использовать таким образом, чтобы под ними каждый раз подразумевалась некоторая операция, не зависящая от смысла высказываний. Рассмотрим следующие высказывания:

- 1) если $0 = 0$, то $1 = 1$; 2) если $0 = 1$, то $0 = 0$;
3) если $0 = 0$, то $0 = 1$; 4) если $0 = 1$, то $1 = 2$.

Первое утверждение естественно считать истинным, поскольку, используя равенство $0 = 0$, а также другие свойства чисел, можно вывести равенство $1 = 1$ (например, прибавляя 1 к обеим частям равенства $0 = 0$).

Второе утверждение также естественно считать истинным: умножая на 0 обе части равенства $0 = 1$, получаем равенство $0 = 0$.

Третье утверждение приходится считать ложным, ибо, исходя из верного равенства, мы с помощью умозаключений никогда не приходим к ложному.

Четвертое рассуждение естественно считать истинным: прибавляя 1 к обеим частям равенства $0 = 1$, получаем равенство $1 = 2$.

Таким образом, используя оборот "если P , то Q " как логическую операцию (связку), определим её следующим образом. *Импликацией* двух высказываний P и Q называется высказывание, ложное тогда и только тогда, когда P - истинно, а Q - ложно. Импликация высказываний P и Q обозначается через $P \supset Q$ (или $P \Rightarrow Q$) и читается как " P влечет Q " (или, иначе, "если P , то Q ", "из P следует Q "). Высказывание P называется *посылкой* импликации, а высказывание Q - *заключением* импликации. Импликация определяется также таблицей истинности (см. табл. 4).

Таблица 4

P	Q	$P \supset Q$
И	И	И
И	Л	Л
Л	И	И
Л	Л	И

Эквиваленцией двух высказываний P и Q называется высказывание, истинное тогда и только тогда, когда истинностные значения P и Q совпадают. Эквиваленция высказываний P и Q обозначается через $P \sim Q$ и читается как " P эквивалентно Q ". Эквиваленция определяется также таблицей истинности (см. табл. 5).

Таблица 5

P	Q	$P \sim Q$
И	И	И
И	Л	Л
Л	И	Л
Л	Л	И

Задача 1. Кто из караванщиков убийца? В этой истории речь пойдет о караване, идущем через пустыню Сахару. Однажды караван остановился на ночлег. Обозначим трех главных действующих лиц A , B и C . A ненавидел C и решил убить его, подсыпав яду в бурдюк с питьевой водой (единственным запасом воды, которым располагал C). Независимо от A другой караванщик B также решил убить C и (не зная, что принадлежащая тому питьевая вода уже отравлена) проделал в бурдюке крохотную дырочку, чтобы вода потихоньку вытекала. Через несколько дней C умер от жажды. Спрашивается, кто убийца? A или B ?

2.4. Формулы логики высказываний

Алфавитом называется любое непустое множество. Элементы этого множества называются *символами* данного алфавита. *Словом* в данном алфавите называется произвольная конечная последовательность символов (возможно, пустая). Слово a называется *подсловом* слова b , если $b = b_1ab_2$ для некоторых слов b_1 и b_2 .

Алфавит логики высказываний содержит следующие символы: высказывательные переменные X_1, X_2, \dots ; логические символы $\&, \vee, \neg, \supset, \sim$; символы скобок $(,)$.

Слово в алфавите логики высказываний называется *формулой*, если оно удовлетворяет следующему определению:

- 1) любая высказывательная переменная - формула;
- 2) если A и B - формулы, то $(\neg A)$, $(A \& B)$, $(A \vee B)$, $(A \supset B)$, $(A \sim B)$ - формулы.
- 3) только те слова являются формулами, для которых это следует из 1) и 2).

Подформулой формулы A называется любое подслово A , само являющееся формулой.

Для упрощения записи будем в формуле опускать внешние скобки и те пары скобок, без которых можно восстановить эту формулу, если пользоваться следующим правилом: каждое вхождение знака \neg относится к наикратчайшей подформуле, следующей за ним.

Пример 2.1. Слово $(X_1 \& X_2) \supset X_3 \neg X_1$ не является формулой, а слова $(\neg X_1 \supset X_2) \vee X_1$, $(X_1 \sim X_2) \supset \neg X_3$ - формулы. Слова $X_1 \sim X_2$, $\neg X_3$, X_1 , X_2 , X_3 - подформулы последней формулы.

Принцип математической индукции, который будем использовать в рассуждениях, формулируется следующим образом: если какое-то высказывание $P(t)$, зависящее от натурального параметра t , доказано для $t = 0$ и при произвольном t удастся из истинности $P(t)$ обосновать истинность $P(t+1)$, то $P(t)$ истинно для всех t .

Будем применять также и другую формулировку этого принципа: если $P(t)$ истинно при $t = 0$ и для любого t из истинности $P(s)$ при всех $s \leq t$ следует истинность $P(t+1)$, то $P(t)$ истинно для всех t .

Применительно к высказывательным формулам принцип математической индукции можно сформулировать следующим образом:

если какое-то утверждение $P(F)$, зависящее от параметра F , который пробегает все множество высказывательных формул,

- истинно для всех формул, не содержащих логических символов (т. е. формул вида X_i);
 - и при любом натуральном n из того, что $P(F)$ истинно для всех формул F с числом логических символов, меньших n , следует, что $P(F)$ истинно для всех формул с n логическими символами,
- то $P(F)$ истинно для всех формул F .

Пример 2.2. Докажем методом математической индукции, что S_n - сумма натуральных чисел от 1 до n - равна $1/2 (n+1)n$.

Базис индукции. $S_1 = 1 = (2 \cdot 1)/2$.

Индуктивный переход. Пусть $S_n = 1/2 (n+1)n$. Тогда $S_{n+1} = S_n + n+1 = (n+1)n/2 + n+1 = (n^2 + n + 2n + 2)/2 = (n+1)(n+2)/2$, ч. и т. д.

Задача 2. Все лошади одной масти. То, что все лошади одной масти, можно доказать индукцией по числу лошадей в определенном табуне. Вот так:

"Если существует только одна лошадь, то она своей масти, так что база индукции тривиальна. Для индуктивного перехода предположим, что существует n лошадей (с номерами от 1 до n). По индуктивному предположению лошади с номерами от 1 до $n-1$ одинаковой масти и, аналогично, лошади с номерами от 2 до n имеют одинаковую масть. Но лошади посередине с номерами с 2 до $n-1$ не могут изменять масть в зависимости от того, как они сгруппированы - это лошади, а не хамелеоны. Поэтому лошади с номерами от

1 до n также должны быть одинаковой масти. Таким образом, все n лошадей одинаковой масти. Что и требовалось доказать".

Есть ли ошибка в приведенном рассуждении и какая именно?

Пусть $\{X_1, X_2, \dots, X_n\}$ - множество высказывательных переменных, входящих в формулу F . Если каждой высказывательной переменной придать истинностные значения И и Л, то формула F определяет *истинностную функцию* $\{И, Л\}^n \rightarrow \{И, Л\}$.

Эту истинностную функцию можно представить с помощью таблицы истинности.

Пример 2.3.

- 1) Таблица 6 - таблица истинности для формулы $(X_1 \supset X_2) \vee (X_1 \supset (X_1 \& X_2))$.
- 2) Таблица 7 - таблица истинности для формулы $(X_1 \supset X_2) \vee \neg X_3$.

Таблица 6

X_1	X_2	$X_1 \supset X_2$	$X_1 \& X_2$	$X_1 \supset (X_1 \& X_2)$	$(X_1 \supset X_2) \vee (X_1 \supset (X_1 \& X_2))$
И	И	И	И	И	И
И	Л	Л	Л	Л	Л
Л	И	И	Л	Л	И
Л	Л	И	Л	И	И

Таблица 7

X_1	X_2	X_3	$\neg X_3$	$X_1 \supset X_2$	$(X_1 \supset X_2) \vee \neg X_3$
И	И	И	Л	И	И
И	И	Л	И	И	И
И	Л	И	Л	Л	Л
И	Л	Л	И	Л	И
Л	И	И	Л	И	И
Л	И	Л	И	И	И
Л	Л	И	Л	И	И
Л	Л	Л	И	И	И

Упорядоченный набор высказывательных переменных $\langle X_1, X_2, \dots, X_n \rangle$ назовем *списком переменных формулы A*, если все переменные формулы содержатся в этом наборе.

В списке переменных формулы A часть переменных может быть фиктивной, т. е. не входить явно в формулу A .

Оценкой списка переменных назовем сопоставление каждой переменной списка некоторого истинностного значения.

Если в списке k переменных, то имеем 2^k оценок (и 2^k строк в соответствующей таблице истинности).

Пример 2.4. Для формулы $(X_1 \supset X_2) \vee (X_1 \supset (X_1 \& X_2))$ списком переменных является $\langle X_1, X_2 \rangle$ или $\langle X_1, X_2, X_3 \rangle$ или $\langle X_1, X_2, X_3, X_4 \rangle$ и т. д.

Пусть $\langle X_1, X_2, \dots, X_n \rangle$ - список переменных формулы F . Определим индуктивно значение формулы F на данной оценке списка:

- $F \equiv X_i$, тогда значение формулы F на данной оценке списка есть истинностное значение X_i ;
- $F \equiv (\neg A)$, тогда значение формулы F на данной оценке списка есть $\neg s$, где s - значение формулы A ;
- $F \equiv (A \& B)$ (или $(A \vee B)$ или $(A \supset B)$ или $(A \sim B)$), тогда значение формулы F на данной оценке списка есть $s \& t$ (или $s \vee t$ или $s \supset t$ или $s \sim t$), где s - значение формулы A , t - значение формулы B .

2.5. Равносильность формул

Пусть A и B - две формулы, зависящие от одного и того же списка переменных $\langle X_1, X_2, \dots, X_n \rangle$. Будем называть их равносильными, если на любой оценке списка $\langle X_1, X_2, \dots, X_n \rangle$ они принимают одинаковые оценки. Равносильность формул A и B будем обозначать $A \equiv B$. В определении равносильности безразлично какой список переменных берется.

Нужно различать символы \sim и \equiv . Так, \sim является символом формального языка, с помощью которого строятся формулы, а символ \equiv обозначает отношение на множестве формул.

Отношение равносильности есть отношение эквивалентности. Действительно, оно рефлексивно, так как для любой формулы A $A \equiv A$; симметрично, так как для любых формул A и B , если $A \equiv B$, то $B \equiv A$; транзитивно, так как для любых формул A, B, C , если $A \equiv B$ и $B \equiv C$, то $A \equiv C$.

Основные равносильности. Для любых формул A, B, C справедливы следующие равносильности:

1. $A \& B \equiv B \& A$ (коммутативность $\&$);
2. $A \& A \equiv A$ (идемпотентность $\&$);
3. $A \& (B \& C) \equiv (A \& B) \& C$ (ассоциативность $\&$);
4. $A \vee B \equiv B \vee A$ (коммутативность \vee);
5. $A \vee A \equiv A$ (идемпотентность \vee);
6. $A \vee (B \vee C) \equiv (A \vee B) \vee C$ (ассоциативность \vee);
7. $A \vee (B \& C) \equiv (A \vee B) \& (A \vee C)$ (дистрибутивность \vee относительно $\&$);
8. $A \& (B \vee C) \equiv (A \& B) \vee (A \& C)$ (дистрибутивность $\&$ относительно \vee);

9. $A \& (A \vee B) \equiv A$ (первый закон поглощения);
10. $A \vee (A \& B) \equiv A$ (второй закон поглощения);
11. $\neg \neg A \equiv A$ (снятия двойного отрицания);
12. $\neg (A \& B) \equiv \neg A \vee \neg B$ (первый закон де Моргана);
13. $\neg (A \vee B) \equiv \neg A \& \neg B$ (второй закон де Моргана);
14. $A \equiv (A \& B) \vee (A \& \neg B)$ (первый закон расщепления);
15. $A \equiv (A \vee B) \& (A \vee \neg B)$ (второй закон расщепления).

Все эти равносильности легко доказываются либо с помощью таблиц истинности, либо без них. В качестве примера, докажем 7 с помощью таблицы истинности.

Таблица 8

A	B	C	$B \& C$	$A \vee (B \& C)$	$A \vee B$	$A \vee C$	$(A \vee B) \& (A \vee C)$
И	И	И	И	И	И	И	И
И	И	Л	Л	И	И	И	И
И	Л	И	Л	И	И	И	И
И	Л	Л	Л	И	И	И	И
Л	И	И	И	И	И	И	И
Л	И	Л	Л	Л	И	Л	Л
Л	Л	И	Л	Л	Л	И	Л
Л	Л	Л	Л	Л	Л	Л	Л

Доказательство 12 без таблицы истинности.

Пусть на некоторой оценке списка переменных формула $\neg(A \& B)$ принимает значение Л. Тогда формула $A \& B$ принимает значение И, а поэтому обе формулы A и B принимают значение И. Но в этом случае, очевидно, и правая часть равносильности 12 принимает значение Л. И наоборот, пусть формула $\neg A \vee \neg B$ принимает значение Л. Тогда формулы $\neg A$, $\neg B$ принимают значение Л, а формулы A , B - значение И. Очевидно, что и левая часть равносильности 12 принимает значение Л.

Следующая группа равносильностей показывает, что одни связки могут быть выражены через другие:

16. $A \sim B \equiv (A \supset B) \& (B \supset A) \equiv (A \& B) \vee (\neg A \& \neg B)$;
17. $A \supset B \equiv \neg A \vee B \equiv \neg(A \& \neg B)$;
18. $A \vee B \equiv \neg A \supset B \equiv \neg(\neg A \& \neg B)$;
19. $A \& B \equiv \neg(A \supset \neg B) \equiv \neg(\neg A \vee \neg B)$.

В силу транзитивности отношения равносильности, если $A_1 \equiv A_2$, $A_2 \equiv A_3, \dots, A_{k-1} \equiv A_k$, то $A_1 \equiv A_k$. В таком случае для простоты будем записывать цепочку $A_1 \equiv A_2 \equiv A_3 \equiv \dots \equiv A_{k-1} \equiv A_k$.

Приведем правило, с помощью которого можно переходить от одних равносильностей к другим.

Лемма 2.1. Пусть $A \equiv B$ и C - произвольная формула. Тогда $\neg A \equiv \neg B$, $A \& C \equiv B \& C$, $C \& A \equiv C \& B$, $A \vee C \equiv B \vee C$, $C \vee A \equiv C \vee B$, $A \supset C \equiv B \supset C$, $C \supset A \equiv C \supset B$, $A \sim C \equiv B \sim C$, $C \sim A \equiv C \sim B$.

Докажем например равносильность $A \supset C \equiv B \supset C$. На произвольной оценке списка переменных, от которых зависят A , B , C , формулы A и B принимают одинаковое значение (скажем, s). Пусть t - значение C на этой оценке. Обе части рассматриваемой равносильности принимают одно и то же значение $s \supset t$.

Лемма 2.2. Пусть $A \equiv B$ и C - формула, в которой выделено одно вхождение переменной X_i . Пусть C_A получается из C заменой этого вхождения X_i на A , а C_B - из C заменой того же вхождения X_i на B . Тогда $C_A \equiv C_B$.

Докажем это индукцией по числу n логических символов в C . Если $n=0$, то формула C должна совпадать с X_i (так как в ней имеется вхождение переменной X_i). В этом случае C_A есть A , C_B есть B , $C_A \equiv C_B$ - не что иное, как $A \equiv B$.

Пусть лемма доказана для числа логических символов меньше n и пусть C - формула с n логическими символами. Она имеет вид $\neg D$, или $D \& E$, или $D \vee E$, или $D \supset E$, или $D \sim E$, причем в первом случае выделенное вхождение X_i содержится в D , а в остальных случаях - либо в D , либо в E , но не в D и E сразу. Рассмотрим, например, случай когда C имеет вид $D \supset E$ и выделенное вхождение X_i содержится в D . Заменяя X_i в этом вхождении в D на A и B , получаем соответственно формулы D_A и D_B . Ясно, что C_A есть $D_A \supset E$, а C_B есть $D_B \supset E$. Так как в формуле D , меньше логических символов, чем в C , то $D_A \equiv D_B$. Применим теперь лемму 2.1 в случае $A \supset C \equiv B \supset C$, где в роли A выступает D_A и в роли B - D_B , в роли C - E . В результате получаем $C_A \equiv C_B$. Другие случаи рассматриваются аналогично.

Теорема 2.1. (правило равносильных преобразований). Пусть C_A - формула, содержащая A в качестве своей подформулы. Пусть C_B получается из C_A заменой A в этом вхождении на B . Тогда, если $A \equiv B$, то $C_A \equiv C_B$.

Рассмотрим произвольную переменную X_i и получим формулу C из C_A заменой A на X_i . Будем считать это вхождение X_i в C выделенным. Тогда C , A , B , C_A , C_B удовлетворяют условиям леммы 2.2, а значит, $C_A \equiv C_B$.

Теорема 2.2 (правило устранения логических символов \supset и \sim). Для каждой формулы можно указать равносильную ей формулу, не содержащую логических символов \supset и \sim .

В самом деле, опираясь на правило равносильных преобразований, можно в исходной формуле каждую подформулу вида $A \sim B$ заменить на

$(A \& B) \vee (\neg A \& \neg B)$, а каждую подформулу вида $A \supset B$ на $\neg A \vee B$ (см. равносильности 16 и 17).

Пример 2.5. Формула $(X_1 \supset (X_2 \supset X_3)) \sim \neg(X_2 \supset X_1)$ преобразуется следующим образом: $(X_1 \supset (X_2 \supset X_3)) \sim \neg(X_2 \supset X_1) \equiv (X_1 \supset (\neg X_2 \vee X_3)) \sim (\neg(\neg X_2 \vee X_1)) \equiv (\neg X_1 \vee (\neg X_2 \vee X_3)) \sim (\neg(\neg X_2 \vee X_1)) \equiv ((\neg X_1 \vee (\neg X_2 \vee X_3)) \& \neg(\neg X_2 \vee X_1)) \vee (\neg(\neg X_1 \vee (\neg X_2 \vee X_3)) \& \neg \neg(\neg X_2 \vee X_1))$.

Задача 3. Четыре колпака в пещере. В темной пещере лежат 4 колпака – два белых и два черных. В пещеру входят 3 мудреца, они знают, сколько и каких колпаков находится в пещере, однако в темноте они не видят, какие колпаки на себя надевают. Надев колпаки, они по одному выходят из темноты пещеры на свет: первый идет, куда глаза глядят; второй идет за первым и видит, какого цвета на нем колпак; третий идет за вторым и видит, какого цвета колпаки на первом и втором. Найдется ли мудрец, который догадается, какого цвета на нем колпак и воскликнет "Я знаю!"?

2.6. Тавтоженно-истинные формулы

Пусть формула A зависит от списка переменных $\langle X_1, X_2, \dots, X_n \rangle$.

Формула A называется *тавтологией* (или *тождественно-истинной* формулой), если на любых оценках списка переменных $\langle X_1, X_2, \dots, X_n \rangle$ она принимает значение И.

Формула A называется *выполнимой*, если на некоторой оценке списка переменных $\langle X_1, X_2, \dots, X_n \rangle$ она принимает значение И.

Формула A называется *тождественно-ложной*, если на любых оценках списка переменных $\langle X_1, X_2, \dots, X_n \rangle$ она принимает значение Л.

Формула A называется *опровержимой*, если на некоторой оценке списка переменных $\langle X_1, X_2, \dots, X_n \rangle$ она принимает значение Л.

Как и в определении равносильности, здесь не имеет значения, будут ли в списке фиктивные переменные.

Приведем утверждения, которые являются очевидными следствиями данных определений:

- A - тавтология тогда и только тогда, когда A не является опровержимой;
- A - тождественно-ложна тогда и только тогда, когда A не является выполнимой;
- A - тавтология тогда и только тогда, когда $\neg A$ - тождественно-ложна;
- A - тождественно-ложна тогда и только тогда, когда $\neg A$ - тавтология;
- $A \sim B$ - тавтология тогда и только тогда, когда A и B - равносильны.

С точки зрения логики тавтологии суть не что, иное, как логические законы, ибо при любой подстановке вместо переменных тавтологии конкретных высказываний в результате получим истинное высказывание.

Перечислим наиболее важные тавтологии (A, B, C - произвольные формулы):

1. $A \vee \neg A$ (закон исключенного третьего или *tertium nondatur*);
2. $A \supset A$;
3. $A \supset (B \supset A)$;
4. $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$ (цепное рассуждение);
5. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;
6. $(A \& B) \supset A$; $(A \& B) \supset B$;
7. $A \supset (B \supset (A \& B))$;
8. $A \supset (A \vee B)$; $B \supset (A \vee B)$;
9. $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$;
10. $((A \supset B) \supset A) \supset A$ (закон Пирса).

Каждую из этих тавтологий можно обосновать, например, составив таблицу и вычислив по ней значение формулы при произвольных значениях A, B и C .

Задача 4. Остров рыцарей и лжецов. На острове жили рыцари, которые всегда говорили правду, и лжецы, которые всегда лгали.

Трое жителей острова (A, B и C) разговаривали между собой в саду. Проходивший мимо незнакомец спросил у A : "Сколько рыцарей среди вас?" На этот вопрос A ответил неразборчиво. Поэтому незнакомцу пришлось спросить у B : "Что сказал A ?" B ответил: " A сказал, что среди нас один рыцарь". И тогда C закричал "Не верьте B ! Он лжет".

Кто из двух персонажей B и C рыцарь и кто лжец?

2. 7. Правильные рассуждения

При доказательстве утверждений различных математических теорий обычно используют рассуждения, которые на языке логики можно выразить формулами.

Рассуждение называется *правильным*, если из конъюнкции посылок следует заключение, т. е. всякий раз, когда посылки истинны, заключение тоже истинно.

Пусть P_1, P_2, \dots, P_n - посылки, D - заключение. Тогда для определения правильности рассуждения по схеме $\frac{P_1, P_2, \dots, P_n}{D}$, т. е. утверждения о том, что из данных посылок P_1, P_2, \dots, P_n следует заключение D , требуется установить тождественную истинность формулы $(P_1 \& P_2 \& \dots \& P_n) \supset D$.

Так как речь идет лишь о правильности рассуждения, истинность заключения не является ни необходимым, ни достаточным условием правильности рассуждения.

Пример 2.6. Рассмотрим два рассуждения:

1. Если число 5 простое, то оно нечетное. Число 5 нечетное. Следовательно, число 5 простое. Заключение истинно, но рассуждение не правильное. Это рассуждение по схеме $\frac{A \supset B, B}{A}$. Легко проверить, что формула $((A \supset B) \& B) \supset A$ не является тавтологией.
2. Если Петр занимается спортом, то Петр никогда не болеет. Петр занимается спортом. Следовательно, Петр никогда не болеет. Это рассуждение по схеме $\frac{A \supset B, A}{B}$. Формула $((A \supset B) \& A) \supset B$ тождественно-истинна, и, значит, рассуждение правильное.

Распространенными схемами правильного рассуждения являются следующие схемы: $\frac{A \supset B, A}{B}$ и $\frac{A \supset B, \neg B}{\neg A}$.

Рассмотрим условное высказывание вида $A \supset B$, где A - конъюнкция посылок, B - заключение. Иногда удобнее вместо доказательства истинности этого условного высказывания установить логическую истинность некоторого другого высказывания, равносильного исходному. Такие формы доказательства называются косвенными методами доказательства.

Одним из них является способ доказательства от противного. Предположим, что утверждение $A \supset B$ ложно. Тогда, исходя из этого предположения, приходим к противоречию, т. е. доказываем, что некоторое утверждение (соответствующее высказыванию C) выполняется и не выполняется (одновременно). Применимость этой формы косвенного метода доказательства оправдывается равносильностью

$$A \supset B \equiv \neg(A \supset B) \supset (C \& \neg C) \equiv (A \& \neg B) \supset (C \& \neg C).$$

Существуют и другие схемы доказательства от противного:

$$A \supset B \equiv (A \& \neg B) \supset \neg A,$$

$$A \supset B \equiv (A \& \neg B) \supset B.$$

Еще одной формой косвенного метода доказательства, является доказательство по закону контрапозиции, основанное на равносильности

$$A \supset B \equiv \neg B \supset \neg A,$$

когда вместо истинности $A \supset B$ мы доказываем истинность $\neg B \supset \neg A$.

Решение следующей задачи поможет вам лучше понять, как математическая логика относится к реальному миру.

Задача 5. Две шкатулки. Перед вами две шкатулки, серебряная и золотая. На крышках шкатулок надписи. На золотой: "Приз не в этой шкатулке". На серебряной: "Ровно одно из двух высказываний, выгравированных на крышках истинно". В какой шкатулке приз?

2.8. Нормальные формы формул

Будем рассматривать формулы, содержащие только логические операции $\&$, \vee , \neg . Символы $\&$ и \vee называются *двойственными* друг другу.

Формула A^* называется *двойственной* формуле A , если она получена из A одновременной заменой всех символов $\&$, \vee на двойственные. Например, формула $X_1 \& (X_2 \vee \neg X_1)$ двойственна формуле $X_1 \vee (X_2 \& \neg X_1)$.

Очевидно, что $(A^*)^*$ совпадает с A .

Теорема 2.3. (принцип двойственности) Если $A \equiv B$, то $A^* \equiv B^*$.

Принцип двойственности можно использовать для нахождения новых равносильностей. Например, используя следующий частный случай дистрибутивности $\&$ относительно \vee

$$X \& (Y \vee Z) \equiv (X \& Y) \vee (X \& Z),$$

получаем равносильность

$$X \vee (Y \& Z) \equiv (X \vee Y) \& (X \vee Z).$$

Заметим, что в силу ассоциативности операций $\&$ и \vee , как бы мы не расставляли скобки в выражениях $A_1 \& A_2 \& \dots \& A_n$ и $A_1 \vee A_2 \vee \dots \vee A_n$ ($n > 3$), всегда будем приходить к равносильным формулам. Допуская некоторую вольность речи, каждое из этих выражений будем считать формулами и называть соответственно многочленной конъюнкцией и дизъюнкцией формул A_1, A_2, \dots, A_n . Для этих формул, используя, например, индукцию по $\max(k, n)$, нетрудно получить равносильности, выражающие обобщенную дистрибутивность (для простоты записи, положим $k=2, n=3$):

$$\begin{aligned} (A_1 \vee A_2) \& (B_1 \vee B_2 \vee B_3) &\equiv (A_1 \& B_1) \vee (A_1 \& B_2) \vee (A_1 \& B_3) \vee \\ &\quad (A_2 \& B_1) \vee (A_2 \& B_2) \vee (A_2 \& B_3), \\ (A_1 \& A_2) \vee (B_1 \& B_2 \& B_3) &\equiv (A_1 \vee B_1) \& (A_1 \vee B_2) \& (A_1 \vee B_3) \& \\ &\quad (A_2 \vee B_1) \& (A_2 \vee B_2) \& (A_2 \vee B_3). \end{aligned}$$

Точно также получаем обобщенные законы де Моргана:

$$\begin{aligned} \neg(A_1 \& A_2 \& \dots \& A_n) &\equiv \neg A_1 \vee \neg A_2 \vee \dots \vee \neg A_n, \\ \neg(A_1 \vee A_2 \vee \dots \vee A_n) &\equiv \neg A_1 \& \neg A_2 \& \dots \& \neg A_n. \end{aligned}$$

Определим теперь некоторые канонические виды формул.

Формула называется *элементарной конъюнкцией*, если она является конъюнкцией (быть может, одночленной) переменных и отрицаний перемен-

ных. Например, формулы $\neg X_2$, X_1 , $X_1 \& X_2$, $X_1 \& \neg X_2 \& \neg X_1 \& X_4$ являются элементарными конъюнкциями.

Говорят, что формула находится в *дизъюнктивной нормальной форме* (ДНФ), если она является дизъюнкцией (быть может, одночленной) элементарных конъюнкций. Например, формулы $\neg X_2$, X_1 , $X_1 \& X_2$, $X_1 \& \neg X_2 \& \neg X_1 \& X_4$, $(X_1 \& X_2) \vee (X_1 \& \neg X_2 \& \neg X_1 \& X_4) \& X_1$ находятся в ДНФ.

Теорема 2.4 (о приведении к ДНФ). Для любой формулы A можно найти такую формулу B , находящуюся в ДНФ, что $A \equiv B$. Формула B называется *дизъюнктивной нормальной формой формулы A* .

Доказательство теоремы распадается на три этапа:

1-ый этап. Для формулы A строим такую формулу A_1 , что $A \equiv A_1$ и в A_1 не содержатся символы \sim и \supset (теорема 2.2).

2-ой этап. Докажем теперь, что для формулы A_1 можно найти формулу A_2 такую, что $A_1 \equiv A_2$ и в A_2 отрицание находится только перед переменными. Такая формула называется формулой с "тесными" отрицаниями. Докажем это утверждение математической индукцией по числу n логических символов формулы A_1 .

Если $n=0$, то A_1 есть какая-то переменная X_i . В качестве A_2 нужно взять X_i .

Пусть утверждение выполняется для всех формул A_1 с числом символов меньше n . Пусть в формуле A_1 содержится точно n логических символов. Рассмотрим следующие случаи:

- 1) A_1 имеет вид $B_1 \vee C_1$. Тогда в B_1 , C_1 логических символов меньше, чем n . Поэтому существуют формулы B_2 , C_2 такие, что $B_1 \equiv B_2$, $C_1 \equiv C_2$ и в B_2 и C_2 отрицание встречается только перед переменными. Ясно, что $B_2 \vee C_2$ равносильна A_1 и является формулой с "тесными" отрицаниями;
- 2) A_1 имеет вид $B_1 \& C_1$. Доказательство аналогично предыдущему случаю;
- 3) A_1 имеет вид $\neg \neg B_1$. Тогда $A_1 \equiv B_1$ в B_1 логических символов меньше, чем n . Поэтому к B_1 применимо индуктивное предположение;
- 4) A_1 имеет вид $\neg (B_1 \vee C_1)$. Тогда $A_1 \equiv \neg B_1 \& \neg C_1$ и в $\neg B_1$, $\neg C_1$ логических символов меньше, чем n . Поэтому существуют такие формулы B_2 , C_2 , что $\neg B_1 \equiv B_2$, $\neg C_1 \equiv C_2$ и в B_2 и C_2 отрицание встречается только перед переменными. Ясно, что $A_1 \equiv B_2 \& C_2$ и $B_2 \& C_2$ является формулой с "тесными" отрицаниями;
- 5) A_1 имеет вид $\neg (B_1 \& C_1)$. Тогда $A_1 \equiv \neg B_1 \vee \neg C_1$, и далее поступаем как в предыдущем случае.

При практическом преобразовании встречающиеся в формуле отрицания просто передвигают к переменным, используя законы де Моргана и уничтожая пары стоящих рядом отрицаний, если таковые встречаются.

Пример 2.7. Преобразуем к формуле с "тесными" отрицаниями:

$$\begin{aligned} \neg(\neg\neg(X_1 \& \neg X_2) \vee (X_2 \& \neg X_1)) &\equiv \neg\neg\neg(X_1 \& \neg X_2) \& \neg(X_2 \& \neg X_1) \equiv \\ \neg(X_1 \& \neg X_2) \& (\neg X_2 \vee \neg\neg X_1) &\equiv (\neg X_1 \vee \neg\neg X_2) \& (\neg X_2 \vee X_1) \equiv \\ (\neg X_1 \vee X_2) \& (\neg X_2 \vee X_1). \end{aligned}$$

3-ий этап. Полученная формула A_2 построена из переменных и их отрицаний с помощью многочленных конъюнкций и дизъюнкций. Применив теперь обобщенную дистрибутивность $\&$ относительно \vee , последовательно преобразуем формулу (аналогично приведению алгебраического выражения, составленного из переменных, с помощью сложений и умножений, к виду многочлена). Заметим, что при этом \vee аналогично сложению, а $\&$ - умножению. Полученная в результате преобразований формула B будет удовлетворять требованиям теоремы.

Пример 2.8. Применим преобразования третьего этапа к формуле с "тесными" отрицаниями, полученной в примере 2.7:

$$(\neg X_1 \vee X_2) \& (\neg X_2 \vee X_1) \equiv (\neg X_1 \& \neg X_2) \vee (\neg X_1 \& X_1) \vee (X_2 \& \neg X_2) \vee (X_2 \& X_1).$$

Говорят, что формула A находится в *конъюнктивной нормальной форме* (КНФ), если формула A^* определена (т. е. в A нет символов \sim и \supset) и находится в ДНФ.

КНФ можно дать и другое равносильное определение. Формулу называют *элементарной дизъюнкцией*, если она является дизъюнкцией (возможно, одночленной) переменных и отрицаний переменных. Формула находится в КНФ, если она является конъюнкцией (возможно, одночленной) элементарных дизъюнкций.

Теорема 2.5 (о приведении к КНФ). Для любой формулы A можно найти такую формулу B , что A находится в КНФ и $A \equiv B$. Формула B называется *конъюнктивной нормальной формой формулы A* .

Первое доказательство. Пусть $A \equiv A_1$ и A_1 не содержит символов \sim , \supset . Пусть B_1 - дизъюнктивная нормальная форма формулы A_1^* . Тогда B_1^* находится в КНФ и, кроме того, по принципу двойственности $B_1^* \equiv (A_1^*)^* \equiv A_1 \equiv A$. Значит, B_1^* удовлетворяет требованиям теоремы.

Второе доказательство. Применив первые два этапа из доказательства теоремы 2.6 о ДНФ, получим формулу A_2 , равносильную A , не содержащую символов \sim , \supset и содержащую отрицания только перед переменными. Преобразуем теперь A_2 как алгебраическое выражение, считая на этот раз $\&$ аналогом сложения, а \vee - аналогом умножения и применяя дистрибутивность \vee относительно $\&$. Приведение формулы A_2 к виду многочлена даст на этот раз КНФ.

Пример 2.9. Приведем к КНФ формулу:

$$\begin{aligned}
& (X_1 \& X_2) \sim (\neg X_1 \& X_3) \equiv \\
& ((X_1 \& X_2) \& (\neg X_1 \& X_3)) \vee (\neg (X_1 \& X_2) \& \neg (\neg X_1 \& X_3)) \equiv \\
& (X_1 \& X_2 \& \neg X_1 \& X_3) \vee ((\neg X_1 \vee \neg X_2) \& (\neg \neg X_1 \vee \neg X_3)) \equiv \\
& (X_1 \& X_2 \& \neg X_1 \& X_3) \vee ((\neg X_1 \vee \neg X_2) \& (X_1 \vee \neg X_3)) \equiv \\
& (X_1 \vee \neg X_1 \vee \neg X_2) \& (X_1 \vee X_1 \vee \neg X_3) \& (X_2 \vee \neg X_1 \vee \neg X_2) \& (X_2 \vee X_1 \vee \neg X_3) \& \\
& (\neg X_1 \vee \neg X_1 \vee \neg X_2) \& (X_1 \vee X_1 \vee \neg X_3) \& (X_3 \vee \neg X_1 \vee \neg X_2) \& \\
& (X_3 \vee X_1 \vee \neg X_3).
\end{aligned}$$

Заметим, что первое преобразование основано на равносильности 16.

Нетрудно видеть, что ДНФ и КНФ не являются однозначно определенными. Формула может иметь несколько равносильных друг другу ДНФ и КНФ.

Задача 6. Примечания Литлвуда

Английский математик Дж. Литлвуд в своей книге "Математическая смесь" приводит в качестве примера (якобы) бесконечного повторения три примечания, сделанные в конце одной из его статей. Статья была опубликована во французском журнале и примечания (на французском языке) гласили:

1. Я весьма признателен проф. Риссу за перевод настоящей статьи.
2. Я признателен проф. Риссу за перевод предыдущего примечания.
3. Я признателен проф. Риссу за перевод предыдущего примечания.

Предположим, что Литлвуд совершенно не знает французского языка. С помощью какого рассуждения (и действий) он может избежать бесконечного повторения одинаковых примечаний и остановиться на третьем примечании?

2.9. Разрешимость для логики высказываний

Проблемой разрешимости для логики высказываний называют следующую проблему: существует ли алгоритм, который позволил бы для произвольной формулы в конечном числе шагов определить, является ли она тавтологией?

Ясно, что эта проблема разрешима, поскольку всегда можно перебрать все оценки списка переменных и вычислить на них значения формулы. Опишем другую более экономичную процедуру распознавания, связанную с приведением формулы к КНФ.

Теорема 2.6. Формула является тавтологией в том и только том случае, если в ее КНФ в любую из элементарных дизъюнкций в качестве дизъюнктивных членов входит какая-нибудь переменная и ее отрицание.

Двойственное утверждение справедливо и для тождественно-ложной формулы.

Теорема 2.7. Формула является тождественно-ложной в том и только том случае, если в ее ДНФ каждая элементарная конъюнкция одновременно содержит в качестве конъюнктивных членов какую-нибудь переменную и ее отрицание.

Задача 7. Каким образом удалось Канту поставить верное время?

Известно, что Кант был холостяком и имел столь укоренившиеся привычки, что жители Кенигсберга, завидев, как он проходил мимо того или иного дома, могли проверять по нему свои часы.

Однажды вечером Кант с ужасом обнаружил, что его стенные часы отстали. Очевидно, слуга, который в тот день уже кончил работать, забыл их завести. Великий философ никак не мог узнать, который час, ибо его наручные часы находились в ремонте, поэтому он не стал переставлять стрелки, а пошел в гости к своему другу Шмидту, купцу, жившему примерно в миле от Канта. Войдя в дом, Кант взглянул на часы в прихожей и, пробыв в гостях несколько часов, отправился домой. Он возвращался по той же дороге, что и всегда, медленно, степенной походкой, которая не менялась у него в течение двадцати лет. Кант не имел не малейшего представления о том, сколько времени он шел домой. Однако, войдя в свой дом, он сразу же поставил часы правильно. Каким образом Кант сумел узнать верное время?

3. БУЛЕВЫ АЛГЕБРЫ

Характерная черта современных компьютеров - сведение всех вычислительных структур (чисел, символов, массивов и т. п.) к двоичным словам и алгоритмам их обработки. С математической точки зрения мы имеем дело с частным случаем булевых алгебр.

3.1. Абстрактное определение булевых алгебр

Множество элементов с заданным на нем двуместными операциями \wedge и \vee (конъюнкцией и дизъюнкцией) и одноместной операцией \neg (отрицанием) называется *булевой алгеброй*, если выполнены следующие законы (f, g, h - произвольные элементы множества):

1. $f \wedge g = g \wedge f, f \vee g = g \vee f$ (коммутативность);
2. $(f \wedge g) \wedge h = f \wedge (g \wedge h), (f \vee g) \vee h = f \vee (g \vee h)$ (ассоциативность);
3. $f \wedge f = f, f \vee f = f$ (идемпотентность);
4. $f \wedge (g \vee f) = f, f \vee (g \wedge f) = f$ (законы поглощения);
5. $f \wedge (g \vee h) = (f \wedge g) \vee (f \wedge h), f \vee (g \wedge h) = (f \vee g) \wedge (f \vee h)$ (дистрибутивность);
6. $\neg(\neg f) = f$ (закон инволюции);
7. $\neg(f \wedge g) = \neg f \vee \neg g, \neg(f \vee g) = \neg f \wedge \neg g$ (законы де Моргана);
8. $f \wedge (g \vee \neg g) = f, f \vee (g \wedge \neg g) = f$ (законы нейтральности).

Из перечисленных законов можно вывести, что для произвольных f, g справедливы равенства $f \wedge \neg f = g \wedge \neg g$ и $f \vee \neg f = g \vee \neg g$. Например, в силу законов нейтральности и коммутативности имеем

$$f \wedge \neg f = (f \wedge \neg f) \vee (g \wedge \neg g) = (g \wedge \neg g) \vee (f \wedge \neg f) = g \wedge \neg g.$$

Если обозначить $f \wedge \neg f$ через ϵ и $f \vee \neg f$ через \varnothing , то выполняются равенства

$$\begin{aligned} \neg \varnothing &= \epsilon, & \neg \epsilon &= \varnothing, \\ f \wedge \varnothing &= f, & f \wedge \epsilon &= \epsilon, \\ f \vee \varnothing &= \varnothing, & f \vee \epsilon &= f. \end{aligned}$$

Булева алгебра называется *вырожденной*, если ϵ и \varnothing совпадают; в таком случае ввиду равенств $f = f \wedge \varnothing = f \wedge \epsilon = \epsilon$ она не содержит никаких других элементов, а значит состоит ровно из одного элемента. Всякая невырожденная булева алгебра - а только такие и будут рассматриваться в дальнейшем - содержит два *нейтральных элемента*: ϵ (*нулевой элемент*) и \varnothing (*единичный элемент*).

Из $f \wedge g = \varnothing$ следует, что $f = g = \varnothing$. Действительно, $f = f \vee (f \wedge g) = f \vee \varnothing = \varnothing$. Этот факт называют неразложимостью нейтрального элемента \varnothing .

Сейчас укажем некоторые модели - конкретные примеры булевых алгебр.

Двоичная модель

Булева алгебра содержит только два (нейтральных) элемента и операции на ней вводятся с помощью следующих таблиц значений.

\wedge	\varnothing	\in
\varnothing	\varnothing	\in
\in	\in	\in

\vee	\varnothing	\in
\varnothing	\varnothing	\varnothing
\in	\varnothing	\in

	\varnothing	\in
\neg	\in	\varnothing

Модель исчисления высказываний

Булева алгебра содержит только два элемента И и Л (И является единичным элементом, Л - нулевым). Операции \wedge , \vee , \neg - обычные логические операции конъюнкции, дизъюнкции и отрицания.

Теоретико-множественная модель

Пусть A - непустое множество, тогда множество-степень $P(A)$ является моделью булевой алгебры, если условиться о следующем.

Элементы этой булевой алгебры - это различные подмножества множества A .

Операция \wedge определяется как пересечение множеств, операция \vee обозначает объединение множеств и операция \neg является абсолютным дополнением (до A). Нетрудно убедиться, что все аксиомы булевой алгебры при таких определениях выполнены и множества A и \emptyset являются соответственно единичным и нулевым элементом алгебры.

Кроме конъюнкции и дизъюнкции особенно важны с точки зрения технической реализации переключательных функций следующие операции:

$f \downarrow g = \neg(f \vee g)$ (функция Пирса);

$f | g = \neg(f \wedge g)$ (штрих Шеффера);

$f \supset g = \neg f \vee g$ (импликация);

$f \setminus g = f \wedge \neg g$ (разность, теоретико-множественная разность в $P(A)$);

$f \sim g = (f \wedge g) \vee (\neg f \wedge \neg g)$ (эквивалентность);

$f + g = (f \wedge \neg g) \vee (\neg f \wedge g)$ (симметрическая разность, исключающее "или", неэквивалентность).

Для произвольного элемента f булевой алгебры имеем:

$$\epsilon \supset f = \varnothing, \quad \varnothing \supset f = f,$$

$$f \supset \varnothing = \varnothing, \quad f \supset \epsilon = \neg f.$$

Кроме того, $f \setminus g = \neg(f \supset g)$.

Для симметрической разности имеем также

$$f + g = (f \setminus g) \vee (g \setminus f)$$

$$f + g = \neg(f \sim g)$$

$$\epsilon + \epsilon = \epsilon \quad \epsilon + \varnothing = \varnothing$$

$$\varnothing + \epsilon = \varnothing \quad \varnothing + \varnothing = \epsilon$$

При отождествлении ϵ с 0, а \varnothing с 1, получаем операцию сложения по модулю 2:

$$0+0=0 \quad 1+0=1$$

$$1+1=0 \quad 0+1=1$$

Возможно теперь стало понятным почему основные равносильности логики высказываний и основные тождества алгебры множеств так похожи - они просто законы булевой алгебры.

На основании законов булевой алгебры можно доказывать утверждения о тождественности (эквивалентности) выражений с булевыми операциями. Например, $(f \wedge g) \vee (\neg f \wedge b) \vee (f \wedge \neg g) = g \vee f$. Действительно,

$$\begin{aligned} & (f \wedge g) \vee (\neg f \wedge b) \vee (f \wedge \neg g) = \\ & ((f \wedge g) \vee (\neg f \wedge g)) \vee (f \wedge \neg g) = \\ & ((f \vee \neg f) \wedge g) \vee (f \wedge \neg g) = \\ & (\epsilon \wedge g) \vee (f \wedge \neg g) = \\ & g \vee (f \wedge \neg g) = \\ & (g \vee f) \wedge (g \vee \neg g) = \\ & (g \vee f) \wedge \epsilon = \\ & g \vee f. \end{aligned}$$

Докажем, что все булевы выражения можно выразить через функцию Пирса. Для этого достаточно показать представимость с помощью функции Пирса базисных операций \wedge , \vee , \neg .

Имеем

$$\neg f = \neg(f \vee f) = f \downarrow f.$$

Далее, по определению,

$$f \downarrow g = \neg(f \vee g) \Rightarrow f \vee g = \neg(f \downarrow g) \Rightarrow f \vee g = (f \downarrow g) \downarrow (f \downarrow g).$$

И, наконец,

$$f \wedge g = \neg(\neg f \vee \neg g) = (\neg f) \downarrow (\neg g) = (f \downarrow f) \downarrow (g \downarrow g).$$

Задача 8. Теорема о неподвижной точке

Однажды утром, как раз в тот момент, когда взошло солнце, один буддийский монах начал восхождение на высокую гору. Узкая тропа шириной не более одного-двух футов вилась серпантином по склону горы к сверкающему храму на ее вершине.

Монах шел по дорожке с разной скоростью; он часто останавливался, чтобы отдохнуть и поест сушеных фруктов, которые взял с собой. К храму он пошел незадолго до захода солнца. После нескольких дней поста и размышлений монах пустился в обратный путь по той же тропе. Он вышел на рассвете и опять спускался с неодинаковой скоростью, много раз отдыхая по дороге. Средняя скорость спуска, конечно, превышала среднюю скорость подъема. Докажите, что на тропе есть такая точка, которую монах во время спуска и во время подъема проходил в одно и то же время суток.

3.2. Булевы функции. Теорема о нормальной булевой форме

Рассмотрим еще одну модель булевой алгебры. Пусть M - произвольная булева алгебра с базисными операциями \wedge , \vee , \neg . Рассмотрим множество n -местных функций

$$f: M^n \rightarrow M$$

с поточечно определенными операциями \wedge , \vee и \neg . А именно, пусть

$$f: (x_1, x_2, \dots, x_n) \rightarrow f(x_1, x_2, \dots, x_n).$$

Тогда, по определению,

$$f_1 \wedge f_2: (x_1, x_2, \dots, x_n) \rightarrow f_1(x_1, x_2, \dots, x_n) \wedge f_2(x_1, x_2, \dots, x_n),$$

$$f_1 \vee f_2: (x_1, x_2, \dots, x_n) \rightarrow f_1(x_1, x_2, \dots, x_n) \vee f_2(x_1, x_2, \dots, x_n),$$

$$\neg f: (x_1, x_2, \dots, x_n) \rightarrow \neg f(x_1, x_2, \dots, x_n).$$

Множество таким образом определенных функций вместе с введенными операциями является булевой алгеброй и *называются булевыми функциями*.

Две постоянные функции

$$0: (x_1, x_2, \dots, x_n) \rightarrow \in$$

$$1: (x_1, x_2, \dots, x_n) \rightarrow \not\in$$

являются соответственно нулевым и единичным нейтральным элементом.

Если булева алгебра M - двухэлементна (т. е. содержит только $\not\in$ и \in), то булевы функции называются *двоичными функциями*.

Если в двухэлементной булевой алгебре элементы $\not\in$ и \in интерпретировать как "включено" и "выключено", то двоичные функции называются *переключаемыми функциями*. При такой интерпретации $\not\in$ и \in обозначаются соответственно через 1 и 0.

Если $M = \{И, Л\}$ - булева алгебра значений истинности, то булевы функции являются функциями истинности или функциями логики высказываний.

Переключательные функции одной переменной имеют вид

$$f: \{0,1\} \rightarrow \{0,1\},$$

и может быть только четыре различных одноместных переключательных функций:

$$0: x \rightarrow 0;$$

$$1: x \rightarrow 1;$$

$$id: x \rightarrow x, \text{ тождественная функция};$$

$$neg: x \rightarrow \neg x, \text{ функция отрицания}.$$

Всякую переключательную функцию от n переменных можно задать таблицей из 2^n строк, в которой в каждой строке записывают одну из оценок списка переменных, принимающих значение 0 или 1. Например, для $n=3$ переключательную функцию можно задать таблицей 9.

Таблица 9

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

Так как длина каждого столбца равна 2^n , а различных столбцов из 0 и 1 длины 2^n имеется $2^{(2^n)}$, то существует точно $2^{(2^n)}$ переключательных функций от n переменных. В частности, при $n=2$ имеем 16 различных переключательных функций.

Вопрос: Нельзя ли свести все переключательные функции к какому-нибудь меньшему числу "базисных" переключательных функций?

Ответ: это возможно. Например, можно все переключательные функции представить как композицию только трех функций:

$$(\text{двуместная конъюнкция}) \wedge : (x_1, x_2) \rightarrow x_1 \wedge x_2;$$

$$(\text{двуместная дизъюнкция}) \vee : (x_1, x_2) \rightarrow x_1 \vee x_2;$$

$$(\text{одноместная функция отрицания}) \neg : x \rightarrow \neg x.$$

Лемма 3.1. Для всякой n -местной переключательной функции f выполняется соотношение

$$f(a_1, a_2, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) = \\ (a_i \wedge f(a_1, a_2, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)) \vee (\neg a_i \wedge f(a_1, a_2, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n)).$$

Для доказательства рассмотрим два случая.

1. Пусть $a_i=1$, тогда $\neg a_i=0$. Правая часть доказываемого соотношения равна $(1 \wedge f(a_1, a_2, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)) \vee (0 \wedge f(a_1, a_2, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n))$. Первый член в дизъюнкции равен $f(a_1, a_2, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$, а второй 0. Следовательно, правая часть равна $f(a_1, a_2, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$, но точно такое же значение имеет левая часть.
2. Пусть $a_i=0$. Совершенно аналогично получаем, что правая часть равна $f(a_1, a_2, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n)$.

Эта лемма позволяет "выносить" переменную a_i за знак переключательной функции. Последовательным применением леммы к a_1, a_2, \dots, a_n устанавливается

Теорема 3.1 (о булевой нормальной форме). Каждую переключательную функцию можно однозначно представить в следующей (дизъюнктивной) нормальной форме:

$$f(a_1, a_2, \dots, a_n) = \\ (a_1 \wedge a_2 \wedge \dots \wedge a_{n-1} \wedge a_n \wedge f(1, 1, \dots, 1, 1)) \\ \vee (\neg a_1 \wedge a_2 \wedge \dots \wedge a_{n-1} \wedge a_n \wedge f(0, 1, \dots, 1, 1)) \\ \vee (a_1 \wedge \neg a_2 \wedge \dots \wedge a_{n-1} \wedge a_n \wedge f(1, 0, \dots, 1, 1)) \\ \dots \\ \vee (\neg a_1 \wedge \neg a_2 \wedge \dots \wedge \neg a_{n-1} \wedge a_n \wedge f(0, 0, \dots, 0, 1)) \\ \vee (\neg a_1 \wedge \neg a_2 \wedge \dots \wedge \neg a_{n-1} \wedge \neg a_n \wedge f(0, 0, \dots, 0, 0)).$$

Если $f(a_1, a_2, \dots, a_{n-1}, a_n)=0$, то соответствующий член, разумеется выпадает из представления. Таким образом, всякая переключательная функция представима в виде дизъюнкции k , $0 \leq k \leq 2^k$, членов - так называемых *совершенных конъюнкций*, каждая совершенная конъюнкция - это n -местная конъюнкция, у которых все аргументы - либо сами переменные, либо их отрицания.

Пример 3.1. Переключательную функцию с таблицей значений

a_1	1	0	1	0	1	0	1	0
a_2	1	1	0	0	1	1	0	0
a_3	1	1	1	1	0	0	0	0
$f(a_1, a_2, a_3)$	1	0	0	1	0	1	1	0

можно представить в виде

$$f(a_1, a_2, a_3) = (a_1 \wedge a_2 \wedge a_3) \vee (\neg a_1 \wedge \neg a_2 \wedge a_3) \vee (\neg a_1 \wedge a_2 \wedge \neg a_3) \vee (a_1 \wedge \neg a_2 \wedge \neg a_3).$$

Всего имеется 16 двуместных переключательных функций. Они распадаются на следующие группы:

Функция без совершенных конъюнкций

$$f(x_1, x_2) = 0$$

Функция со всеми четырьмя совершенными конъюнкциями

$$f(x_1, x_2) = (x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2) = 1$$

Четыре функции по одной совершенной конъюнкции

$x_1 \wedge x_2$ - конъюнкция

$\neg x_1 \wedge \neg x_2$ - функция Пирса

$$x_1 \wedge \neg x_2 = x_1 \setminus x_2$$

$$\neg x_1 \wedge x_2 = x_2 \setminus x_1$$

Четыре функции по три совершенных конъюнкции

$$x_1 \vee x_2 = (x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) - \text{дизъюнкция}$$

$$x_1 | x_2 = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2) - \text{штрих Шеффера}$$

$$x_1 \supset x_2 = (x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$$

$$x_2 \supset x_1 = (x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge \neg x_2)$$

Шесть функций по две совершенных конъюнкции

$$x_1 \sim x_2 = (x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2) - \text{эквивалентность}$$

$$x_1 + x_2 = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) - \text{симметрическая разность}$$

$$(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$$

$$(\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$$

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2)$$

$$(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge \neg x_2)$$

Вопрос о тождественности двух переключательных функций можно решить, приведя их обоих к совершенной дизъюнктивной нормальной форме или преобразуя булевы выражения по законам булевой алгебры.

Задача 9. Рыцари, лжецы и нормальные люди

На острове жили три типа людей: рыцари - они всегда говорят правду; лжецы - они всегда лгут; нормальные люди - они могут сказать правду, а могут солгать.

Перед нами трое людей А, В и С. Один из них рыцарь, другой лжец, третий – нормальный человек (типы людей могут быть перечислены не в том

порядке, в каком "выписаны" их имена А, В, С). Наши знакомые высказывают следующие утверждения.

А: Я нормальный человек.

В: Это правда.

С: Я не нормальный человек.

Кто такие А, В и С?

3.3. Полные системы булевых функций

Система функций $\{f_1, f_2, \dots, f_n\}$ называется *полной*, если любая булева функция может быть выражена через функции f_1, f_2, \dots, f_n с помощью композиции (т. е. составления сложных функций).

Теорема 3.2. Следующие системы булевых функций полны:

$\{\neg, \wedge, \vee\};$

$\{\neg, \vee\};$

$\{\neg, \wedge\};$

$\{\neg, \supset\};$

$\{+, \wedge, 1\};$

$\{\downarrow\};$

$\{\}\}.$

Рассмотрим систему $\{+, \wedge, 1\}$. Будем вместо \wedge писать знак умножения \bullet , или вообще опускать, т. е. вместо $X \wedge Y$ писать XY .

Таблица 10

X	Y	$X+Y$	XY
1	1	0	1
1	0	1	0
0	1	1	0
0	0	0	0

С помощью табл. 10 можно доказать тождества:

- 1) $X+Y = Y+X$, $XY = YX$;
- 2) $(X+Y)+Z = X+(Y+Z)$, $(XY)Z = X(YZ)$;
- 3) $X+X = 0$, $XX = X$;
- 4) $X(Y+Z) = XY + XZ$;
- 5) $0+X = X$;
- 6) $0X = 0$;
- 7) $1X = X$.

Все правила, за исключением 3, выражают свойства, аналогичные обычным свойствам арифметики сложения и умножения.

Поскольку система $\{+, \wedge, 1\}$ полная, то любую переключательную функцию можно представить в виде многочлена (не выше чем первой степени с коэффициентами 0 и 1) от своих переменных. Такие многочлены называются *многочленами Жегалкина*.

В частности,

$$\neg X = X + 1,$$

$$X \vee Y = XY + X + Y,$$

$$X \vee Y \vee Z = XYZ + XY + XZ + YZ + X + Y + Z.$$

3.4. Переключательные элементы

Пусть имеется "черный ящик" - некоторое устройство, внутренняя структура которого нас не интересует, а известно лишь, что оно имеет n упорядоченных "входов" (например, занумерованных числами от 1 до n) и один "выход" (рис. 2).

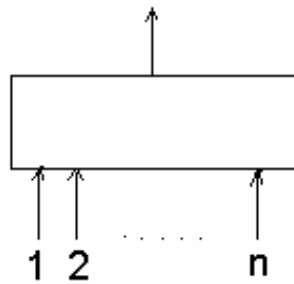


Рис. 2

На каждый из входов могут подаваться два сигнала (например, отсутствие электрического тока или наличие его), которые мы условимся обозначать символами 0 и 1, и при каждом наборе сигналов на входах однозначно определяется сигнал на выходе. Такое устройство назовем *переключательным элементом*. Ясно, что каждому переключательному элементу соответствует переключательная функция $f(x_1, x_2, \dots, x_n)$, которая строится следующим образом: входу с номером i ($1 \leq i \leq n$) ставится в соответствие переменная x_i и каждому (двоичному) набору значений этих переменных отвечает величина $f(x_1, x_2, \dots, x_n)$, равная 0 или 1 в зависимости от того, какой сигнал возникает на выходе при подаче на входы переключательного элемента.

Если у нас имеется несколько переключательных элементов, то из них можно получать новые сложные переключательные элементы следующим образом. Один из входов одного переключательного элемента можно соединить с выходом другого переключательного элемента (рис. 3).

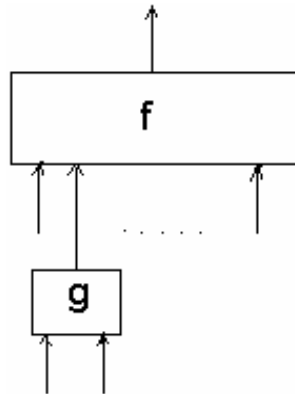


Рис. 3

Возникающее при этом устройство можно считать новым переключательным элементом, выходом которого является выход первого элемента (f), а входами все оставшиеся свободными входы первого элемента и входы второго элемента (g).

При таком соединении новому сложному переключательному элементу соответствует переключательная функция, полученная в результате суперпозиции исходных функций. Так, например, для элемента на рис. 3 имеем

$$h(x_1, y_1, y_2, \dots, x_n) = f(x_1, g(y_1, y_2), \dots, x_n).$$

Кроме этой операции можно отождествлять входы функционального элемента (рис. 4). При этом возникает новый переключательный элемент, у которого тот же выход и те же входы, за исключением отождествленных, которые теперь считаются одним входом. Для этого элемента соответствующая переключательная функция строится из первоначальной:

$$h(x_1, x_2, x_3) = f(x_1, x_2, x_2, x_3).$$

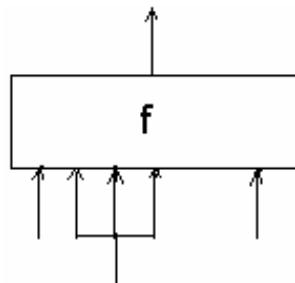
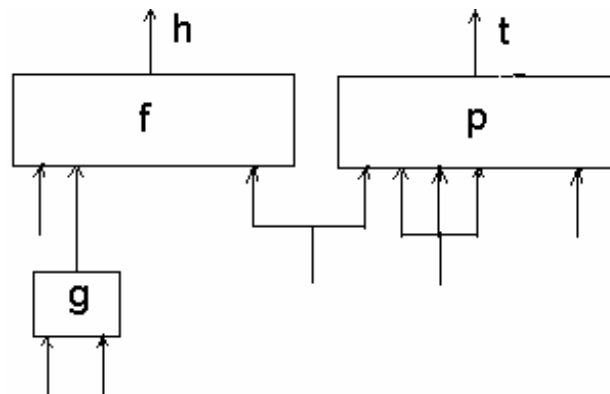


Рис. 4

Можно использовать несколько соединений указанных выше двух типов. В этом случае получается сложный переключательный элемент или мо-

жет получиться более сложное соединение, когда отождествляются некоторые входы различных переключательных элементов (рис. 5). В последнем случае такое соединение *называется переключательной (комбинационной*



схемой).

Рис. 5

Комбинационным схемам соответствует уже несколько переключательных функций (своя для каждого внешнего выхода), составленных с помощью суперпозиции. Для рис. 5 получаем две переключательные функции $\{h, t\}$:

$$h(x_1, x_2, x_3, x_4, x_5, x_6) = f(x_1, g(x_2, x_3), x_4),$$

$$t(x_1, x_2, x_3, x_4, x_5, x_6) = p(x_4, x_5, x_5, x_5, x_6).$$

Комбинационная схема изображается уже черным ящиком с несколькими выходами (рис. 6)

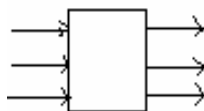


Рис. 6. Комбинационная схема

Символические изображения переключательных функций

Для трех переключательных функций: отрицания, конъюнкции и дизъюнкции - вместо прямоугольника используют три особых символических изображения (рис. 7). Соответствующие переключательные элементы называются *НЕ-элементом*, *И-элементом* и *ИЛИ-элементом*; о них говорят как о *логических элементах*.

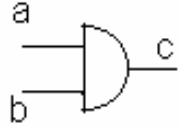
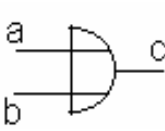
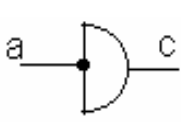
Символическое изображение			
Формула	$c = a \wedge b$	$c = a \vee b$	$c = \neg a$
Название	И-элемент	ИЛИ-элемент	НЕ-элемент

Рис.7. Символические изображения для конъюнкции, дизъюнкции и отрицания

Применение основных операций к переключательным функциям реализуется посредством соответствующего соединения символических изображений. Таким образом возникают комбинационные схемы (в том числе и с многими выходами), построенные лишь из конъюнкции, дизъюнкции и отрицания. Вместо отрицания на входе конъюнкции или дизъюнкции ставят просто жирную "точку отрицания"; это дает такие картинки, как, например, на рис. 8.

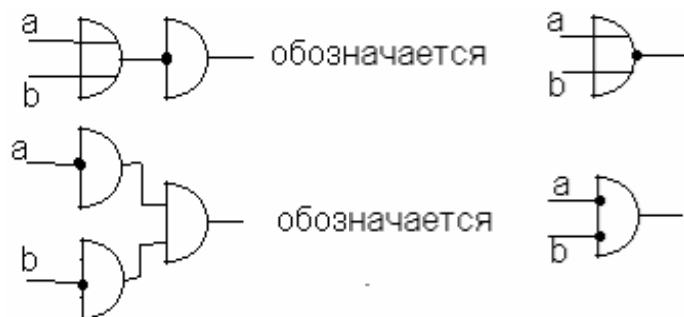


Рис.8. Символическое изображение функции

Пирса: $\neg(a \vee b) = \neg a \wedge \neg b$

Закон ассоциативности отражает возможность снабжать символические изображения логических элементов более чем двумя входами (рис. 9).

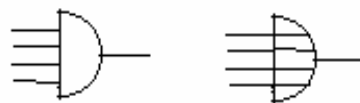


Рис. 9 И- и ИЛИ-элементы со многими входами

Пример: полусумматор

Для поразрядного сложения двух двоичных закодированных чисел применяется комбинационная схема, называемая полусумматором, с двумя перестановочными входами a , b и двумя выходами s и u

$$s = a + b, u = a \wedge b.$$

На рис. 10 представлены две реализации полусумматора, для правой реализации использовано преобразование

$$a + b = \neg((a \wedge b) \vee \neg(a \vee b)).$$

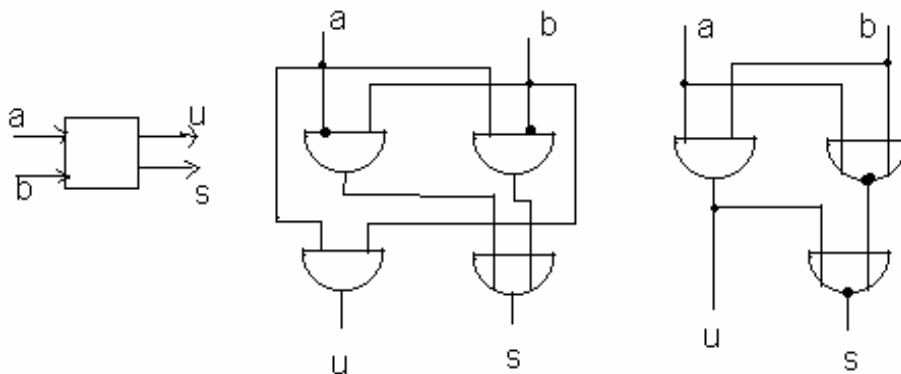


Рис. 10. Реализации полусумматора

Задача 10. Четверо подсудимых А, В, С и D

Установлено следующее:

1. Если А виновен, то В был соучастником.
2. Если В виновен, то либо С был соучастником, либо А не виновен.
3. Если D не виновен, то А виновен и С не виновен.
4. Если D виновен, то А виновен.

Кто из подсудимых виновен и кто не виновен?

4. ЛОГИКА ПРЕДИКАТОВ

4.1. Формулы логики предикатов

Логика высказываний позволяет формализовать только небольшую часть множества рассуждений. В качестве примера рассмотрим следующее рассуждение:

Все люди смертны. (P)

Сократ - человек. (Q)

Следовательно, Сократ смертен. (R)

Для того, чтобы это рассуждение было правильным с точки зрения логики высказываний, необходимо, чтобы формула $(P \& Q) \supset R$ была тавтологией. Но эта формула - не тавтология, хотя и рассуждение правильное. В логике высказываний высказывание неделимо, а в научных рассуждениях высказывания имеют внутреннюю структуру.

Перепишем предыдущее рассуждение, в таком виде, чтобы можно было лучше увидеть его структуру, в частности, обнаружить, что некоторые подразумеваемые словесные обороты присутствуют более одного раза.

Для всех x , если x является человеком, то x является смертным.

Сократ является человек.

Следовательно, Сократ является смертным.

Вот новые синтаксические компоненты, присутствие которых влияет на правильность рассуждения (в скобках - название и обозначение синтаксической категории в логике предикатов):

"для всех" (квантор общности \forall);

x (предметная переменная);

"Сократ" (предметная константа);

"является человеком" (предикат H);

"является смертным" (предикат M).

В логике предикатов данное рассуждение о Сократе запишется в форме $(\forall x (H(x) \supset M(x)) \& H(\text{Сократ})) \supset M(\text{Сократ})$, что позволяет установить, что данная формула истинна.

Рассмотрим предложения, зависящие от параметров:

" x - четное число";

" x меньше y ";

" $x + y = z$ ";

" x - отец Иванова Олега";

" x и y - братья";

" x - является смертным".

Все эти предложения становятся истинными или ложными при замене предметных переменных на соответствующие предметные константы.

Предикатом $P(x_1, x_2, \dots, x_n)$ называется функция

$$P : M^n \rightarrow \{И, Л\}.$$

Множество M определяется контекстом, элементы этого множества *предметные (индивидные) константы*.

Предикат от n аргументов называется n -местным или n -арным. Любое высказывание можно рассматривать как нульместный предикат (постоянная функция).

Некоторые примеры предикатов мы уже видели:

$H(x)$ - "х - является человеком";

$M(x)$ - "х - является смертным";

$Brothers(x, y)$ - "х и у - братья".

Над предикатами можно проводить обычные логические операции и, тем самым, создавать новые предикаты.

Пример 4.1.

1. $P(x) \equiv$ "х делится на 2",

$Q(x) \equiv$ "х делится на 3",

$P(x) \& Q(x) \equiv$ "х делится на 6".

2. $S(x, y) \equiv$ "х = у",

$\neg S(x, x) \supset S(x, y)$ - предикат истинен при любых х и у.

Операции квантификации или "связывания квантором переменную"

Квантор общности

Пусть $P(x)$ - предикат, тогда формула $\forall x P(x)$ обозначает высказывание, которое истинно тогда и только тогда, когда для всех $x \in M$ предикат $P(x)$ - истинен.

$\forall x P(x)$ читается как "для всех х $P(x)$ ".

Формула $\forall x P(x)$ от x не зависит - вместо x нельзя подставить никакую предметную константу. Символ \forall называется *квантором общности* или *универсальным квантором*.

Квантор существования

Пусть $P(x)$ - предикат, тогда формула $\exists x P(x)$ обозначает высказывание, которое истинно тогда и только тогда, когда найдется такой $x \in M$, что предикат $P(x)$ - истинен.

$\exists x P(x)$ читается как "существует такой х, что $P(x)$ ".

Формула $\exists x P(x)$ от x не зависит - вместо x нельзя подставить никакую предметную константу. Символ \exists называется *квантором существования или экзистенциальным квантором*.

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

Пример 4.2.

$\exists x (P(x) \& Q(x)) \equiv$ "существует x , который делится на 6" - истинное высказывание.

$\forall x (P(x) \& Q(x)) \equiv$ "все x делятся на 6" - ложное высказывание.

Алфавит языка логики предикатов содержит:

- 1) символы предметных переменных x, y, z, x_1, y_1, z_1 и т. д.;
- 2) символы предикатов P, Q, P_1, Q_1 и т. д.;
- 3) символы логических операций $\&, \vee, \neg, \supset, \sim$;
- 4) символы кванторов \forall, \exists .

Слово в алфавите логики предикатов называется *формулой*, если выполнены следующие условия (одновременно определяются понятия *свободной* и *связанной переменной* формулы).

1. $P(x_1, x_2, \dots, x_n)$ - формула, если P - n -местный предикат. Все переменные x_1, x_2, \dots, x_n - свободные переменные, связанных переменных в этой формуле нет.
2. Пусть A - формула, тогда $\neg A$ - формула с теми же свободными и связанными переменными, что и в формуле A .
3. Пусть A и B - формулы, причем нет таких переменных, которые были бы связаны в одной формуле и свободными - в другой. Тогда $(A \& B)$, $(A \vee B)$, $(A \supset B)$, $(A \sim B)$ суть формулы, в которых свободные переменные формул A и B остаются свободными, а связанные переменные формул A и B остаются связанными.
4. Пусть A - формула, содержащая свободную переменную x . Тогда $\forall x A$, $\exists x A$ тоже формулы. Переменная x в них связана. Остальные же переменные, которые в формуле A свободны, остаются свободными. Переменные, которые в формуле A были связаны, остаются связанными. В этих вновь полученных формулах формула A называется *областью действия квантора* $\forall x$ и $\exists x$ соответственно.
5. Слово в алфавите логики предикатов называется формулой только в том случае, если это следует из правил 1-5.

Пример 4.3.

1. Следующие выражения являются формулами логики предикатов:
 $P(x_1, x_2, x_7)$ - атомарная формула, в которой x_1, x_2, x_7 - свободные переменные;
 $(\forall x \exists y P(x, y, z)) \supset \forall x Q(x, w)$ - формула, в которой переменные x, y связаны, а переменные z, w свободны.

2. Выражение $(\forall x \exists y P(x, y, z)) \supset \forall x Q(x, y)$ не является формулой.

Значение формулы определено лишь тогда, когда задана какая-нибудь интерпретация входящих в нее символов.

Мы говорим, что задана *интерпретация формулы*, если зафиксировано множество M - множество значений всех предметных переменных в формуле и каждый предикатный символ однозначно определяет соответствующий предикат на множестве M .

Пусть задана конкретная интерпретация, тогда

- 1) если формула не содержит свободных переменных, то это высказывание - истинное или ложное;
- 2) если формула содержит свободные переменные, то это предикат на множестве M , который истинен при одних значениях переменных из этого множества и ложен при других.

Дадим индуктивное определение *значения формулы* (в данной интерпретации).

Значение формулы F на n -ке $\langle a_1, a_2, \dots, a_n \rangle$, $a_i \in M$, своих свободных переменных $\langle x_1, x_2, \dots, x_n \rangle$ будем обозначать $F|\langle a_1, a_2, \dots, a_n \rangle$.

Формула f есть атомарная переменная $A(x_1, x_2, \dots, x_n)$, где x_1, x_2, \dots, x_n - свободные переменные, тогда $F|\langle a_1, a_2, \dots, a_n \rangle$ есть значение n -местного предиката, сопоставленного предикатному символу A , при соответствующем замещении его переменных элементами a_1, a_2, \dots, a_n .

Формула F имеет вид $\neg A$. Пусть $A|\langle a_1, a_2, \dots, a_n \rangle = \varepsilon$, тогда $F|\langle a_1, a_2, \dots, a_n \rangle = \neg \varepsilon$.

Формула F имеет вид $A \vee B$, $A \& B$, $A \supset B$ или $A \sim B$. Пусть $A|\langle a_1, a_2, \dots, a_n \rangle = \alpha$, $B|\langle a_1, a_2, \dots, a_n \rangle = \beta$, тогда $F|\langle a_1, a_2, \dots, a_n \rangle$ равно соответственно $\alpha \vee \beta$, $\alpha \& \beta$, $\alpha \supset \beta$, $\alpha \sim \beta$.

Формула F имеет вид $\forall x A$. Если x_1, x_2, \dots, x_n - все свободные переменные формулы F , то x, x_1, x_2, \dots, x_n - все свободные переменные формулы A . Значение $\forall x A|\langle a_1, a_2, \dots, a_n \rangle = I$ тогда и только тогда, когда для любого $a \in M$ имеем $A|\langle a, a_1, a_2, \dots, a_n \rangle = I$.

Формула F имеет вид $\exists x A$. Если x_1, x_2, \dots, x_n - все свободные переменные формулы F , то x, x_1, x_2, \dots, x_n - все свободные переменные формулы A . Значение $\exists x A|\langle a_1, a_2, \dots, a_n \rangle = I$ тогда и только тогда, когда существует такое $a \in M$, что $A|\langle a, a_1, a_2, \dots, a_n \rangle = I$.

Пример 4.4. Рассмотрим три формулы:

- 1) $A(x, y)$;
- 2) $\forall y A(x, y)$;
- 3) $\exists x \forall y A(x, y)$.

Возьмем в качестве области интерпретации множество целых положительных чисел и интерпретируем $A(x, y)$ как $x \leq y$. Тогда первая формула - это

предикат $x \leq y$, который принимает значение И для всех пар a, b целых положительных чисел таких, что $a \leq b$. Вторая формула выражает свойство: "для каждого целого положительного числа y $x \leq y$ ", которое выполняется только при $x=1$. Наконец, третья формула - это истинное высказывание о существовании наименьшего целого положительного числа. Если бы в качестве области интерпретации мы рассматривали множество целых чисел, то третья формула была бы ложным высказыванием.

Пример 4.5. Пусть задана следующая интерпретация. M - множество натуральных чисел $(0, 1, 2, \dots)$, предикатные символы $S(x, y, z)$ и $P(x, y, z)$ обозначают следующие предикаты " $x + y = z$ " и " $x \times y = z$ " соответственно.

Запишем формулы, истинные на M тогда и только тогда, когда выполнены следующие условия:

- 1) $x = 0$;
- 2) $x = 1$;
- 3) x - четное число;
- 4) x - простое число;
- 5) $x = y$;
- 6) $x \leq y$;
- 7) x делит y ;
- 8) коммутативность сложения.

Ответы:

- 1) $F_1(x) = \forall y S(x, y, y)$, так как $x+y=y$ для любого y тогда и только тогда, когда $x = 0$;
- 2) $F_2(x) = \forall y P(x, y, y)$;
- 3) $F_3(x) = \exists y P(x, y, y)$;
- 4) $F_4(x) = \neg F_1(x) \& \neg F_2(x) \& (\forall y \forall z (P(y, z, x) \supset (F_2(y) \vee F_2(z))))$, где F_1, F_2 - формулы, определенные в пп. 1 и 2;
- 5) $F_5(x, y) = \forall z \forall u (S(x, z, u) \supset S(y, z, u))$;
- 6) $F_6(x, y) = \exists z S(x, z, y)$;
- 7) $F_7(x, y) = \exists z P(x, z, y)$;
- 8) $\forall x \forall y \forall z (S(x, y, z) \supset S(y, x, z))$.

Пример 4.6. Пусть $f(x)$ - произвольная фиксированная функция, заданная на отрезке $[a, b]$.

1. Рассмотрим интерпретацию: M - множество действительных чисел, $P(x, \delta)$ обозначает $|x - x_0| < \delta$, $Q(x, \varepsilon)$ обозначает $|f(x) - A| < \varepsilon$, $R(\varepsilon)$ обозначает $\varepsilon > 0$. Здесь x_0 - фиксированный элемент отрезка $[a, b]$; A - некоторое фиксированное действительное число. Тогда утверждение о том, что A - предел функции $f(x)$ при $x \rightarrow x_0$, записывается формулой $\forall \varepsilon \exists \delta \forall x ((R(\varepsilon) \& P(x, \delta)) \supset Q(x, \varepsilon))$.

2. Рассмотрим интерпретацию: M - множество действительных чисел, $P(x, \delta)$ обозначает $|x - x_0| < \delta$, $S(x, \varepsilon)$ обозначает $|f(x) - f(x_0)| < \varepsilon$, $R(\varepsilon)$ обозначает $\varepsilon > 0$. Здесь x_0 - фиксированный элемент отрезка $[a, b]$. Тогда утверждение о том, что функция f - непрерывна в точке x_0 записывается в виде формулы $\forall \varepsilon \exists \delta \forall x ((R(\varepsilon) \& P(x, \delta)) \supset S(x, \varepsilon))$.
3. Рассмотрим интерпретацию: M - множество действительных чисел, $P(x, x_1, \delta)$ обозначает $|x - x_1| < \delta$, $S(x, x_1, \varepsilon)$ обозначает $|f(x) - f(x_1)| < \varepsilon$, $R(\varepsilon)$ обозначает $\varepsilon > 0$, $D(x)$ обозначает $x \in [a, b]$. Тогда утверждение о том, что функция f - непрерывна на отрезке $[a, b]$ записывается в виде формулы $\forall x_1 \forall \varepsilon \exists \delta \forall x ((D(x_1) \& R(\varepsilon) \& P(x, x_1, \delta)) \supset S(x, x_1, \varepsilon))$.

Задача 11. В Бронкс или Бруклин?

Один молодой человек живет в Манхэттене возле станции метро. У него есть две знакомые девушки. Одна из них живет в Бруклине, вторая – в Бронксе. Когда он едет к девушке из Бруклина, то садится в поезд, подходящий к платформе со стороны центра города. Когда же едет к девушке из Бронкса, то садится в поезд, идущий в центр. Поскольку обе девушки нравятся ему одинаково, он просто садится в тот поезд, который приходит первым. Таким образом, в выборе, куда ехать, он полагается на случай. Молодой человек приходит на станцию каждую субботу в разное время. И в Бруклин и в Бронкс поезда ходят с одинаковым интервалом в 10 минут. Тем не менее, по каким-то непонятным причинам большую часть времени он проводит с девушкой из Бруклина; в среднем из каждых десяти поездок девять приходятся на Бруклин. Попробуйте догадаться, почему у Бруклина такой огромный перевес?

4.2. Равносильность формул в логике предикатов

Пусть F и G - формулы, имеющие одно и то же множество свободных переменных (может быть пустое).

Формулы F и G *равносильны в данной интерпретации*, если на любом наборе значений свободных переменных они принимают одно и то же значение.

Формулы F и G *равносильны на множестве M* , если они равносильны во всех интерпретациях, заданных на множестве M .

Формулы F и G *равносильны* (в логике предикатов), если они равносильны на всех множествах (и пишут $F \equiv G$).

Пример 4.7.

1. Пусть $M = \{a, b\}$ и предикат $P(x, y)$ задан таблицей

x	y	P(x,y)
a	a	И
a	b	Л
b	a	Л
b	b	И

тогда формулы $F(x, y, z) = P(x, y) \& P(x, z)$ и $G(x, y, z) = P(x, y) \& P(y, z)$ равносильны в данной интерпретации.

Пусть $P(x, y)$ задан таблицей

x	y	P(x,y)
a	a	И
a	b	И
b	a	Л
b	b	Л

тогда формулы F и G не равносильны в данной интерпретации, так как $F(a,b,b) = И$, $G(a,b,b) = Л$.

2. Пусть $M = \{a\}$ - одноэлементное множество. Тогда формулы $\exists x A(x)$ и $\forall x A(x)$ равносильны на множестве M .

Если $M = \{a,b\}$ и

x	A(x)
a	И
b	Л

Тогда формулы $\exists x A(x)$ и $\forall x A(x)$ не равносильны на множестве M .

Правила перехода от одних формул к другим, им равносильным (в логике предикатов).

Остаются в силе правила равносильных преобразований из логики высказываний.

Перенос квантора через отрицание

Пусть A содержит свободную переменную x . Тогда справедливо

$$\neg \forall x A(x) \equiv \exists x \neg A(x)$$

$$\neg \exists x A(x) \equiv \forall x \neg A(x)$$

Вынос квантора за скобки

Пусть A содержит свободную переменную x . Пусть B не содержит свободную переменную x . Тогда справедливы равносильности

$$\exists x (A(x) \& B(x)) \equiv \exists x A(x) \& B(x)$$

$$\forall x (A(x) \& B(x)) \equiv \forall x A(x) \& B(x)$$

Перестановка одноименных кванторов

$$\forall y \forall x A(x, y) \equiv \forall x \forall y A(x, y)$$

$$\exists y \exists x A(x, y) \equiv \exists x \exists y A(x, y)$$

Переименование связанных переменных

Заменяя связную переменную x формулы A другой переменной y , не входящей в эту формулу, в кванторе и всюду в области действия этого квантора получаем формулу, равносильную A .

4.3. Выполнимость и общезначимость в логике предикатов

Формула A *выполнима* в данной интерпретации, если существует такой набор $\langle a_1, a_2, \dots, a_n \rangle$, $a_i \in M$, значений свободных переменных x_1, x_2, \dots, x_n формулы A , что $A|\langle a_1, a_2, \dots, a_n \rangle = И$.

Формула A *истинна* в данной интерпретации, если она принимает значение И на любом наборе значений своих свободных переменных.

Формула A *общезначима* или *тождественно истинна* (в логике предикатов), если она истинна в любой интерпретации.

Формула A *выполнима* (в логике предикатов), если существует интерпретация, в которой она выполнима.

Формула A общезначима тогда и только тогда, когда формула $\neg A$ не является выполнимой, а формула A выполнима тогда и только тогда, когда формула $\neg A$ не является общезначимой.

Очевидно, что если F и G - равносильные формулы (в логике предикатов), то формула $F \sim G$ общезначима.

Теорема 4.1. Формула

$\forall x A(x) \supset A(y)$, где y не входит в формулу $A(x)$, общезначима.

Теорема 4.2. Формула

$A(y) \supset \exists x A(x)$, где y не входит в формулу $A(x)$, общезначима.

Задача распознавания общезначимости формул логики предикатов существенно сложнее, чем формул логики высказываний. Так же, как и в логике высказываний, она называется *проблемой разрешимости* и ставится следующим образом: указать алгоритм распознавания общезначимости формул (т. е. является ли данная формула общезначимой или нет).

Теорема 4.3 (теорема Черча о неразрешимости логики предикатов, 1936). Не существует алгоритма, который для любой формулы логики предикатов устанавливает, общезначима она или нет.

Задача 12. Метаголоволомка – Дело Джона

Как-то раз шло судебное расследование по делу двух братьев-близнецов. Было известно, что, по крайней мере, один из них никогда не говорил правду, хотя и неясно, кто же именно. Одного из братьев звали Джон, именно он и совершил преступление. (При этом вовсе не обязательно, чтобы

Джон был тем из близнецов, который всегда лгал.) Цель расследования заключалась в том, чтобы выяснить, кого же из братьев зовут Джон.

--- Вы - Джон? – спросил судья одного из близнецов.

--- Да, я Джон, - последовал ответ.

--- А вы – Джон? – спросил судья второго брата.

Второй близнец ответил ему вполне определенно (либо "да", либо "нет"), и тут судья сразу догадался, кто из них Джон.

Был Джон первым или вторым из близнецов?

5. ИСЧИСЛЕНИЯ

Как было сказано выше, в логике предикатов, в отличие от логики высказываний, нет эффективного способа для распознавания общезначимости формул. Выходом из этой неприятной ситуации является следующий подход: выделяем небольшое множество общезначимых формул и указываем правила, с помощью которых из известных общезначимых формул создаются новые общезначимые формулы. Если окажется, что таким образом мы можем получить любую общезначимую формулу, то это нас вполне устроит.

Указанный путь реализуется в рамках так называемых формальных аксиоматических теорий.

5.1. Аксиоматические теории

Формальная аксиоматическая теория T считается определенной, если:

- 1) задано некоторое счетное множество символов - символов теории T ; конечные последовательности символов теории T называются *выражениями* теории T ;
- 2) имеется подмножество выражений теории T , называемых *формулами* теории T ;
- 3) выделено некоторое множество формул, называемых *аксиомами* теории T ;
- 4) имеется конечное множество R_1, R_2, \dots, R_m отношений между формулами, называемых *правилами вывода*.

Если формула A и формулы A_1, A_2, \dots, A_j находятся в некотором отношении R_i , то A называют *непосредственным следствием* из формул A_1, A_2, \dots, A_j , полученных по правилу R_i .

Выводом в теории T называется всякая последовательность A_1, A_2, \dots, A_n формул такая, что для любого i формула A_i есть либо аксиома теории T , либо непосредственное следствие каких-либо предыдущих формул.

Формула A называется *теоремой* теории T , если в ней существует вывод, в котором последней формулой является A . Этот вывод называется *выводом* (доказательством) формулы A . Иными словами, теоремы аксиоматической теории - это формулы, которые могут выведены (доказаны) по определенным правилам.

5.2. Исчисление высказываний

Оказывается множество тавтологий логики высказываний можно описать в рамках простой формальной аксиоматической теории - исчисления высказываний.

Определим исчисление высказываний следующим образом:

1. Символы исчисления высказываний: \neg , \supset , $($, $)$ и буквы X_i с целыми положительными числами в качестве индексов: X_1, X_2, \dots . Символы \neg и \supset - логические символы, символы X_1, X_2, \dots - переменные.
2. Формулы исчисления высказываний: а) все переменные X_i - формулы; б) если A и B - формулы, то $(\neg A)$ и $(A \supset B)$ тоже формулы.

Пример 5.1. Последовательность символов $\neg X_1 \supset X_2 \supset X_1$ - выражение, но не формула.

Пример 5.2. Пусть A, B, C - формулы. Тогда
 $(C \supset (A \supset B)), (((\neg A) \supset B) \supset (\neg C))$

тоже формулы.

Для сокращения записи опустим в формуле внешние скобки и те пары скобок, без которых можно восстановить формулы по следующему правилу: каждое вхождение знака \neg относится к наикратчайшей подформуле, следующей за этим знаком. Тогда две предыдущие формулы примут вид

$$C \supset (A \supset B), (\neg A \supset B) \supset \neg C.$$

3. Аксиомы исчисления высказываний. Каковы бы ни были формулы A, B и C , следующие формулы являются аксиомами:

- A1. $A \supset (B \supset A)$;
- A2. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;
- A3. $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.

Выражения A1-A3 называются схемами аксиом, поскольку каждое из них порождает бесконечное множество формул, являющихся аксиомами исчисления высказываний. Например, формула $X_1 \supset (X_2 \supset X_1)$ есть аксиома, полученная по схеме A1, формула $(\neg A \supset \neg A) \supset ((\neg A \supset A) \supset A)$ (где A - любая формула) - аксиома полученная по схеме A3.

4. Единственным правилом вывода формулы служит правило *modus ponens* (правило отделения, утверждающий модус). Пусть имеется три формулы: $A, A \supset B$ и B . Про формулу B будем говорить, что она получается по правилу *modus ponens* из формул A и $A \supset B$. Это правило вывода записывается в виде $\frac{A, A \supset B}{B}$.

Хотя для исчисления высказываний мы выбрали только два логических символа \neg и \supset , с помощью подходящих определений можно ввести и остальные операции \vee , $\&$, \sim , например, $A \sim B$ означает $\neg((B \supset A) \supset \neg(A \supset B))$.

Пример 5.3. Для любой формулы A построим вывод формулы $A \supset A$, т. е. $A \supset A$ - теорема.

Подставляем в схему аксиом A2 вместо B формулу $A \supset A$ и вместо C формулу A , получаем аксиому

$$(A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A)).$$

Подставляем в A1 вместо формулы B формулу $A \supset A$, получаем аксиому

$$A \supset ((A \supset A) \supset A).$$

Из формул (1) и (2) по правилу *modus ponens* получаем

$$(A \supset (A \supset A)) \supset (A \supset A).$$

Подставляем в A1 вместо формулы B формулу A, получаем аксиому

$$A \supset (A \supset A).$$

Из формул (3) и (4) по правилу *modus ponens* получаем $A \supset A$.

Теорема 5.1

1. Любая аксиома в исчислении высказываний является тавтологией.
2. Любая теорема в исчислении высказываний является тавтологией.

Теорема 5.2. (Пост, 1921) Формула A в исчислении высказываний является теоремой тогда и только тогда, когда A - тавтология.

Исчисление высказываний можно описать системами аксиом, отличными от A1, A2 и A3. Например, если использовать штрих Шеффера $x|y = \neg(x \& y)$, то достаточно одной схемы аксиом

$$((P|(Q|R))|(S|(S|S))|(T|Q)|((P|T)|(P|T)))$$

и единственного правила вывода "из A и A|(B|C) следует C".

Задача 13. Три дамы с испачканными лицами

Три дамы A, B и C сидят в купе пассажирского вагона с испачканными лицами и все три смеются. Внезапно A понимает, что смеются над ней. Как она рассуждает?

5.3. Исчисление предикатов

Исчисление предикатов - это аксиоматическая теория, символами которой являются, по существу, те же символы, что и в логике предикатов:

- 1) символы предметных переменных: x_1, x_2, \dots ;
- 2) символы предикатов P, Q, R, A, ...;
- 3) логические символы \neg, \supset ;
- 4) символы кванторов; \forall, \exists ;
- 5) скобки и запятая.

Сформулированное в разделе 4.1 определение формулы остается в силе и для исчисления предикатов (с той лишь разницей, что мы употребляем только два логических символа: \neg и \supset ; остальные связки можно определить через эти).

Аксиомы исчисления предикатов. Каковы бы ни были формулы A и B, следующие формулы являются аксиомами (при этом не должно нарушаться определение формулы):

- A1. $A \supset (B \supset A)$;
 A2. $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$;
 A3. $(\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.
 A4. $\forall x A(x) \supset A(y)$, где формула $A(x)$ не содержит переменной y .
 A5. $A(x) \supset \exists y A(y)$, где формула $A(x)$ не содержит переменной y .

Правила вывода исчисления предикатов:

1. Правило *modus ponens*;
2. Правило связывания квантором общности: $\frac{B \supset A(x)}{B \supset \forall x A(x)}$, где формула B не содержит переменной x .
3. Правило связывания квантором существования: $\frac{A(x) \supset B}{\exists x A(x) \supset B}$, где формула B не содержит переменной x .
4. Правило переименования связанной переменной. Связанную переменную формулы A можно заменить (в кванторе и во всех вхождениях в области действия квантора) другой переменной, не являющейся свободной в A .

Теорема 5.3

- 1) Аксиомы исчисления предикатов - общезначимые формулы.
- 2) Формула, получающаяся из общезначимых формулы по любому из правил вывода 1-4, является общезначимой.
- 3) Любая доказуемая в исчислении предикатов формула общезначима.

Теорема 5.4 (теорема Геделя о полноте исчисления предикатов, 1930).
 Всякая общезначимая формула выводима в исчислении предикатов.

5.4. Неполнота математики

Таким образом, показано, что класс всех теорем исчисления предикатов совпадает с классом общезначимых формул. На этом примере мы видим силу формального аксиоматического метода. Но насколько этот метод действительно силен? Из школьной программы вы знаете, что аксиоматическую теорию еще использовал Евклид при изложении геометрии. Может быть возможно аксиоматизировать всю математику?

В 30-годы анонимная группа французских математиков под псевдонимом Никола Бурбаки начала писать трактат "Начала математики" (он не окончен и по сей день). Используя аксиомы теории множеств и исчисления предикатов (в несколько большем варианте, чем в предыдущем изложении), Н. Бурбаки излагает всю современную математику с единой (формально-аксиоматической) точки зрения. Они начали не на пустом месте.

В 1889 г. Пеано предложил свои аксиомы для аксиоматизации понятия натурального числа и, следовательно, арифметики:

- 1) 1 есть натуральное число;
- 2) следующее за натуральным числом есть натуральное число;
- 3) 1 не следует ни за каким натуральным числом;
- 4) если натуральное число a следует за натуральным числом b и за натуральным числом c , то натуральные числа b и c тождественны;
- 5) если какое-либо предложение доказано для 1 и если из допущения, что оно верно для натурального числа n , вытекает, что оно верно для следующего за n натурального числа, то это предложение верно для всех натуральных чисел (принцип математической индукции).

Естественно было надеяться, что метод формальной аксиоматической теории позволит строить все содержание математики на такой точной и, казалось бы, надежной основе, как понятие выводимой формулы (теоремы формальной системы). Однако в 1931 году Курт Гедель доказал свою знаменитую теорему о неполноте.

Теорема 5.5 (теорема Геделя о неполноте). Всякая естественная непротиворечивая аксиоматическая теория T (формализация) арифметики или любой другой математической теории, содержащей арифметику (например, теория множеств), неполна и непополнима в том смысле, что а) в T имеются содержательно истинные неразрешимые формулы, т. е. такие формулы A , что ни A , ни отрицание A не выводимы (не доказуемы) в T ; б) каким бы конечным множеством дополнительных аксиом не расширить систему T , в новой, усиленной таким образом формальной системе неизбежно появятся свои неразрешимые формулы.

При доказательстве своей теоремы Гедель, образно говоря, построил математическую формулу, которая гласит следующее: "Я не доказуема". Если эта формула ложна, то тогда получаем, что она доказуема. Но поскольку любое доказательство в математике приводит только к истинным утверждениям, то мы приходим к противоречию. Обратное предположение, т. е. истинность этой формулы, сразу приводит к неполноте математики.

Со времен доказательства Геделем своей теоремы математики искали пример такой истинной теоремы, которую было бы невозможно доказать используя аксиоматику Пеано. Только в 1977 году удалось обнаружить такую теорему в комбинаторике, так называемую, бесконечную теорему Рамсея.

То, что истинное предложение бывает недоказуемым, можно проиллюстрировать таким примером. Рассмотрим предложение: для всякого натурального n имеет место формула $1+2+\dots+n = n(n+1)/2$. Обычно это доказывают, применяя аксиому математической индукции. Если бы в нашем распоряжении не было аксиомы индукции, то эту формулу нельзя было бы доказать, ибо среди всех аксиом арифметики и логики одна лишь аксиома индукции позволяет делать утверждения о всей бесконечной совокупности натуральных чисел.

Можно было бы попытаться сбросить ярмо индукции и рассуждать так: если бы для некоторого n сумма $1+2+\dots+n$ не равнялась числу $n(n+1)/2$, то существовало бы наименьшее такое n ; оно не могло бы равняться 1, поскольку наше утверждение для $n=1$ верно; но оно не могло бы и быть больше 1, ибо тогда можно было бы показать, что $n-1$ тоже исключительное число, а это противоречит тому, что n - наименьшее из таких чисел. Увы, это рассуждение основано на принципе, утверждающем, что каждое непустое множество натуральных чисел имеет наименьший элемент, а этот принцип равносильен аксиоме индукции.

Итак без аксиомы индукции простые арифметические утверждения вроде $1+2+\dots+n = n(n+1)/2$ даже несмотря на то, что они истинны, нельзя было бы вывести из остальных аксиом; можно сказать, что без аксиомы индукции арифметика была бы неполной.

Задача 14. Рубины и изумруды

У одного восточного владыки было 10 мудрецов-советников. Однажды к нему в гости приехал величайший мудрец Востока Абу Али Ибн-Сина, которого в Европе прозвали Авиценной.

И вот призывает падишах своих советников, ставит перед каждым шкатулку и говорит: "У меня в руках мешочек с рубинами и изумрудами. Сейчас я положу каждому в шкатулку рубин или изумруд. Тот, в чью шкатулку я кладу камень, отворачивается и не видит, какой камень ему положен. Но зато он видит, какие камни я кладу всем остальным. Я положу хотя бы один рубин и один изумруд. Вы должны догадаться, какой камень лежит у вас в шкатулке. Все!"

Разложил падишах камни и, выждав некоторое время, обратился к 10 мудрецам, стоявшим перед ним со шкатулками в руках: "Выйдите вперед те, кому в шкатулку я положил изумруд!" – Никто не шелохнулся. – "О, Аллах! – шепнул падишах Ибн-Сине, они не сообразили!" – подожди, повелитель, еще рано", - улыбнулся мудрейший. – "У кого в шкатулке изумруд, выходи!" – второй раз воскликнул падишах. Но опять никто не вышел. – "Терпение", - успокоил повелителя Ибн-Сина. – "У кого в шкатулке изумруд, выходи!" – в третий раз обратился падишах к мудрецам. И опять они остались неподвижны.

"Горе мне!" – гневно закричал падишах. - Мои советники – бородатые ослы! Теперь мне ясно, почему дела в государстве идут так плохо" – "Попробуй еще раз, - предложил Ибн-Сина, - может быть твои советники мудрее, чем ты думаешь" – "Хорошо, - согласился падишах. –В четвертый раз обращаюсь к вам: у кого в шкатулке изумруд – выходи!" – И вот здесь то 4 мудреца вышли вперед, открыли свои шкатулки и В каждой из них густым зеленым светом сиял изумруд! В шкатулках остальных мудрецов оказались рубины.

Как мудрецы догадались, какой камень лежит в их шкатулке? Почему они вышли только после 4-го приглашения?

6. ПОЗИЦИОННЫЕ СИСТЕМЫ СЧИСЛЕНИЯ

6.1. Определение и перевод целых чисел из одной системы счисления в другую

Позиционное представление с основанием (или по основанию) b чисел определяется правилом

$$(a_n \dots a_2 a_1 a_0 . a_{-1} a_{-2} \dots a_{-m})_b = \sum_{i=-m}^n a_i \times b^i .$$

Таким образом, $530.3_6 = 5 \times 6^2 + 3 \times 6 + 0 + 3 \times 6^{-1} = 198.5$.

Используемая нами система счисления является *десятичной*, $b=10$ и $\{a_i\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Стандартные позиционные системы счисления - это когда $b > 1$ - целое число и цифры a_i представляют все множество целых значений $0 \leq a_i < b$. При $b=2$ система счисления называется двоичной, при $b=3$ - троичной и т. д. Точка между a_0 и a_1 называется *позиционной (разделительной) точкой*. Цифра a_n называется *наиболее значимой*, цифра a_{-m} - *наименее значимой*.

Если основание системы счисления b имеет много делителей, то в этой системе удачно представляются дроби, так, например, в системе счисления с основанием $b=60$ в конечном виде представимы дроби со знаменателями 2, 3, 4, 5, 6, 10, 12, 15, 20, 30.

История

В Месопотамии (Вавилонии) использовалась шестидесятеричная система счисления, $b=60$, но не имелось обозначение для цифры 0. Остатки шестидесятеричной системы используются при измерении углов (градусы, минуты, секунды) и времени (часы, минуты, секунды).

В Древнем Риме использовали римские цифры - это не позиционная система счисления.

Индейцы майя использовали систему счисления по основанию 20.

Двоичная система счисления применяется в Англии при измерении жидкостей; единицы измерения:

один полуштоф = два джилла;

одна пинта = два полуштофа;

одна кварта = две пинты;

один потл = две кварталы;

один галлон = два потла;

один пек = два галлона;

один полубушель = два пека;

один бушель или фиркин (маленький бочонок) = два полбушеля;

один килдеркин = два бушеля;

один баррель = два килдеркина;

один хогзхед = два барреля;

один пайп = два хогзхеда;

один тан (большая бочка) = два пайпа.

Шведский король Карл 12 хотел ввести в Швеции 8-ричную систему.

При основании системы счисления $b > 10$ в качестве недостающих цифр используют начальные буквы латинского алфавита. Так цифрами в 16-ричной системе счисления являются следующие символы: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Поэтому $AFFE_{16} = 45054$.

Чтобы перевести из b -ичной системы счисления в десятичную достаточно использовать определение.

Для перевода из десятичной системы счисления в b -ичную можно воспользоваться следующим алгоритмом.

Дано число x и основание системы b . На каждом шаге следующего цикла переменная a будет получать очередную самую левую цифру числа x в b -ичной системе.

```
while  $x \neq 0$  do
  begin
     $a := x \bmod b$ ;
     $x := x \div b$ 
  end;
```

Легко осуществить перевод из системы счисления с основанием b в систему с основанием b^n и обратно. Если исходное число X задано в системе счисления по основанию b , то для перевода в b^n -ичную систему счисления надо цифры числа X разбить на группы слева направо по n цифр. Каждая такая группа цифр затем переводится в число по основанию b^n , для изображения таких чисел потребуется только по одной цифре в b^n -ичной системе счисления. Так, например, имеем

$$10\ 10\ 11\ 10\ 00\ 01_2 = 1 \times 4^0 + 0 \times 4^1 + 2 \times 4^2 + 3 \times 4^3 + 2 \times 4^4 + 2 \times 4^5 = 223201_4,$$

$$101\ 011\ 100\ 001_2 = 1 \times 8^0 + 4 \times 8^1 + 3 \times 8^2 + 5 \times 8^3 = 5341_8,$$

$$1010\ 1110\ 0001_2 = 1 \times 16^0 + E \times 16^1 + A \times 16^2 = AE1_{16}.$$

Вычислительные машины могут обрабатывать лишь числа, лежащие в диапазонах, определенных допустимым количеством разрядов t :

$$0 \leq x \leq \sum_{i=0}^{t-1} (b-1) \times b^i = b^t - 1.$$

6.2. Представление отрицательных чисел

Для того чтобы имелась возможность обрабатывать и отрицательные числа, диапазон обрабатываемых положительных чисел ограничивают. Освобождающие при этом кодовые слова интерпретируют как отрицательные числа. Здесь применяют три метода.

Прямой код. Знак и само число кодируются по отдельности. Этот сейчас редко используемый метод представляет интерес прежде всего для представления чисел в системе счисления с основанием 2. Диапазон представимых чисел будет $|x| \leq b^{t-1} - 1$. Первый разряд интерпретируется как знак числа, причем $a_t \neq 0$ означает отрицательный знак. Число 0 кодируется неоднозначно: +0 и -0.

Дополнительный код. В этом случае отрицательное число $-x$ кодируется числом $b^t - x$, т. е. числом

$$b^t - x = 1 + \sum_{i=0}^{t-1} (b-1) \times b^i - \sum_{i=0}^{t-1} a_i \times b^i = 1 + \sum_{i=0}^{t-1} (b-1-a_i) \times b^i.$$

Пусть, например, $t=10$, т. е. используется 10 разрядов, тогда десятичное отрицательное число -1234567890 представляется как $8765432109 + 1 = 8765432110$. Диапазон представимых чисел несимметричен относительно нуля: $-b^{t-1} \leq x \leq b^{t-1} - 1$.

Пусть $b=2$ и $t=16$, тогда $-32768 \leq x \leq 2^{15} - 1 = 32767$. Поэтому двоичные числа от 0 до $2^{15} - 1$ включительно представляют положительные числа, а диапазон от 2^{15} до 2^{16} включительно служит для представления отрицательных чисел (тип integer в Паскале).

Обратный код. Сумма $\bar{x} = \sum_{i=0}^{t-1} (b-1-a_i) \times b^i$ называется обратным кодом

(для x), она также может служить для кодирования $-x$. При этом

$$x + \bar{x} = \sum_{i=0}^{t-1} (b-1) \times b^i = b^t - 1.$$

Диапазон представимых чисел $|x| \leq b^{t-1} - 1$. Так, например, отрицательное десятичное число -1234567890 (при $t=10$) кодируется как 8765432109. Записи 0000000000 (положительный ноль) и 9999999999 (отрицательный ноль) представляют 0.

6.3. Нестандартные позиционные системы счисления

Нега-десятичная

В качестве основания системы берется $b = -10$. Цифры стандартные десятичные: $0 \leq a_i \leq 9$.

$$(\dots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \dots)_{-10} = \dots -1000a_3 + 100a_2 - 10a_1 + a_0 - a_{-1}/10 + a_{-2}/100 \dots$$

$$1234567890 = 19375573910_{-10}$$

$$-1234567890 = 2846648290_{-10}$$

Любое вещественное число (положительное или отрицательное) может быть представлено в нега-десятичной системе *без знака*.

Мнимо-четвертичная

$b = 2i$ (i - мнимая единица). Цифры - $\{0, 1, 2, 3\}$. Каждое комплексное число может быть представлено в этой системе при помощи цифр 0, 1, 2 и 3, причем тех же цифр, взятых со знаком минус, не требуется.

Например, $7\frac{3}{4} - 7\frac{1}{2}i = 11210.31_{2i}$.

Бинарная комплексная система

Основание $b=i-1$, цифры 0 и 1. Каждое комплексное число допускает такое представление.

Уравновешенная троичная система

Основание системы $b=3$, цифры: 0, 1, $\bar{1} = -1$. Эта система обладает приятными свойствами:

- переход от числа к противоположному по знаку - взаимная замена 1 на -1;
- знак числа задается его наиболее значимым ненулевым тритом;
- операция округления до ближайшего целого сводится к отбрасыванию дробной части.

Примеры: $8 = 10\bar{1}$, $-33 = \bar{1}\bar{1}10$, $1/2 = 0.1111\dots$

Позиционные системы со смешанным основанием

Факториальная система. Любое неотрицательное целое число можно единственным образом представить в виде

$$c_n \times n! + c_{n-1} \times (n-1)! + \dots + c_2 \times 2! + c_1, \quad 0 \leq c_k \leq k.$$

Примеры используемых смешанных систем:

3 недели 2 дня 9 часов 22 минуты 57 секунд 492 миллисекунды;

10 фунтов 6 шиллингов $3\frac{1}{2}$ пенса (12 пенсов = 1 шиллинг, 20 шиллингов = 1 фунт).

7. РЕШЕНИЯ ЛОГИЧЕСКИХ ЗАДАЧ

Задача 1. Кто из караванщиков убийца?

Вот как автор задачи, Рэймонд М. Смаллиан, отвечает на этот вопрос. "Не думаю, чтобы рассуждения сторонников любого из двух мнений относительно того, кто убийца, можно было считать ☐правильными☐ или ☐неправильными☐. В проблемах подобного типа, как мне кажется, одно мнение ничем не хуже и не лучше другого. Лично я считаю, что если какого-нибудь и обвинять в смерти караванщика С, то его недруга А. Если бы я был защитником караванщика В, то обратил бы внимание суда на два обстоятельства: 1) лишить человека отравленной воды не означает убить его; 2) в любом случае действия караванщика В способствовали продлению жизни караванщика С (хотя это и не входило в намерения караванщика В), поскольку смерть от отравления наступила бы быстрее, чем смерть от жажды. Защитник караванщика А мог бы возразить мне: ☐Как можно, находясь в здравом уме, обвинять моего подзащитного в отравлении, если С в действительности не выпил ни капли яда?☐ Как видите, мы столкнулись с поистине головоломной проблемой. Дело усложняется тем, что проблему можно рассматривать с точки зрения морали, права и подходить к ней с чисто научных позиций, используя такое понятие, как *причинность*. С точки зрения морали и А и В виновны в том, что замыслили убийство, но наказание за совершенное убийство по строгости не сравнимо с наказанием за преступный замысел. Правовая оценка этого дела мне не известна. Думаю, что приговоры, вынесенные различными составами присяжных не были бы одинаковыми. Что же касается научного подхода к решению нашей головоломки, то само понятие причинности затрагивает множество проблем. Мне кажется, что об этой головоломке можно было бы написать целую книгу."

Задача 2. Все лошади одной масти

Доказательство безупречно за исключением случая $n=2$. Если все пары лошадей состоят из лошадей одинаковой масти, данное утверждение справедливо для любого числа лошадей.

Задача 3. Четыре колпака в пещере

На первых двух мудрецах могут быть надеты такие сочетания колпаков: 1) белый-белый; 2) черный-черный; 3) белый-черный; 4) черный-белый.

Если третий мудрец видит перед собой два белых колпака, то он догадывается, что на нем самом черный колпак; если он видит перед собой два черных колпака, то опять-таки он догадывается, что на нем самом белый колпак. Таким образом, в случаях 1) и 2) догадывается и воскликнет третий мудрец. Если же он идет и молчит, то второй мудрец понимает, что имеет место 3) и 4) варианты. Посмотрев на колпак первого мудреца, второй мудрец опре-

деляет какой колпак на нем самом: цвет его колпака противоположен по цвету колпака на первом мудреце.

Таким образом, один из мудрецов обязательно догадается, какого цвета на нем колпак.

Задача 4. Остров рыцарей и лжецов

Прежде всего заметим, что В и С не могут быть оба рыцарями или оба лжецами, так как В противоречит С. Следовательно, В и С не могут оба рыцарями или оба лжецами: один из них рыцарь, а другой - лжец. Если бы А был рыцарем, то всего было бы два рыцаря. Следовательно, А не лгал и сказал, что среди троих персонажей рыцарь лишь один. С другой стороны, если бы А был лжецом, то утверждение о том, что из трех островитян А, В и С рыцарь лишь один, было бы истинным. Но тогда А, будучи лжецом, не мог бы высказать это истинное утверждение. Следовательно, на вопрос незнакомца А не мог бы ответить: "Среди нас один рыцарь". Следовательно, В неверно передал высказывание А, из чего мы заключаем, что В - лжец, а С - рыцарь.

Задача 5. Две шкатулки

Вы можете рассуждать следующим образом. Если высказывание, выгравированное на крышке серебряной шкатулки, истинно, то это означает, что истинно ровно одно из двух высказываний. Тогда высказывание, выгравированное на крышке золотой шкатулки, должно быть ложным. С другой стороны, предположим что высказывание, помещенное на крышке серебряной шкатулки ложно. В этом случае утверждение о том, что ровно одно из двух высказываний истинно, было бы неверным. Это означает, что-либо оба высказывания истинны, либо оба высказывания ложны. Оба высказывания не могут быть истинными, так как по предположению второе высказывание ложно. Следовательно, оба высказывания ложны. Таким образом, высказывание, выгравированное на крышке золотой шкатулки, и в этом случае оказывается ложным. Итак, независимо от того, истинно или ложно высказывание на крышке серебряной шкатулки, высказывание, выгравированное на крышке золотой шкатулки, должно быть ложным. Следовательно, приз должен находиться в золотой шкатулке.

Каково же будет ваше удивление, если вы откроете золотую шкатулку и не обнаружите приза. Приз может быть в серебряной шкатулке или отсутствовать вообще. Где в ваши рассуждения вкралась ошибка?

Кто нам мешает взять любое число шкатулок и призов и разложить призы произвольным образом по шкатулкам? Дополнительно, мы можем написать произвольные надписи на шкатулках. Не зная ничего об истинности или ложности надписей, мы не можем прийти к какому-либо заключению. С самого начала в предыдущем рассуждении предполагается, что надпись, выгравированная на серебряной шкатулке, либо истинна, либо ложна и других вариантов нет. Да в логике высказываний у истинности всего два значения.

Но логика высказываний всего лишь модель логических отношений, и в данном случае надпись на серебряной шкатулке не может быть ни истинной ни ложной, ибо в любом случае мы приходим к противоречию с реальным положением вещей (точнее, положение призов в шкатулках). Вопрос о значениях истинности высказываний, определяемых в зависимости от их содержательной интерпретации (а именно такое высказывание на крышке серебряной шкатулки), относится к одному из наиболее тонких и фундаментальных разделов современной логики.

Приведем еще несколько цитат об отношении логики к реальному миру.

Ю. И. Манин ("Доказуемое и недоказуемое"):

"Предметом логики не является внешний мир, но лишь системы его осмысливания. Логика одной из таких систем – математики – в силу своей нормализованности представляет подобие жесткого трафарета, который можно накладывать на любую другую систему. Соответствие или расхождение этого трафарета с системой, однако, не служит критерием ее пригодности либо мерилom ценности.

Физик не обязан быть ни последовательным, ни непротиворечивым – он должен эффективно описывать природу на определенных уровнях. Тем менее логичны естественные науки и непосредственная работа сознания. Вообще, логичность, как условие эффективности появляется лишь в узкоспециализированных сферах человеческой деятельности"

Эдвард де Боно ("Латеральное мышление"):

Задача мышления – прийти не столько к правильному, сколько к эффективному решению. Эффективность в конечном счете предполагает и его правильность, но между этими двумя понятиями существует одно немаловажное отличие. Быть во всем правым – значит не позволить себе ни разу ошибиться. Быть эффективным – значит оказаться наконец правым только на самом последнем этапе"

П. С. Таранов ("Секреты поведения людей"):

"Однажды бедняк пришел к своему духовному наставнику:

- Бедность моя достигла предела, дети пухнут с голоду, жена болеет и нет денег на лечение – что делать?
- Нет ничего проще, - ответил духовный наставник. – Надо купить лотерейный билет и выиграть сто тысяч.
- Сто тысяч – это как раз то, что нужно. Но мне всегда не везет, как я узнаю, какой билет купить?
- Нет ничего проще. Ты пришел ко мне в четверг, сегодня у нас июль, так что покупай двадцать седьмой билет.

Бедняк послушался, купил двадцать седьмой билет, выиграл сто тысяч и со слезами на глазах пришел благодарить.

- Ты спас меня, отче, но как ты узнал, что нужен именно двадцать седьмой билет?
- Нет ничего проще, - ответил духовный наставник. – Ты пришел в четверг- это четыре, июль – седьмой месяц, четырежды семь – двадцать семь!
- Но четырежды семь – двадцать восемь?
- Глупец! – рассердился духовный наставник. – Ты выиграл и еще споришь!"

Задача 6. Примечания Литлвуда

Литлвуд законно ограничился примечанием 3: даже если он не знает французского языка, он в состоянии переписать французскую фразу.

Задача 7. Каким образом удалось Канту поставить верное время?

Выходя из дому, Кант заводит часы и запоминает, в каком положении находятся стрелки. Придя к другу и уходя из гостей, он отмечает время своего прихода и ухода. Это позволяет ему узнать, сколько он находился в гостях. Вернувшись домой и взглянув на часы, Кант определяет продолжительность своего отсутствия. Вычитая из этого времени то время, которое он провел в гостях, Кант узнает время, затраченное на дорогу туда и обратно. Прибавив ко времени выхода из гостей половину времени, затраченного на дорогу, Кант получает возможность узнать время прихода домой и перевести соответствующим образом стрелки своих часов.

Задача 8. Теорема о неподвижной точке

Представьте себе, что одновременно с монахом, взбирающимся в гору, сверху по той же тропинке стал спускаться его двойник. Поскольку эти два путника идут навстречу друг другу и каждый достиг своего пункта назначения, то, очевидно, в некоторой точке пути они встретились.

Задача 9. Рыцари, лжецы и нормальные люди

Прежде всего заметим, что А не может быть рыцарем, потому что рыцарь не назвал бы себя нормальным человеком. Следовательно, А- либо лжец, либо нормальный человек. Тогда истинно высказывание островитянина В. Значит, В - либо рыцарь, либо нормальный человек. Но В не может быть нормальным человеком (так как А - нормальный человек), поэтому В - рыцарь, а С - лжец. Но лжец не может сказать о себе, что он не нормальный человек (так как любой лжец - не нормальный человек), и мы приходим к противоречию. Итак, А не может быть нормальным человеком. Следовательно, А - лжец. Это означает, что высказывание островитянина В ложно, в силу чего В должен быть нормальным человеком (лжецом он быть не может, так как лжец - островитянин А). Итак, А - лжец, а В - нормальный человек. Отсюда мы заключаем, что С - рыцарь.

Задача 10. Четверо подсудимых А, В, С и D

Обозначим через А, В, С и D соответствующие высказывания "А виновен", "В виновен", "С виновен" и "D виновен". Имеем следующие истинные формулы:

- 1) $A \supset B$;
- 2) $B \supset (\neg A \vee C)$;
- 3) $\neg D \supset (A \& \neg C)$;
- 4) $D \supset A$.

Предположим, что D ложно, тогда из 3) следует, что А истинно и С ложно. Из 1) следует, что В истинно, поэтому из 2) следует $\neg A \vee C$ должно быть истинным высказыванием, но это противоречит истинности А и ложности С. Следовательно, наше исходное предположение было неверным. Поэтому D истинно. Из 4) и 1) следует, что А и В - истинные высказывания. Далее из 2) следует, что С истинно. При таком значении переменной D - истина. Тем самым установили, что все четыре подозреваемые являются виновными.

Задача 11. В Бронкс или Бруклин?

Необъяснимые на первый взгляд предпочтения парня к поездам в Бруклин заданы расписанием. Хотя поезда в обоих направлениях идут с интервалом 10 минут, расписание составлено так, что поезд в Бронкс прибывает и отправляется на 1 минуту позже, чем ближайший поезд в Бруклин. (Расписание могло быть такое: в Бруклин - 12.00, 12.10, 12.20,..., в Бронкс - 12.01, 12.11, 12.21,...) Чтобы попасть в поезд, идущий в Бронкс, молодой человек должен оказаться на станции в течении одного из минутных интервалов (12.00-12.01, 12.10-12.11, 12.20-12.21,...), а чтобы попасть на поезд, идущий в Бруклин, он должен прибыть на станцию в течении любого из девятиминутных интервалов (12.01-12.10, 12.11-12.20, 12.21-12.30,...). Вероятность поехать в Бронкс составляет 1/10, вероятность отправиться в Бруклин составляет 9/10.

Задача 12. Метаголоволомка - дело Джона

Если бы второй близнец также ответил "да", то судья, очевидно, не смог бы узнать, кто из них Джон. Поэтому ясно, что второй близнец должен быть ответить "нет". Это означает, что либо оба брата говорили правду, либо оба лгали. Однако они не могут говорить правду одновременно, поскольку согласно условию задачи, по крайней мере один из них всегда лжет. Следовательно, они оба лгали, и, значит Джоном зовут второго близнеца. (При этом, правда, нельзя установить, кто же из братьев всегда лжет.)

Задача 13. Три дамы с испачканными лицами

Формально: если я, А, не выгляжу смешной, то В должна рассуждать: если я, В, не выгляжу смешной, то С не над чем смеяться. Так как В так не рассуждает, то, следовательно, я, А, выгляжу смешной.

В принципе возможно обобщение на случай n дам с испачканными лицами и смеющихся.

По индукции: в $(n+1)$ -ситуации A рассуждает: если я не выгляжу смешной, то B, C, \dots образуют n -ситуацию и B должна бы перестать смеяться, но этого, однако, не происходит.

Задача 14. Рубины и изумруды

Задача кажется очень сложной, поэтому, как рекомендовал Декарт, попробуем упростить ее.

Допустим, что перед падишахом стоят всего два мудреца. - Вы один из них. Вы знаете, что хотя бы один изумруд положен в шкатулки. Вы видели, что вашему коллеге положили рубин. Отсюда вы с уверенностью заключаете, что изумруд у вас, и когда падишах издает свой клич, вы смело выходите вперед. Если же вы видели, что вашему коллеге положили изумруд, то вы спокойно стоите на месте: у вас может быть только рубин.

Теперь чуть-чуть усложним задачу: мудрецов может быть сколько угодно, но вы видели, что всем им положили рубины. Сможете вы сделать вывод о том, что вам положили изумруд? - Конечно! Хотя бы один изумруд должен быть и раз никому его не положили, значит он у меня. Таким образом, количество положенных рубинов вообще не имеет значения: что 5, что 10, что 100 - безразлично. Важны изумруды.

Следующее усложнение: Вы видели, как одному из ваших коллег положили изумруд. Тогда остается вопрос, что положили мне? - Это может быть рубин, а может быть и второй изумруд. Падишах приглашает в первый раз - вы остаетесь на месте, ибо не знаете, что у вас в шкатулке. Вы ждете, что выйдет тот мудрец, которому, как вы видели, положили изумруд. Но он не выходит! Почему? - Потому, что он тоже не знает, что у него в шкатулке. А почему не знает? Если бы всем, кроме него, положили рубины, он бы знал и вышел. Но он не выходит, значит, он видел, что кому-то еще положили изумруд. Но кому? Я видел, что всем, кроме него, положили рубины, следовательно, изумруд положили мне и тот мудрец это видел. - И когда падишах во второй раз произносит свое приглашение, я смело выхожу вперед. - Второй падишах с изумрудом рассуждает точно также и, поэтому, тоже выходит.

В сущности, ход рассуждения уже ясен. И основная идея уже отчетлива проявилась: падишаху придется повторять свое приглашение столько раз, сколько положено изумрудов. - Убедимся в этом еще раз. Пусть вы видели, что двоим из ваших коллег положили изумруды. Что у вас - вы не знаете. После первого приглашения никто не вышел. Вы спокойны. Но и после второго приглашения никто не вышел! Вот тут вы начинаете соображать: значит есть третий изумруд! Но у кого? Я видел только два, следовательно, третий должен быть у меня, поэтому на третье приглашение падишаха я выхожу.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература

1. Нефедов В. Н., Осипова В. А. Курс дискретной математики. М., 1992.
2. Бауэр Ф. Л., Гооз Г. Информатика. Вводный курс: Часть 2, М.: Мир, 1990.

Дополнительная литература

1. Кнут Д. Искусство программирования для ЭВМ. т.2. Получисленные алгоритмы. М.: Мир, 1977.
2. Никифоров А. Книга о логике. М.: "Гнозис", 1996
3. Манин Ю. И. Доказуемое и недоказуемое. М.: "Советское радио", 1979.
4. Смаллиан Р. Как же называется эта книга? М.: Мир, 1981.
5. Смаллиан Р. Принцесса или тигр? М.: Мир, 1985.
6. Смаллиан Р. Алиса в стране смекалки. М.: Мир, 1987.
7. Мендельсон Э. Введение в математическую логику. М., 1976.
8. Гарднер М. А ну-ка, догадайся! М.: Мир, 1984.