ФИНАНСОВАЯ АКАДЕМИЯ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Кафедра «Математика и финансовые приложения»

В.Б. Гисин

Лекции по дискретной математике

(часть 1)

МОСКВА 2001 ГОД

Аннотация

Пособие предназначено студентам, изучающим дискретную математику, и преподавателям, проводящим занятия по указанной дисциплине. Дисциплина «Дискретная математика» является обязательной для студентов дневного отделения института «Антикризисное управление и математические методы в экономике». Настоящее пособие содержит первую часть курса лекций по дискретной математике. В курсе изучаются теория множеств и математическая логика, комбинаторика, графы, бинарные отношения. Основные задачи курса – оснастить студентов математическим аппаратом, необходимым для построения и анализа экономико-математических моделей, и создать базу для изучения других математических дисциплин и информатики.

Оглавление

Предисловие

Математику традиционно делят на непрерывную и дискретную. К непрерывной математике относят то, что в той или иной форме опирается на идеи предела и непрерывности,

все остальное относят к дискретной математике в широком смысле. Содержание дискретной математики как одной из математических дисциплин существенно уже. Дискретная математика изучает те математические объекты, в которых дискретность, проявляющаяся в строении объекта и в динамике его изменения, является определяющей характеристикой.

Учебные курсы дискретной математики обычно содержат те разделы дискретной математики в широком смысле, которые не попали в другие математические курсы, но необходимы для полноценной подготовки специалистов соответствующего профиля, а также разделы, традиционно относимые к дискретной математике (булевы функции, дискретное представление информации, комбинаторика, графы).

В предлагаемом курсе можно выделить три главные линии. Во-первых, в курсе изучаются так называемые основания математики (теория множеств и математическая логика), без которых немыслима серьезная и профессиональная математическая подготовка. Во-вторых – теоретические основы современной информатики (теория алгоритмов и вычислимых функций, теория кодирования, алгебра логики). В третьих – те факты, методы и конструкции дискретной математики, которые применяются в экономико-математических моделях. Эти линии переплетаются и расходятся, но явно прослеживаются в любой теме курса.

В разделе «Начальные сведения» приводятся сведения из теории множеств, с которыми читатели частично могли познакомиться еще в школе. По сравнению со школьным материал заметно расширен и систематизирован. Понятия, которые вводятся в этом разделе, не являются специфическими для дискретной математики. Они составляют основу современного математического языка, общеупотребительны и используются во всех математических курсах.

При изучении каждой темы мы стараемся познакомить читателя с основными идеями и фундаментальными фактами и довести изложение до нетривиальных результатов. Объем, цели и задачи курса заставляют сводить к минимуму технически сложные и громоздкие построения (их в курсе, похоже, и нет). Приводимые доказательства, как правило, содержат некоторую важную идею (иногда, может быть, более важную, чем доказываемый факт). В ряде случаев мы не приводим доказательств. Это делается тогда, когда доказательства слишком сложны и объемны или не добавляют ничего нового к пониманию существа дела. Иногда мы ограничиваемся проведением доказательства для частных случаев. Это делается тогда, когда доказательство в общем случае, не давая ничего нового в смысле идей, связано со значительными техническими усложнениями.

Конец доказательства или примера отмечается значком “□”. Тем же значком отмечается конец формулировки теоремы, если

она приводится без доказательства, а также и других формулировок.

Рекомендуемая литература

1. *Горбатов В.А.* Фундаментальные основы дис-кретной математики, М., Наука, 2000. – 544 с.
2. *Грэхем Р., Кнут Д., Паташник О.* Конкретная математика, М., Мир, 1998. – 703 с.
3. *Ерусалимский Я.М.* Дискретная математика, М., Вузовская книга, 1999. – 280 с.
4. *Кемени Дж., Снелл Дж., Томпсон Дж.* Введение в конечную математику. М., Мир, 1965. – 486 с.
5. *Макаров И.М., и др.* Теория выбора и принятия решений. М., Наука, 1982. – 327 с.
6. *Нефедов В.Н., Осипова В.А.* Курс дискретной математики, М., Изд-во МАИ, 1992. – 262 с.
7. *Робертс Ф.С.* Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам, М., Наука, 1986. – 495 с.

Начальные сведения

1. Множества

1. Понятие множества. Понятие множества является одним из наиболее общих математических понятий. Его определение не удается свести к другим понятиям. Поэтому для понятия множества дается описательное определение, содержание и смысл которого раскрываются при изучении теории множеств. *Множество* – это набор, совокупность каких-

либо объектов, называемых его *элементами*, обладающих некоторым общим для них *характеристическим свойством*. В качестве примеров можно привести множество действительных чисел, множество решений заданного алгебраического уравнения, множество прямых, проходящих через заданную точку. В принципе никаких ограничений на природу элементов, их количество и свойства не налагается, так что допустимо рассмотрение таких множеств, как множество налогоплательщиков, множество процентных ставок и т. п.

Элементы, составляющие множество, обычно обозначаются малыми латинскими буквами, а само множество – большой латинской буквой. Знак $\in$ используется для обозначения принадлежности элемента множеству. Запись $a \in A$ означает, что элемент a принадлежит множеству A. Если некоторый объект x не является элементом множества A, пишут $x \notin A$. Например, если A – это множество четных чисел, то $2 \in A$, а $1 \notin A$. Множества A и B считаются равными (пишут $A=B$), если они состоят из одних и тех же элементов.

Если множество содержит конечное число элементов, его называют *конечным*; в противном случае множество называется *бесконечным*. Если множество A конечно, символом $|A|$ будет обозначаться число его элементов. Множество, не содержащее ни одного элемента, называется *пустым* и обозначается символом $\varnothing$. Очевидно, $|\varnothing|=0$.

Пример. Пусть A – множество действительных решений квадратного уравнения $x^2+px+q=0$. Множество A конечно, $|A|\le 2$. Если дискриминант $D = p^2-4q$ отрицателен, множество A пусто. Множество действительных решений квадратичного неравенства $x^2+px+q\le 0$ конечно, если $D\le 0$, и бесконечно, если $D>0$.□

Конечное множество может быть задано перечислением всех его элементов. Если множество A состоит из элементов x, y, z, …, пишут $A=\{x, y, z, \ldots\}$. Например, $A=\{0, 2, 4, 6, 8\}$ – множество четных десятичных цифр; $B=\{2, 3\}$ – множество решений уравнения $x^2-5x+6=0$; $C=\{0, 1, 2, 3, 4, 5, 6\}$ – множество остатков при делении целых чисел на 7.

Иногда перечислением элементов задают и бесконечное множество. Это делают в тех случаях, когда ясен алгоритм последовательного порождения элементов. Например, $A=\{0, 1, 4, 9, 16, \ldots\}$ – множество квадратов целых чисел.

В общем случае множества можно определять по так называемой *схеме свертывания*. При заданном характеристическом свойстве F и заданном классе элементов K множество A определяется как множество, которое содержит все элементы из K, обладающие свойством F. Для определения по схеме свертывания используется следующая запись:

$$A = \{x \mid x \text{ обладает свойством } F\}.$$

Применяя сокращение $F(x)$ для обозначения того, что элемент x обладает свойством F, будем писать

$$A = \{x \mid F(x)\}.$$

Класс K может быть указан явно; в этом случае используется запись

$$A = \{x \in K \mid F(x)\}.$$

Множество четных чисел P можно определить как

$$P = \{x \mid x - \text{четное целое число}\},$$

или как

$$P = \{\, x \in \boldsymbol{Z} \mid x \text{ четно}\},$$

где через $\boldsymbol{Z}$ обозначено множество целых чисел.

Неограниченное применение схемы свертывания ведет к противоречиям. Например, можно получить «множество всех множеств»:

$$M = \{x \mid x - \text{множество}\}.$$

Если считать M множеством, то получаем $M \in M$.

Рассмотрим *парадокс Рассела*, открытый в 1902 году. Назовем множество правильным, если оно не является своим элементом, и неправильным в противном случае. Определим множество R как множество всех правильных множеств. Более формально:

$$R = \{x \mid x \notin R\}.$$

В соответствии с определением для любого множества A справедливо утверждение:

$A \in R$ тогда и только тогда, когда $A \notin A$.

В частности, если считать R множеством, то его само можно взять в качестве A, но тогда мы придем к противоречию:

$R \in R$ тогда и только тогда, когда $R \notin R$.

Более подробно. Если R правильное, то есть не является своим элементом, то оно должно находиться в R, то есть быть своим элементом. Если же R неправильное, то оно является своим элементом, то есть содержится в R, но R содержит только правильные множества. Таким образом, R не может быть ни правильным, ни неправильным.

Введем используемое в дальнейшем понятие *индексированного семейства множеств*. Пусть I – некоторое множество, каждому элементу которого i сопоставлено однозначно определенное множество A_i. Элементы множества I называют индексами, а совокупность множеств A_i называют индексированным семейством множеств и обозначают через $(A_i)_{i \in I}$.

2. Подмножества. Говорят, что множество B является *подмножеством* (или *частью*) множества A и пишут $B \subset A$, если всякий элемент множества B является элементом множества A. Например, множество натуральных чисел $\boldsymbol{N}$ является подмножеством множества целых чисел $\boldsymbol{Z}$, а последнее в свою очередь является подмножеством множества рациональных чисел $\boldsymbol{Q}$, то есть $\boldsymbol{N} \subset \boldsymbol{Z}$ и $\boldsymbol{Z} \subset \boldsymbol{Q}$, или, короче, $\boldsymbol{N} \subset \boldsymbol{Z} \subset \boldsymbol{Q}$. Легко видеть, что если $B \subset A$ и $A \subset B$, то множества A и B состоят из одних и тех же элементов, и, значит, $A = B$. Наряду

с обозначением $B \subset A$ используется также $A \supset B$, имеющее тот же смысл.

Вообще говоря, подмножество множества A может быть задано определяющим свойством. Например, свойство быть четным числом определяет в множестве целых чисел подмножество четных чисел. Каково бы ни было множество A, пустое множество и само A являются его подмножествами: $\varnothing \subset A$, $A \subset A$. Пустое множество может быть задано свойством, которым не обладает ни один элемент множества A, например, $x \neq x$. Возможны и более содержательные ситуации. Например, свойство быть корнем уравнения $x^2+1=0$ задает в множестве действительных чисел пустое подмножество. Множество A может быть задано как свое подмножество каким-нибудь свойством, которым обладают все элементы множества A, например, $x=x$. Подмножества множества A, отличные от $\varnothing$ и A, называются *собственными*. Для заданного множества A обозначим через 2^A множество всех его подмножеств.

Пример. Пусть $A=\{a, b, c\}$. Тогда множество 2^A состоит из следующих элементов:

$$\{\varnothing\}, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}.\square$$

Далее будет показано, что если множество A конечно и содержит n элементов, то это множество имеет 2^n подмножеств, то есть $|2^A|=2^{|A|}$.

3. Пересечение и объединение множеств. *Пересечение* множеств A и B, обозначаемое $A \cap B$, – это множество,

состоящее из всех тех элементов, которые принадлежат обоим множествам A и B. Например, если A={1,2,3} и B={2,3,4}, то $A \cap B$={2,3}. В соответствии с определением

$$A \cap B \subset A \quad \text{и} \quad A \cap B \subset B,$$

причем $A \cap B$ является в определенном смысле наибольшим множеством, обладающим этими свойствами:

если $C \subset A$ и $C \subset B$, то $C \subset A \cap B$.

Далее, $A \cap B = B$ тогда и только тогда, когда $B \subset A$. Если множества A и B не имеют общих элементов, их пересечение пусто, $A \cap B = \varnothing$; в этом случае говорят, что множества A и B *не пересекаются*.

Объединение множеств A и B, обозначаемое $A \cup B$, – это множество, состоящее из всех тех элементов, которые принадлежат хотя бы одному из множеств A и B. Например, если A={1,2,3} и B={2,3,4}, то $A \cup B$={1,2,3,4}. В соответствии с определением

$$A \subset A \cup B \text{ и } B \subset A \cup B,$$

причем $A \cup B$ является наименьшим множеством, обладающим этими свойствами:

если $A \subset C$ и $B \subset C$, то $A \cup B \subset C$.

Далее, $A \cup B = B$ тогда и только тогда, когда $A \subset B$.

Операции пересечения и объединения можно обобщить на случай произвольного индексированного семейства множеств.

Пересечением семейства множеств $(A_i)_{i\in I}$ называется множество A, состоящее из всех тех элементов, которые принадлежат каждому из множеств A_i. Пишут $A=\cap_{i\in I}A_i$. Если множество индексов состоит из натуральных чисел, используются и другие обозначения. Например, $A_1\cap A_2\cap A_3$, если $I=\{1,2,3\}$; $A_1\cap A_2\cap\ldots\cap A_n$ или $\bigcap\limits_{i=1}^{n}A_i$, если $I=\{1,2,\ldots,n\}$; $\bigcap\limits_{i=1}^{\infty}A_i$, если I – это множество всех натуральных чисел, и т. п. Аналогично *объединением семейства множеств* $(A_i)_{i\in I}$ называется множество A, состоящее из всех тех элементов, которые принадлежат хотя бы одному из множеств A_i. Для объединения используют обозначение $A=\cup_{i\in I}A_i$ и другие, подобные тем, которые используются для пересечения.

Пример. Пусть $A_n=\left[0;\dfrac{n}{n+1}\right]$, где $n=1,2,\ldots$ пробегает множество натуральных чисел. Тогда, очевидно, $\bigcap\limits_{n=1}^{\infty}A_n=\left[0;\dfrac{1}{2}\right]$, поскольку $A_1\subset A_2\subset\ldots$. Покажем, что $\bigcup\limits_{n=1}^{\infty}A_n=[0;1)$. В самом деле, если $x\in[0;\,1)$, то $x\in A_n$, когда $x>1/n$, то есть при $n>1/x$. Если же $x<0$ или $x>1$, то x не попадает ни в одно из A_n, а значит, и в их объединение.□

4. Разность множеств. Дополнение множества. *Разность* множеств A и B, обозначаемая $A\backslash B$, – это множество, состоящее из всех тех элементов, которые принадлежат множеству A, но

не принадлежат множеству B. Например, если $A=\{1,2,3\}$ и $B=\{2,3,4\}$, то $A\setminus B=\{1\}$. В соответствии с определением

$$A\setminus B\subset A \quad \text{и} \quad (A\setminus B)\cap B=\varnothing,$$

причем $A\setminus B$ является в определенном смысле наибольшим множеством, обладающим этими свойствами:

если $C\subset A$ и $C\cap B=\varnothing$, то $C\subset A\setminus B$.

Далее, $A\setminus B=A$ тогда и только тогда, когда $A\cap B=\varnothing$, и $A\setminus B=\varnothing$ тогда и только тогда, когда $A\subset B$. Если $B\subset A$, то разность $A\setminus B$ называют также дополнением (или *относительным дополнением*) множества B в множестве A. Иногда относительное дополнение будет обозначаться через $\overline{B}_A$. Любое собственное подмножество B множества A вместе со своим относительным дополнением образует разбиение множества A на два непересекающихся множества:

$$B\cap\overline{B}_A=\varnothing,\ B\cup\overline{B}_A=A.$$

Часто в теоретико-множественных конструкциях используется *универсальное* множество U. Считается, что все рассматриваемые множества являются его подмножествами. Относительное дополнение множества A до универсального множества называется *дополнением* (без прилагательного «относительное») и обозначается через $\overline{A}$. Очевидно, $\overline{U}=\varnothing$ и $\overline{\varnothing}=U$.

Симметрическая разность множеств A и B, обозначаемая $A\Delta B$, – это множество, состоящее из всех тех элементов,

которые принадлежат одному из множеств A и B, но не принадлежат другому. Более формально,

$$A\Delta B = (A\backslash B) \cup (B\backslash A).$$

Например, если $A=\{1,2,3\}$ и $B=\{2,3,4\}$, то $A\Delta B=\{1,4\}$.

5. Свойства операций над множествами. Приведем основные тождества так называемой алгебры множеств (будем предполагать, что используемые в тождествах множества A, B, C являются подмножествами универсального множества U).

Коммутативность:

$$1.\ A\cap B=B\cap A; \quad 1'.\ A\cup B=B\cup A.$$

Ассоциативность:

$$2.\ (A\cap B)\cap C=A\cap (B\cap C); \quad 2'.\ (A\cup B)\cup C=A\cup (B\cup C).$$

Дистрибутивность:

$$3.\ (A\cup B)\cap C=(A\cap B)\cup (B\cap C); \quad 3'.\ (A\cap B)\cup C=(A\cup B)\cap (B\cup C).$$

Идемпотентность:

$$4.\ A\cap A=A; \qquad 4'.\ A\cup A=A.$$

Законы поглощения:

$$5.\ A\cap (A\cup B)=A; \qquad 5'.\ A\cup (A\cap B)=A.$$

Законы нуля и единицы:

$$6.\ A\cap U=A; \qquad 6'.\ A\cup\varnothing=A.$$

$$7.\ A\cap\varnothing=\varnothing; \qquad 7'.\ A\cup U=U;$$

$$8.\ A\cap\overline{A}=\varnothing; \quad 8'.\ A\cup\overline{A}=U.$$

Инволютивность дополнения:

$$9.\ \overline{\overline{A}} = A\ .$$

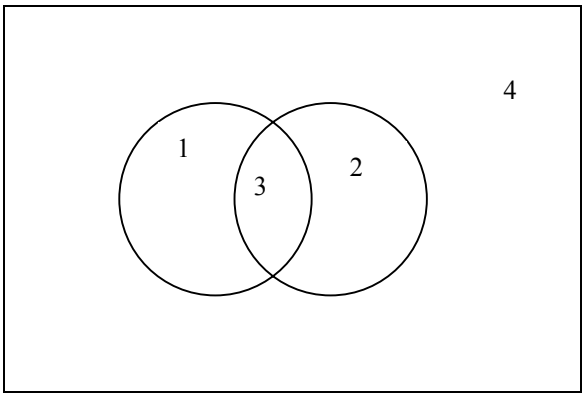
Законы де Моргана:

$$10.\ \overline{A \cap B} = \overline{A} \cup \overline{B}\ ;\quad 10'.\ \overline{A \cup B} = \overline{A} \cap \overline{B}\ .$$

Убедиться в справедливости перечисленных свойств можно путем несложной непосредственной проверки.

Пример. Проверим первый из законов де Моргана. Покажем сначала, что $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$. Предположим, что $x \in \overline{A \cap B}$. Тогда $x \notin A \cap B$, так что x не принадлежит хотя бы одному из множеств A и B. Таким образом, $x \notin A$ или $x \notin B$, то есть $x \in \overline{A}$ или $x \in \overline{B}$. Это означает, что $x \in \overline{A} \cup \overline{B}$. Мы показали, что произвольный элемент множества $\overline{A \cap B}$ является элементом множества $\overline{A} \cup \overline{B}$. Следовательно, $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$. Обратное включение $\overline{A \cap B} \supset \overline{A} \cup \overline{B}$ доказывается аналогично. Достаточно повторить все шаги предыдущего рассуждения в обратном порядке.□

6. Диаграммы Эйлера–Венна. Для наглядного представления операций над подмножествами некоторого универсального множества используются диаграммы Эйлера–Венна. На таких диаграммах фон рисунка соответствует универсальному множеству, а фигуры изображают множества, участвующие в операциях. Например, на следующем рисунке



круги изображают множества A и B. Объединение двух кругов соответствует объединению $A \cup B$; область 3 соответствует пересечению $A \cap B$; область 1 – множеству $A \setminus B = A \cap \overline{B}$; область 2 – множеству $B \setminus A = \overline{A} \cap B$; область 4 – множеству $\overline{A \cup B}$; объединение областей 1 и 2 соответствует симметрической разности $A \Delta B$. Легко видеть, что имеет место следующее соотношение:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

7. Прямое произведение множеств. Из любой пары элементов a и b (не обязательно различных) можно составить новый элемент – *упорядоченную пару* (a,b). Упорядоченные пары (a,b) и (c,d) считают равными и пишут $(a,b)=(c,d)$, если $a=c$ и $b=d$. В частности, $(a,b)=(b,a)$ лишь в том случае, когда $a=b$. Элементы a и b называют координатами упорядоченной пары (a,b) (соответственно первой и второй).

Прямым (декартовым) произведением множеств A и B называется множество всех упорядоченных пар (a,b), где $a \in A$ и

$b \in B$. Прямое произведение множеств A и B обозначается через $A \times B$. В соответствии с определением имеем

$$A \times B = \{(a,b) | \ a \in A, \ b \in B\}.$$

Пример. Пусть $A=\{1,2,3\}$ и $B=\{2,3,4\}$. Тогда множество $A \times B$ состоит из следующих девяти элементов: (1,4), (2,4), (3,4), (1,3), (2,3), (3,3), (1,2), (2,2), (3,2). Графически элементы произведения множеств $A \times B$ удобно помещать на «координатной плоскости», считая, что первый множитель A расположен на горизонтальной полуоси, а второй множитель B – на вертикальной. Например,

(1,4) (2,4) (3,4)

(1,3) (2,3) (3,3)

(1,2) (2,2) (3,2)

□

Подобно парам, можно рассматривать упорядоченные тройки, четверки и, вообще, упорядоченные наборы элементов произвольной длины. Упорядоченный набор элементов длины n обозначается через $(a_1,a_2,\ldots,a_n)$. Для таких наборов используется также название *кортеж* длины n. Допускаются в том числе и кортежи длины 1 – это просто одноэлементные множества. Кортежи $(a_1,a_2,\ldots,a_n)$ и $(b_1,b_2,\ldots,b_n)$ считаются равными, если $a_1=b_1$, $a_2=b_2,\ldots,a_n=b_n$.

По аналогии с произведением двух множеств определим *прямое произведение* множеств A_1, A_2, …, A_n как множество всех

кортежей $(a_1,a_2,\ldots,a_n)$ таких, что $a_1\in A_1$, $a_2\in A_2$, …, $a_n\in A_n$. Обозначается прямое произведение через $A_1\times A_2\times\ldots\times A_n$.

Понятие прямого произведения может быть обобщено на случай произвольного семейства множеств $(A_i)_{i\in I}$. Назовем I-кортежем набор элементов $(A_i)_{i\in I}$ такой, что $a_i\in A_i$ для каждого $i\in I$. Прямое произведение семейства множеств $(A_i)_{i\in I}$ – это множество, состоящее из всех I-кортежей. Для обозначения этого множества используется символ $\Pi_{i\in I}A_i$ и его разновидности, подобные тем, которые применяются для обозначения пересечения и объединения семейства множеств.

В случае, когда множество A умножается само на себя, произведение называют (декартовой) *степенью* и используют экспоненциальные обозначения. Так, в соответствии с определением $A\times A=A^2$, $A\times A\times A=A^3$ и т. д. Считается, что $A^1=A$ и $A^0=\varnothing$.

Непосредственно из определений следует справедливость следующих соотношений:

$$(A\cup B)\times C=(A\times C)\cup(B\times C);\ (A\cap B)\times C=(A\times C)\cap(B\times C);$$

$$(A\setminus B)\times C=(A\times C)\setminus(B\times C).$$

2. Отображения и соответствия

1. Понятие отображения. *Отображение* f множества X в множество Y считается заданным, если каждому элементу x из X сопоставлен ровно один элемент y из Y, обозначаемый $f(x)$.

Множество X называется *областью определения* отображения f, а множество Y – *областью значений*. Множество упорядоченных пар

$$\Gamma_f = \{(x, y) \mid x \in X, y \in Y, y = f(x)\}$$

называют *графиком* отображения f. Непосредственно из определения вытекает, что график отображения f является подмножеством декартова произведения $X \times Y$:

$$\Gamma_f \subset X \times Y.$$

Строго говоря, отображение – это тройка множеств (X, Y, G) такая, что $G \subset X \times Y$, и каждый элемент x из X является первым элементом ровно одной пары (x, y) из G. Обозначая второй элемент такой пары через $f(x)$, получаем отображение f множества X в множество Y. При этом $G = \Gamma_f$. Если $y = f(x)$, мы будем писать $f: x \to y$ и говорить, что элемент x переходит или отображается в элемент y; элемент $f(x)$ называется образом элемента x относительно отображения f. Для обозначения отображений мы будем использовать записи вида $f: X \to Y$. Часто отображения задают равенством вида $y = f(x)$, где x и y – переменные; значениями переменной x, называемой аргументом, служат элементы множества X; переменная y принимает свои значения в множестве Y. В этом случае отображения называют также функциями.

Примеры. 1) Пусть $X = Y$ – множество действительных чисел. Формула $y=2x$ задает отображение множества X в множество Y.

2) Пусть X – множество всех треугольников на плоскости, а Y – множество действительных чисел. Сопоставляя треугольнику его площадь, получаем отображение первого множества во второе.

3) Пусть $X = \{1, 2, 3\}$, $Y = \{2, 3, 4\}$. Множество пар

$$G = \{(1, 2), (2, 2), (3, 3)\}$$

задает отображение f, при котором $f(1)=f(2)=2$, $f(3)=3$.□

Отображение f конечного множества $X = \{a, b, \ldots, c\}$ в себя часто бывает удобно задать с помощью таблицы (матрицы), состоящей из двух строк. В первой строке располагаются элементы множества X, а под ними, во второй строке – их образы:

$$\begin{pmatrix} a & b & \ldots & c \\ f(a) & f(b) & \ldots & f(c) \end{pmatrix}.$$

Например, таблица

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

задает отображение множества четвертей координатной плоскости в себя при повороте плоскости на 90º против часовой стрелки вокруг начала координат (естественно, вместо самих четвертей мы используем их номера).

Пусть $f: X \to Y$ – отображение множества X в множество Y, а A и B – подмножества множеств X и Y соответственно. Множество

$$f(A)=\{y \mid y=f(x) \text{ для некоторого } x \in A\}$$

называется *образом* множества A. Множество

$$f^{-1}(B)=\{x \mid f(x) \in B\}$$

называется *прообразом* множества B. Отображение $f: A \to Y$, при котором $x \to f(x)$ для всех $x \in A$, называется *сужением* отображения f на множество A; сужение будет обозначаться через $f|_A$.

Отображение вида $f: X \times Y \to Z$ называют функцией двух переменных и пишут $z=f(x,y)$. Аналогично определяются функции большего числа переменных.

Пусть имеются отображения $f: X \to Y$ и $g: Y \to Z$. Отображение $X \to Z$, при котором x переходит в $g(f(x))$, называется *композицией* отображений f и g и обозначается через $f \cdot g$ или просто fg. Таким образом,

$$(fg)(x)=g(f(x)).$$

Например, если отображения f, g множества действительных чисел в себя заданы формулами

$$f(x)=x+1,\ g(x)=2x,$$

то

$$(fg)(x)=g(f(x))=g(x+1)=2(x+1);$$

$$(gf)(x)=f(g(x))=f(2x)=2x+1.$$

2. Специальные виды отображений. Отображение множества X в X, при котором каждый элемент переходит сам в себя, $x\to x$, называется *тождественным* и обозначается через id_X.

Для произвольного отображения $f\colon X\to Y$ имеем

$$id_X \cdot f = f\cdot id_Y.$$

Отображение $f\colon X\to Y$ называется *инъективным*, если образы различных элементов также различны, то есть $f(x)\neq f(y)$ при $x\neq y$. Отображение $f\colon X\to Y$ называется *сюръективным* (говорят также, что f – отображение X на Y) если всякий элемент y из Y является образом некоторого элемента x из X, то есть $f(X)=Y$. Отображение $f\colon X\to Y$ называется *биективным*, если оно одновременно инъективно и сюръективно. Биективное отображение $f\colon X\to Y$ *обратимо*. Это означает, что существует отображение $g\colon Y\to X$, называемое *обратным* к отображению f, такое, что

$$g(f(x))=x \text{ и } f(g(y))=y$$

для любых $x\in X$, $y\in Y$.Ясно, что при этом отображение f является обратным к отображению g. Отображение, обратное к отображению f, обозначается через f^{-1}. В соответствие с определением

$$ff^{-1}=id_X,\quad f^{-1}f=id_Y,\quad (f^{-1})^{-1}=f.$$

Нетрудно видеть, что отображение биективно тогда и только тогда, когда оно обратимо. Говорят, что обратимое отображение $f: X \to Y$ устанавливает *взаимно однозначное соответствие* между элементами множеств X и Y, или, короче, между множествами X и Y. Инъективное отображение $f: X \to Y$ устанавливает взаимно однозначное соответствие между множеством X и множеством $f(X)$.

Примеры. 1) Функция $f: \boldsymbol{R} \to \boldsymbol{R}_{>0}$, $f(x)=e^x$, устанавливает взаимно однозначное соответствие множества всех действительных чисел $\boldsymbol{R}$ с множеством положительных действительных чисел $\boldsymbol{R}_{>0}$. Обратным к отображению f является отображение $g: \boldsymbol{R}_{>0} \to \boldsymbol{R}$, $g(x)=\ln x$.

2) Отображение $f: \boldsymbol{R} \to \boldsymbol{R}_{\geq 0}$, $f(x)=x^2$, множества всех действительных $\boldsymbol{R}$ на множество неотрицательных чисел $\boldsymbol{R}_{\geq 0}$ сюръективно, но не инъективно, и поэтому не является биективным.□

3. Операции. *Бинарной операцией* на множестве X называется отображение $f: X \times X \to X$. Результат применения бинарной операции к паре (x,y) принято записывать в виде $x*y$, где $*$ – символ операции. Таким образом, $f: (x,y) \to x*y$.

Примеры. Отображение $f: \boldsymbol{R} \times \boldsymbol{R} \to \boldsymbol{R}$, $f(x,y) = x+y$, – это операция сложения на множестве действительных чисел; $f: 2^X \times 2^X \to 2^X$, $f(A,B) = A \cap B$ – операция пересечения на множестве подмножеств множества X.□

Бинарная операция $*$ на множестве X называется:

коммутативной, если $x*y = y*x$ для всех x, y из X;

ассоциативной, если $(x*y)*z = x*(y*z)$ для всех x, y, z из X.

При записи повторенной несколько раз ассоциативной бинарной операции скобки можно опускать – результат от порядка выполнения операций не зависит. Например,

$$((x*y)*z)*t = (x*(y*z))*t = x*((y*z)*t) = x*(y*(z*t)).$$

Операции сложения и умножения на множестве действительных чисел коммутативны и ассоциативны; операции объединения и пересечения подмножеств универсального множества также коммутативны и ассоциативны. Рассмотрим не столь очевидный пример.

Пример. Зададим бинарную операцию на отрезке [0; 1] формулой

$$x*y = x+y-xy.$$

Очевидно, так определенная операция коммутативна. Покажем, что она и ассоциативна. Имеем

$$(x*y)*z = (x+y-xy))*z = x+y-xy+z-(x+y-xy)z = x+y+z-xy-xz-yz+xyz;$$

$$x*(y*z) = x*(y+z-yz) = x+y+z-yz-x(y+z-yz) = x+y+z-xy-xz-yz+xyz,$$

откуда $(x*y)*z = x*(y*z)$.□

Бинарная операция на конечном множестве может быть задана с помощью таблицы.

Пример. Зададим на множестве X={0, 1, 2, 3, 4} операцию «умножение по модулю 5» (остаток при делении произведения на 5):

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Верхняя строка и левый столбец содержат элементы множества X, которые служат метками соответствующих столбцов и строк. На пересечении строки с меткой x и столбца с меткой y находится произведение xy по модулю 5. Например, произведение 2 на 3 по модулю 5 равно 1.□

4. Характеристические функции. Пусть X – некоторое множество, и A – его подмножество. Определим отображение χ_A множества X в двухэлементное множество {0,1} следующим образом: $\chi_A(x)=1$, если $x\in A$, и $\chi_A(x)=0$, если $x\notin A$. Функция χ_A называется *характеристической функцией* подмножества A.

Очевидно, $A\subset B$ тогда и только тогда, когда $\chi_A(x)\le\chi_B(x)$ для всех x.

Имеется простая связь между операциями над подмножествами множества X и операциями над их характеристическими функциями:

$$\chi_{A\cap B}(x) = \min(\chi_A(x), \chi_B(x)) = \chi_A(x)\cdot\chi_B(x);$$

$$\chi_{A\cup B}(x) = \max(\chi_A(x), \chi_B(x)) = \chi_A(x)+\chi_B(x)-\chi_A(x)\cdot\chi_B(x);$$

$$\chi_{A\setminus B}(x) = \max(\chi_A(x)-\chi_B(x), 0) = \chi_A(x)\cdot(1-\chi_B(x));$$

$$\chi_X(x)\equiv 1;\ \chi_\varnothing(x)\equiv 0.$$

5. Соответствия. Пусть даны множества X и Y. Будем говорить, что задано *соответствие* R из X в Y, если для каждого элемента x множества X указано подмножество $R(x)\subset Y$ соответствующих ему элементов множества Y (возможно, пустое). Множество элементов x из X, для которых $R(x)$ не пусто, будем называть *областью определения* соответствия R и обозначать через $D(R)$. Множество всех тех элементов y из Y, которые принадлежат хотя бы одному множеству $R(x)$, будем называть *полным образом* соответствия R и обозначать через $B(R)$. Более общо, для произвольного $A\subset X$ будем обозначать через $R(A)$ и называть *образом множества* A множество всех тех $y\in Y$, которые принадлежат хотя бы одному множеству $R(x)$ с $x\in X$, то есть $R(A)= \cup_{x\in A}R(x)$. Полный образ соответствия R совпадает с образом множества X. Нетрудно видеть, что $B(R)=R(X)=R(D(R))$.

Понятие соответствия обобщает понятие функции. Если каждое множество $R(x)$ содержит ровно один элемент, то

соответствие R называется *функциональным*. Всякое функциональное соответствие R определяет отображение множества X в множество Y, при котором произвольному элементу x множества X соответствует единственный элемент множества $R(x)$. Ясно, что R является графиком этого отображения. Допуская небольшую вольность, будем обозначать это отображение также через R.

Примеры. 1) Натуральному числу x поставим в соответствие совокупность его простых делителей. Тем самым определяется соответствие R из множества натуральных чисел в множество простых чисел. Имеем $R(10)=\{2, 5\}$, $R(30)=\{2, 3, 5\}$, $R(7)=\{7\}$, $R(1)=\varnothing$.

2) Пусть A – множество участников рынка, а T – множество товаров. Для каждого товара t указана его цена p, для каждого участника ранка a – его бюджет b. Назовем возможным планом потребления участника рынка набор товаров, суммарная стоимость которых не превосходит его бюджета. Сопоставим каждому участнику рынка a множество возможных планов потребления. Этим определяется соответствие R из A в множество всех подмножеств множества T. Например, пусть $T=\{t_0, t_1, t_2, t_3\}$, $p_0=-2$, $p_1=1$, $p_2=2$, $p_3=3$ (отрицательную цену имеет товар, который может быть продан на рынке, например, труд); $A=\{a_1, a_2, a_3\}$, $b_1=0$, $b_2=2$, $b_3=10$. Тогда

$$R(a_1)=\{\{t_0\}, \{t_0, t_1\}, \{t_0, t_2\}\},$$

$$R(a_2)=\{\{t_0\}, \{t_1\}, \{t_2\}, \{t_0, t_1\}, \{t_0, t_2\}, \{t_0, t_3\}, \{t_0, t_1, t_2\}, \{t_0, t_3\}\},$$

$$R(a_3)=2^T.\square$$

Формально соответствие R из множества X в множество Y можно определить как подмножество декартова произведения $X\times Y$, считая, что $(x,y)\in R$, если $y\in R(x)$.

Рассматривая соответствия из X в Y как подмножества множества $X\times Y$, можно говорить о том, что одно соответствие является *частью* другого, можно образовывать *пересечение* и *объединение* соответствий и т. п. Пусть S, $R\subset X\times Y$ – пара соответствий из X в Y. Непосредственно из определений вытекают следующие свойства соответствий:

1) $S\subset R$ *в том и только том случае, если* $S(x)\subset R(x)$ *для всех* $x\in R$;

2) $(S\cap R)(x)=S(x)\cap R(x)$;

3) $(S\cup R)(x)=S(x)\cup R(x)$.

Пусть $R\subset X\times Y$ – соответствие из X в Y.

Сужением соответствия R на подмножество $X'\subset X$ называется соответствие $R'=R\cap X'\times Y$. Легко видеть, что $D(R')=X'\cap D(R)$ и $R'(x)=R(x)$ для любого $x\in X$. Сужение будет иногда обозначаться через $R|_{X'}$.

Соответствие из Y в X, определяемое формулой

$$R^{-1}=\{(y,x)|(x,y)\in R\},$$

называется *обратным* к соответствию R. Очевидно, $x\in R^{-1}(y)$ тогда и только тогда, когда $y\in R(x)$. Непосредственно из определений следует, что

$$(R^{-1})^{-1}=R;\ D(R^{-1})= B(R);\quad B(R^{-1})=D(R).$$

Если соответствие $R\subset X\times Y$ функционально, то обратное соответствие R^{-1} окажется функциональным лишь в том случае, когда отображение, задаваемое соответствием R, биективно; обратное соответствие задает в этом случае обратное отображение.

Для произвольного множества X обозначим через E_X соответствие, определяющее тождественное отображение множества X в себя, при этом соответствии каждому элементу множества X соответствует лишь сам этот элемент, то есть $E_X(x)=\{x\}$. Соответствие E_X задается диагональю декартова квадрата множества X:

$$E_X = \{(x,x) \mid x\in X\} \subset X\times X.$$

Мы будем называть соответствие E_X *тождественным* или *диагональным*.

6. Композиция соответствий. Пусть заданы соответствия R из X в Y и S из Y в Z. Их *композицией* (или произведением) называется соответствие P из X в Z такое, что $P(x)=S(R(x))$ для всех x из X. Композиция соответствий R и S обозначается через RS. Согласно определению имеем

$$RS = \{(x,z) \mid \textit{существует } y\in Y, \textit{ для которого } (x,y)\in R \textit{ и } (y,z)\in S\}.$$

Если $X=Y=Z$ и $R=S$, то вместо RR пишут R^2, вместо $(R^2)R$ – (R^3) и т.д.

Пример. Пусть T – множество наборов товаров такое же, как в примере из предыдущего пункта. Будем считать, что набор товаров улучшается, если к нему добавляется один из товаров с положительной ценой или из него выводится товар с отрицательной ценой. Будем говорить, что набор товаров V лучше, чем набор товаров U, если V может быть получен из U несколькими последовательными улучшениями. Например, наборы $\{t_0,t_1\}$, $\{t_0,t_1,t_2\}$, $\{t_1,t_2\}$ получаются последовательными улучшениям. Обозначим через $P(U)$ множество тех наборов, которые получаются из набора U путем его однократного улучшения. Например, $P(\{t_0,t_1\})=\{\{t_0,t_1,t_2\}, \{t_0,t_1,t_3\}, \{t_1\}\}$; $P(\{t_1,t_2,t_3\})=\varnothing$. Тогда $P^2(U)$ – это множество наборов, которые получаются из U двумя последовательными улучшениями, $P^3(U)$ – это множество наборов, которые получаются из U тремя последовательными улучшениями и т.д. Очевидно, $P^5(U)= \varnothing$ для любого набора U. Положим $S=P\cup P^2\cup P^3\cup P^4$. Тогда $S(U)$ – это множество наборов, которые лучше, чем набор U.□

Укажем некоторые свойства композиции соответствий.

1) *Диагональные соответствия играют роль единиц*: *для любого* $R\subset X\times Y$ *имеем*

$$E_X R=R=RE_Y.$$

2) *Композиция ассоциативна*: *если* $R\subset X\times Y$, $S\subset Y\times Z$, $T\subset Z\times W$, *то*

$$(RS)T=R(ST).$$

3) *Если* $R \subset X \times Y$, $S \subset Y \times Z$, *то*

$$(RS)^{-1} = S^{-1}R^{-1}.$$

4) *Композиция монотонна относительно включения*: *если* $R_1, R_2 \subset X \times Y$, $S \subset Y \times Z$, *то*

$$R_1 \subset R_2 \text{ влечет } R_1S \subset R_2S.$$

5) *Если* $R_1, R_2 \subset X \times Y$, $S \subset Y \times Z$, *то*

$$(R_1 \cup R_2)S = R_1S \cup R_2S.$$

Замечание. Аналог свойства 5 для пересечений, вообще говоря, неверен. Включение

$$(R_1 \cap R_2)S \subset R_1S \cap R_2S$$

имеет место всегда, однако оно может оказаться строгим. Например, пусть

$$X = Y = \{1, 2\}, Z = \{1\};$$

$$R_1 = \{(1,1), (2,2)\},$$

$$R_2 = \{(1,2), (2,1)\},$$

$$S = \{(1,1), (2,1)\}.$$

Тогда $R_1 \cap R_2 = \varnothing$, так что $(R_1 \cap R_2)S = \varnothing$. С другой стороны, $R_1S = S$ и $R_2S = S$, откуда $R_1S \cap R_2S = S$.□

В заключение приведем характеристику функциональных соответствий.

Теорема. *Соответствие R из множества X в множество Y функционально тогда и только тогда*, *когда выполняются следующие соотношения*:

$$RR^{-1} \supset E_X,\ R^{-1}R \subset E_Y.$$

Доказательство. Предположим сначала, что соответствие R функционально. Тогда R состоит из пар вида $(x,f(x))$, $x \in X$, где f – отображение из X в Y. Для любого $x \in X$ имеем $(x,f(x)) \in R$ и $(f(x),x) \in R^{-1}$, и, значит, $(x,x) \in RR^{-1}$. Этим доказывается первое включение. Для доказательства второго достаточно показать, что $(y,y') \in R^{-1}R$ лишь в том случае, когда $y=y'$. В самом деле, если $(y,y') \in R^{-1}R$, то найдется $x \in X$ такой, что $(y,x) \in R^{-1}$ и $(x,y') \in R$. Эти два условия означают соответственно, что $y=f(x)$ и $y'=f(x)$, откуда $y=y'$. Обратно, предположим, что выполняются соотношения из формулировки теоремы и покажем, что R функционально. Из $RR^{-1} \supset E_X$ вытекает, что для произвольного $x \in X$ найдется такой $y \in Y$, что $(x,y) \in R$ и $(y,x) \in R^{-1}$. Значит, $y \in R(x)$ и $R(x) \neq \varnothing$. Следовательно, R определено на всем X, то есть $D(R)=X$. Далее, пусть $(x,y) \in R$ и $(x,y') \in R$. Тогда $(y,x) \in R^{-1}$ и, значит, $(y,y') \in R^{-1}R$. Поскольку $R^{-1}R \subset E_Y$, отсюда следует, что $y=y'$.□

Замечание. Из доказательства теоремы видно, что условие $RR^{-1} \supset E_X$ равносильно тому, что R определено на всем X. Условие $R^{-1}R \subset E_Y$ означает, что $R(x)$ состоит ровно из одного элемента для каждого $x \in D(R)$, то есть сужение R на $D(R)$ – функциональное соответствие. Про соответствие R, удовлетворяющее условию $RR^{-1} \supset E_X$, будем говорить, что оно *всюду определено*, а про соответствие R, удовлетворяющее

условию $R^{-1}R \subset E_Y$, – что оно является *частичным отображением* (*частичной функцией*) и отображает $D(R)$ в Y.

3. Отношения

1. Понятие отношения. Подмножество $R \subset X^n$ называется n-местным или n-арным *отношением* на множестве X. Говорят, что элементы $x_1, x_2, \ldots, x_n$ (в указанном порядке) *связаны отношением* R или *находятся в отношении* R, если $(x_1, x_2, \ldots, x_n) \in R$. Наиболее часто в приложениях используются двухместные, или *бинарные* отношения, которые в основном и будут изучаться в дальнейшем. Иногда используются и другие отношения. При $n=1$ отношение называется *унарным*. Унарное отношение на множестве X – это просто некоторое подмножество R множества X. Унарное отношение можно трактовать как свойство: элемент $x \in X$ обладает свойством R, если $x \in R$. При $n=3$ отношение называется тернарным. В качестве примера приведем отношение R на множестве действительных чисел, которое содержит все тройки чисел (x_1, x_2, x_3) такие, что $x_3 = x_1 + x_2$. Например, $(1, 2, 3) \in R$, $(2, 3, 4) \notin R$.

По определению бинарное отношение R на множестве X – это подмножество декартова произведения $X \times X$. Бинарное отношение можно рассматривать как соответствие из X в X. Тем самым для бинарных отношений на множестве X определены булевы операции (объединение, пересечение и др.), операция

композиции, обращение. Диагональное соответствие E_X отвечает отношению равенства:

$$E_X = \{(x, x) \mid x \in X\} = \{(x,y) \mid x=y,\ x,y \in X\} \subset X \times X.$$

Если x и y связаны отношением R, то часто вместо $(x,y) \in R$ пишут xRy. Например, для отношения «равно» и отношения «меньше» на множестве действительных чисел вместо $(x,y) \in =$ и $(x,y) \in <$ принято писать соответственно $x=y$ и $x<y$. Эти два отношения являются примерами двух важнейших классов бинарных отношений – отношений эквивалентности и отношений порядка.

2. Свойства бинарных отношений. Пусть $R \subset X \times X$ – бинарное отношение на множестве X (мы будем далее опускать слово «бинарное», когда это не ведет к недоразумениям).

Отношение R называется *рефлексивным*, если оно содержит все пары вида (x,x), то есть xRx для любого x из X. Отношение R называется *антирефлексивным*, если оно не содержит ни одной пары вида (x,x). Например, отношение $x \le y$ рефлексивно, а отношение $x<y$ антирефлексивно. Рефлексивное отношение на множестве действительных чисел изображается на координатной плоскости множеством точек, содержащим прямую $y=x$. В общем случае рефлексивность отношения R означает, что $R \supset E_X$, а антирефлексивность – что $R \cap E_X = \varnothing$.

Отношение R называется *симметричным*, если вместе с каждой парой (x,y) оно содержит также и пару (y,x), то есть xRy

выполняется тогда и только тогда, когда выполняется yRx. Отношение R симметрично, если наличие (или отсутствие) связи между элементами x и y не зависит от порядка, в котором указаны эти элементы. Например, отношение $x+y>0$ симметрично, а отношение $x+2y>0$ – нет (симметричное отношение на множестве действительных чисел изображается на координатной плоскости множеством точек, симметричным относительно прямой $y=x$). Симметричность отношения R означает, что $R=R^{-1}$.

Отношение R называется *асимметричным*, если невозможно одновременное выполнение условий xRy и yRx. Например, отношение $x<y$ асимметрично. Асимметричность отношения R означает, что $R\cap R^{-1}=\varnothing$. Отношение R называется *антисимметричным*, если одновременное выполнение условий xRy и yRx невозможно при $x\neq y$, то есть, если xRy и yRx, то $x=y$. Например, отношение $x\leq y$ антисимметрично. Антисимметричность отношения R означает, что $R\cap R^{-1}\subset E_X$. Ясно, что всякое асимметричное отношение является антисимметричным и антирефлексивным.

Отношение R называется *транзитивным*, если вместе с любыми парами (x,y) и (y,z) оно содержит также и пару (x,z), то есть из xRy и yRz следует xRz. Например, отношение $x<y$ транзитивно, а отношение $x+y>0$ – нет. Транзитивность отношения R означает, что $R^2\subset R$.

Приведем некоторые свойства отношений, которые непосредственно вытекают из определений.

Каково бы ни было отношение R, *отношение* $R \cup E_X$ *рефлексивно*.

Каково бы ни было отношение R, *отношения* $R \cap R^{-1}$ *и* $R \cup R^{-1}$ *симметричны*.

Если отношение R *рефлексивно и транзитивно*, *то* $R^2 = R$.

Докажем последнее утверждение.

Доказательство. Поскольку R транзитивно, имеем $R^2 \subset R$. Обратно, так как R рефлексивно, то $E_X \subset R$, откуда, умножая на R, получаем $R = RE_X \subset R^2$.□

Примеры. Рассмотрим несколько отношений на множестве всех подмножеств некоторого множества U. Отношение включения $X \subset Y$ рефлексивно, антисимметрично и транзитивно. Отношение строго включения $X \subset Y$, $X \neq Y$, асимметрично и транзитивно. Пусть R – отношение, которое связывает множества X и Y, имеющие непустое пересечение, $X \cap Y \neq \varnothing$. Это отношение симметрично, но, вообще говоря, не транзитивно (транзитивным оно окажется лишь в том случае, когда множество U состоит из одного элемента). Отношение R не рефлексивно; рефлексивным является его сужение на множество непустых подмножеств множества U.□

3. Отношения эквивалентности. *Рефлексивное, симметричное и транзитивное отношение называется*

отношением эквивалентности. Таким образом, $R \subset X \times X$ – отношение эквивалентности на множестве X, если

$$R \supset E_X,\ R^{-1}=R \text{ и } R^2=R.$$

Простейшим примером отношения эквивалентности на множестве X может служить отношение равенства E_X. Для обозначения отношений эквивалентности принято использовать символ ~.

Рассмотрим несколько примеров.

Примеры. 1) Пусть X – множество функций, определенных на всей числовой прямой. Будем считать, что функции f и g связаны отношением ~, если они принимают одинаковые значения в точке 0, то есть $f(x) \sim g(x)$, если $f(0)=g(0)$. Например, $\sin x \sim x$, $e^x \sim \cos x$. Отношение ~ рефлексивно ($f(0)=f(0)$ для любой функции $f(x)$); симметрично (из $f(0)=g(0)$ следует, что $g(0)=f(0)$); транзитивно (если $f(0)=g(0)$ и $g(0)=h(0)$, то $f(0)=h(0)$). Следовательно, ~ является отношением эквивалентности.

2) Пусть ~ – отношение на множестве натуральных чисел, при котором $x \sim y$, если x и y дают одинаковые остатки при делении на 5. Например, 6~11, 2~7, 1~6. Легко видеть, что это отношение рефлексивно, симметрично и транзитивно и, значит, является отношением эквивалентности.□

Следующая теорема описывает в общем виде типичную ситуацию, в которой возникают отношения эквивалентности.

Теорема. *Пусть* φ *– отображение множества* X в *некоторое множество* Y. *Определим отношение* ~ на X,

полагая $x \sim y$, если $\varphi(x)=\varphi(y)$. *Тогда отношение* $\sim$ *является отношением эквивалентности*.

Доказательство. Достаточно заметить, что отношение $\sim$ рефлексивно, поскольку $\varphi(x) = \varphi(x)$ для любого x, симметрично, поскольку $\varphi(x)=\varphi(y)$ влечет $\varphi(y)=\varphi(x)$, и транзитивно, поскольку из $\varphi(x)= \varphi(y)$ и $\varphi(y)=\varphi(z)$ следует, что $\varphi(x)=\varphi(z)$.□

Про отношение эквивалентности, описанное в предыдущей теореме, будем говорить, что оно *порождается отображением* φ. Будем обозначать это отношение эквивалентности через $\sim_\varphi$ или просто через $\sim$, когда ясно, о каком отображении идет речь. Далее мы увидим, что всякое отношение эквивалентности может быть представлено как $\sim_\varphi$ для подходящего отображения.

Теорема применима к обоим рассмотренным перед ней примерам. В первом примере в качестве Y можно взять множество действительных чисел, а отображение φ определить на множестве функций соответствием $\varphi: f \to f(0)$. Во втором примере в качестве $\varphi(x)$ можно взять остаток от деления x на 5.

Отображение φ порождает разбиение множества X на классы, содержащие элементы, имеющие одинаковый образ, то есть эквивалентные относительно $\sim_\varphi$. Описываемая ниже конструкция устанавливает взаимно однозначное соответствие между отношениями эквивалентности на множестве X и его разбиениями в общем случае.

Будем говорить, что дано *разбиение* множества X, если задано семейство его непустых подмножеств, такое, что два различных подмножества из этого семейства не пересекаются, а объединение всех подмножеств есть X.

Всякому разбиению множества X отвечает отношение эквивалентности, задаваемое следующим образом: *$x \sim y$ в том и только том случае, когда x и y содержатся в одном общем подмножестве из разбиения*.

Опишем теперь обратное построение.

Пусть $\sim$ отношение эквивалентности на X. Для произвольного элемента $x \in X$ обозначим через A_x множество всех элементов, эквивалентных x, то есть

$$A_x = \{y \mid y \sim x\}.$$

Множества вида A_x называются *классами эквивалентности*. Так как $x \sim x$, то $x \in A_x$, так что классы эквивалентности непусты, и их объединение дает все множество X. Покажем, что различные классы эквивалентности не пересекаются. Предположим, что $A_x \cap A_y \neq \varnothing$, и покажем, что в этом случае $A_x = A_y$. Пусть $z \in A_x \cap A_y$. Тогда $z \sim x$ *и* $z \sim y$. Так как отношение эквивалентности симметрично, то $y \sim z$. Теперь из $y \sim z$ и $z \sim x$ в силу транзитивности следует $y \sim x$, так что $y \in A_x$. Пусть z – произвольный элемент из A_y. Тогда $z \sim y$. Так как $y \sim x$, отсюда по транзитивности следует , что $z \sim x$, то есть $z \in A_x$. Таким образом, $A_x \subset A_y$. Аналогично $A_y \subset A_x$.

Замечание. Соответствие $x \to A_x$ задает отображение $\varphi: X \to 2^X$ множества X в множество его подмножеств 2^X. При этом $\varphi(x)=\varphi(y)$ тогда и только тогда, когда $A_x=A_y$, то есть когда $x \sim y$. Значит, $\sim = \sim_\varphi$.Таким образом, произвольное отношение эквивалентности на множестве X порождается некоторым отображением.□

4. Натуральные числа

1. Натуральный ряд. Под натуральным рядом понимают последовательность чисел

$$0, 1, 2, 3, \ldots .$$

В современной математике существование натурального ряда является одним из базовых постулатов. Постулируется существование множества $\boldsymbol{N}$, удовлетворяющего определенным условиям – *аксиомам натурального ряда*.

Натуральный ряд – это множество $\boldsymbol{N}$ вместе с отображением непосредственного следования $s: \boldsymbol{N} \to \boldsymbol{N}$, $s(x)=x'$, удовлетворяющие следующим условиям (аксиомам).

1) Множество $\boldsymbol{N}$ содержит элемент, обозначаемый через 0, который не следует ни за каким элементом: $0 \in \boldsymbol{N}$ и $0 \neq x'$ каков бы ни был элемент $x \in \boldsymbol{N}$.

2) Отображение непосредственного следования инъективно: если $x'=y'$, то $x=y$.

3) *Аксиома индукции*: единственное подмножество множества $\boldsymbol{N}$, которое, во-первых, содержит 0 и, во-вторых,

вместе с каждым элементом x содержит непосредственно следующий за ним элемент x', – это само множество $\boldsymbol{N}$.

Из первых двух условий следует, что последовательность

$$0, 0', 0'', 0''' \ldots$$

не содержит повторяющихся элементов. В самом деле, если, например, $0''=0''''$, то, по аксиоме 2, $0'=0'''$ и $0=0''$, что противоречит аксиоме 1. Аксиома индукции говорит о том, что элементами этой последовательности исчерпывается все множество $\boldsymbol{N}$. Таким образом, повторяя отображение s, можно, начав с 0, добраться до произвольного $x \in \boldsymbol{N}$ за конечное число шагов. Используя привычные обозначения $0'=1$, $0''=2$, $0'''=3$, …, получаем

$$\boldsymbol{N} = \{0, 1, 2, 3, \ldots\}.$$

2. Метод математической индукции. Многие математические доказательства основываются на аксиоме индукции, которую можно переформулировать следующим образом.

Принцип полной индукции. Пусть P – утверждение относительно натуральных чисел n такое, что

1) P верно для $n=0$;

2) из справедливости P для $n=k$ следует справедливость P для $n=k+1$.

Тогда P верно для всех натуральных чисел.

Замечание. Чтобы показать, что эта формулировка следует из предыдущей, достаточно рассмотреть множество

$$A=\{x\in \boldsymbol{N} \mid P \text{ верно для } x\}.$$

Для доказательства в обратную сторону, множеству $A\subset \boldsymbol{N}$ можно сопоставить свойство P «быть элементом множества A».□

О доказательствах, основанных на аксиоме индукции, говорят, что они проведены *методом математической индукции*. Такие доказательства имеют следующую структуру:

•устанавливается справедливость P для $n=0$ (*посылка индукции*);

•предполагается, что P справедливо для некоторого произвольного, но фиксированного $n=k$ (*индуктивное предположение*);

•доказывается, что из индуктивного предположения, следует, что P верно для $n=k+1$ (*индуктивный шаг*).

Примеры. Проведем два доказательства методом математической индукции.

1) *Сумма первых натуральных чисел от* 0 *до* n *включительно равна* $0{,}5n(n+1)$:

$$0+1+\ldots+n = 0{,}5n(n+1).$$

Доказательство. Утверждение верно при $n=0$: имеем $0=0{,}5\cdot 0\cdot(0+1)$ (посылка индукции).

Предположим, что доказываемое утверждение верно для $n=k$ (индуктивное предположение), то есть

$$0+1+\ldots+k = 0{,}5k(k+1).$$

Покажем, что тогда оно верно и для $n=k+1$, то есть

$$0+1+\ldots+k+(k+1) = 0{,}5(k+1)(k+2)$$

(индуктивный шаг). Сумма во втором равенстве отличается от суммы из первого равенства слагаемым $k+1$. Поэтому, в силу индуктивного предположения, получаем

$$0+1+\ldots+k+(k+1) = 0{,}5k(k+1)+k+1 = 0{,}5(k+1)(k+2),$$

что и требовалось доказать.

В соответствии с принципом математической индукции, доказываемое утверждение верно для всех n.

2) *Число подмножеств множества, содержащего n элементов, равно* 2^n.

Доказательство. Утверждение верно при $n=0$: пустое множество $\varnothing$ (единственное множество, содержащее 0 элементов) имеет ровно одно подмножество $\varnothing$.

Предположим теперь, что всякое множество с $n=k$ элементами имеет 2^k подмножеств, и покажем , что множество с $n=k+1$ элементами имеет 2^{k+1} подмножеств. Пусть A – произвольное множество с $n=k+1$ элементами. Так как $k+1>0$, то A не пусто и содержит хотя бы один элемент. Пусть $a \in A$. Разобьем совокупность всех подмножеств множества A на два класса. В класс U входят все подмножества, содержащие a, в класс V входят все подмножества, не содержащие a:

$$U=\{X \subset A \mid a \in X\};\ V=\{Y \subset A \mid a \notin Y\}.$$

Положим $A'=A\setminus\{a\}$. Множество A' содержит k элементов, так что по индуктивному предположению, число его подмножеств равно 2^k. Но подмножества множества A' – это в точности подмножества множества A, не содержащие a. Следовательно, $|V|=2^k$. Пара взаимно обратных отображений $U\to V$, $X\to X\setminus\{a\}$ и $V\to U$, $Y\to Y\cup\{a\}$ устанавливает между U и V взаимно однозначное соответствие, так что $|U|=|V|=2^k$. Поэтому общее число подмножеств множества A составляет

$$|U|+|V|=2^k+2^k=2^{k+1},$$

что и требовалось доказать.□

Иногда принцип полной индукции применяется в следующей форме.

Пусть P – утверждение относительно натуральных чисел n такое, что

1) P верно для $n=n_0$;

2) из справедливости $P(n)$ для $n= n_0, n_0+1, \ldots, n_0+k$ следует справедливость $P(n)$ для $n= n_0+k+1$.

Тогда P верно для всех $n\geq n_0$.

Принцип полной индукции в этой форме может быть сведен к предыдущей формулировке заменой утверждения P утверждением P': утверждение P имеет место для всех t, таких, что $n_0\leq t\leq n$.

Возможны и другие модификации принципа полной индукции.

Теорема. Всякое непустое подмножество натурального ряда содержит наименьший элемент.

Доказательство. Пусть $A \subset N$ – непустое подмножество. Возможны два случая: $0 \in A$ и $0 \notin A$. В первом случае 0 является наименьшим элементом множества A. Рассмотрим второй случай. Предположим, что в A нет наименьшего элемента. Пусть A' – это множество всех таких n, что ни одно число t из промежутка от 0 до n не содержится в A. Так как $0 \notin A$, то $0 \in A'$. Далее, если $k \in A'$, то и $k+1 \in A'$. В самом деле, в противном случае мы имели бы $0,1,\ldots,k \notin A$, но $k+1 \in A$ – а это означает, что $k+1$ – наименьший элемент множества A в противоречие с предположением об отсутствии такового. По аксиоме индукции множество A' совпадает с $\boldsymbol{N}$. Но это находится в противоречии с предположением о том, что множество A не пусто.□

1. Логика высказываний

1.1. Высказывания и операции над ними

В математике под высказыванием понимают утверждение, которому может быть приписано *значение истинности*. Обычно используют два значения: «*истина*» и «*ложь*», и говорят соответственно об истинности или ложности высказываний. Например, в арифметике высказывания «$1 \le 2$», «$2 \cdot 2 = 4$» считаются истинными, а высказывание «$0 = 1$» ложным. В геометрии аксиомы считают истинными высказываниями; истинность других высказываний устанавливают, доказывая теоремы. Высказывания и доказательства в математике (и ряде других областей знания) строятся по определенным точно формулируемым правилам. Для описания этих правил, построения и анализа высказываний и доказательств используется математическая логика.

Высказывания будут обозначаться, как правило, большими латинскими буквами, значения истинности – символами 0 (ложь) и 1 (истина). *Значение истинности высказывания* A обозначается через $[A]$. Запись $[A]=1$означает, что высказывание A истинно, а запись $[A]=0$ – что высказывание A ложно.

Рассмотрим логические операции, которые, будучи примененными к одному или двум высказываниям, позволяют получить новые высказывания.

Отрицание. Отрицание высказывания A обозначается через $\overline{A}$ или через $\neg A$; читается «не A». Высказывание $\neg A$ истинно, если A ложно, и ложно, если A истинно. Значение истинности высказывания $\neg A$ определяется формулой

$$[\neg A]=1-[A].$$

Конъюнкция. Конъюнкция высказываний A и B обозначается через $A\wedge B$; читается «A и B». Высказывание $A\wedge B$ истинно, если истинны оба высказывания A и B, и ложно, если ложно хотя бы одно из этих высказываний. Значение истинности высказывания $A\wedge B$ определяется формулой

$$[A\wedge B] = \min\{[A], [B]\}.$$

Дизъюнкция. Дизъюнкция высказываний A и B обозначается через $A\vee B$; читается «A или B». Высказывание $A\vee B$ ложно, если ложны оба высказывания A и B, и истинно, если истинно хотя бы одно из этих высказываний. Значение истинности высказывания $A\vee B$ определяется формулой

$$[A\vee B] = \max\{[A], [B]\}.$$

Импликация. Импликация высказываний A и B обозначается через $A\to B$; читается «если A, то B», «из A следует B». Высказывание $A\to B$ ложно, если высказывание B ложно, а высказывание A истинно; во всех остальных случаях

высказывание $A \to B$ истинно. Высказывание A называют *посылкой* импликации $A \to B$, а высказывание B – *заключением*. Значение истинности высказывания $A \to B$ определяется формулой

$$[A \to B] = \max\{1 - [A], [B]\}.$$

Предыдущие определения можно свести в следующие таблицы:

A	$\neg A$
0	1
1	0

A	B	$A \wedge B$	$A \vee B$	$A \to B$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

Примеры.

$[\neg 2=3]=[2\neq 3] = 1$; $[2<3 \vee 2=3] = [2\leq 3] = 1$;

$[2=2 \wedge 2=3] = 0$; $[2=3 \to 2=2] = 1$;

$[2=2 \to 2=3] = 0$.□

1.2. Формулы логики высказываний

При построении формул логики высказываний мы будем использовать символы логических операций, скобки и символы $X, Y, Z, \ldots$ (быть может, с индексами) для обозначения *переменных высказываний* (высказывательных, или *пропозициональных переменных*). Совокупность этих символов мы будем называть *алфавитом логики высказываний*. Любая конечная последовательность символов алфавита называется

словом. Среди всех слов мы выделяем те, которые построены по определенным правилам, и называем их *формулами логики высказываний*. Запись $(X\wedge(\neg Y))\to Z$ естественно считать формулой, а запись $\wedge(Z\neg Y))\to$ – нет.

Уточним понятие формулы, описав процедуру построения формул.

Во-первых, мы считаем формулой символ любой пропозициональной переменной. Во-вторых, если U и V – формулы, то $(\neg U)$, $(U\wedge V)$, $(U\vee V)$, $(U\to V)$ – также формулы. Слово в алфавите логики высказываний считается формулой, если оно получено в соответствии с этим правилами.

Часть формулы, которая сама является формулой, называется *подформулой*. Так, формула U является подформулой формулы $(\neg U)$, а формулы U и V – подформулами формул $(U\wedge V)$, $(U\vee V)$, $(U\to V)$. Мы будем называть формулу *булевой*, если в ее записи не используется импликация.

Для упрощения записи условимся опускать в формулах внешние скобки. Далее будем считать, что отрицание «выполняется» раньше остальных операций, и опускать скобки, если отрицание относится к кратчайшей, стоящей за ним подформуле. Часто мы будем записывать отрицание с помощью горизонтальной черты над подформулой, к которой оно относится. Мы будем иногда опускать знак конъюнкции и вместо $U\wedge V$ писать просто UV. Наконец, мы будем считать, что конъюнкция выполняется раньше, чем дизъюнкция (подобно

тому, как в арифметических выражениях умножение выполняется раньше, чем сложение), и опускать скобки, которые могут быть с учетом этого восстановлены. Например, формула

$$((((\neg(X))\wedge(Y))\vee((X)\wedge(\neg(Y))))$$

может быть коротко записана в виде

$$\overline{X}\,Y\vee X\overline{Y}\,.$$

Чтобы указать, что в записи формулы U участвуют пропозициональные переменные X, Y, …, Z (а никаких других нет), мы будем писать $U=U(X,Y,\ldots,Z)$.

Формула превращается в высказывание, если в ней каждую пропозициональную переменную заменить некоторым высказыванием. Так, подставив в формулу

$$U(X,Y)=\overline{X}\,Y\vee X\overline{Y}$$

высказывание A:(1=2) вместо X и высказывание B:(3>2) вместо Y, получим высказывание

$$U(A,B)=(1\neq 2)(3>2)\vee(1=2)(3\leq 2).$$

Несложно посчитать значение истинности полученного высказывания: $[U(A,B)]=1$. Ясно, что значение истинности высказывания $U(A,B)$ зависит не от самих высказываний A и B, а лишь от их значений истинности. Каковы бы ни были высказывания A и B, если только $[A]=0$, а $[B]=1$, мы получим $[U(A,B)]=1$. Составим таблицу, в которой вычисляется значение истинности высказывания, полученного при замене в формуле

U переменных X и Y высказываниями, в зависимости от значений истинности этих высказываний.

X	Y	$\overline{X}$	$\overline{Y}$	$\overline{X}Y$	$X\overline{Y}$	$\overline{X}Y \vee X\overline{Y}$
0	0	1	1	0	0	0
0	1	1	0	1	0	1
1	0	0	1	0	1	1
1	1	0	0	0	0	0

Подобные таблицы называются *таблицами истинности*.

Назовем *оценкой списка переменных* формулы $U=U(X,Y,\ldots,Z)$ сопоставление каждой переменной некоторого истинностного значения. Допуская некоторую вольность речи, можно сказать, что каждой оценке переменных соответствует значение истинности формулы U.

Пример. Составим таблицу истинности для формулы $X\to(Y\to Z)$.

X	Y	Z	$Y\to Z$	$X\to(Y\to Z)$
0	0	0	1	1
0	0	1	1	1
0	1	0	0	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

□

1.3. Равносильность формул

Формулы $U=U(X,Y,\ldots,Z)$ и $V=V(X,Y,\ldots,Z)$ называются *равносильными*, если они принимают одинаковые значения для любой оценки переменных $X,Y,\ldots,Z$.

Если для формул U и V построены таблицы истинности, то равносильность означает, что итоговые столбцы в этих таблицах совпадают. Равносильность формул U и V будем обозначать через $U\cong V$. Легко заметить, что отношение равносильности рефлексивно, симметрично и транзитивно и, значит, является отношением эквивалентности. Каждый класс эквивалентности состоит из равносильных между собой формул.

Теорема (основные равносильности). *Имеют место следующие равносильности.*

Коммутативность конъюнкции и дизъюнкции:

$X\wedge Y\cong Y\wedge X$; $X\vee Y\cong Y\vee X$.

Ассоциативность конъюнкции и дизъюнкции:

$(X\wedge Y)\wedge Z\cong X\wedge(Y\wedge Z)$; $(X\vee Y)\vee Z\cong X\vee(Y\vee Z)$.

Идемпотентность конъюнкции и дизъюнкции:

$X\wedge X\cong X$; $X\vee X\cong X$.

Дистрибутивность конъюнкции и дизъюнкции друг относительно друга:

$$X\wedge(Y\vee Z)\cong(X\wedge Y)\vee(X\wedge Z);\quad X\vee(Y\wedge Z)\cong(X\vee Y)\wedge(X\vee Z).$$

Законы поглощения:

$$X\wedge(X\vee Y)\cong X; \qquad X\vee(X\wedge Y)\cong X.$$

Снятие двойного отрицания:

$$\neg\neg X\cong X.$$

Законы де Моргана:

$$\neg(X\wedge Y)\cong\neg X\vee\neg Y; \qquad \neg(X\vee Y)\cong\neg X\wedge\neg Y.$$

Законы расщепления:

$$(X\wedge Y)\vee(X\wedge\neg Y)\cong X; \quad (X\vee Y)\wedge(X\vee\neg Y)\cong X.$$

Устранение импликации:

$$X\to Y\cong\neg X\vee Y.$$

□

Любая из перечисленных равносильностей легко может быть доказана с помощью таблиц истинности. Используя основные равносильности, удобно записывать последовательность равносильных преобразований формулы в виде цепочки. Например:

$$X\to(Y\to Z)\cong X\to(\neg Y\vee Z)\cong\neg X\vee(\neg Y\vee Z)\cong(\neg X\vee\neg Y)\vee Z\cong$$

$$\cong(\neg Y\vee\neg X)\vee Z\cong\neg Y\vee(\neg X\vee Z)\cong Y\to(\neg X\vee Z)\cong Y\to(X\to Z).$$

При записи равносильных преобразований удобно использовать и некоторые другие равносильности. Например, покажем, что

$$X\vee(\neg YY)\cong X.$$

Последовательно применяя законы дистрибутивности и расщепления, получаем:

$$X\vee(\neg YY) \cong (X\vee\neg Y)(X\vee Y) \cong X.$$

Аналогично

$$X(\neg Y\vee Y) \cong X.$$

Сформулируем еще несколько правил, которые позволяют получать равносильные формулы без непосредственной проверки по таблицам истинности.

Если в равносильных формулах пропозициональные переменные заменить формулами (одинаковые переменные одинаковыми формулами) получатся равносильные формулы.

Если формулы U и *V равносильны*, *U≅V, а W – произвольная формула, то имеют место следующие равносильности:*

$$\neg U\cong\neg V;\quad U\wedge W\cong V\wedge W;\qquad U\vee W\cong V\vee W;$$

$$U\to W\cong V\to W;\quad W\to U\cong W\to V.$$

Используя устранение импликации, любую формулу можно с помощью равносильных преобразований привести к булевой формуле.

1.4. Принцип двойственности

Пусть $U=U(X,Y,\ldots,Z)$ – формула алгебры высказываний. Формула

$$U^* = \neg U(\neg X,\neg Y,\ldots,\neg Z)$$

называется *двойственной* к формуле *U*.

Из закона двойного отрицания следует, что $(U^*)^*\cong U$. Между таблицами истинности исходной формулы и двойственной к

ней имеется простая связь. Предположим для определенности, что формула U содержит две переменных, $U=U(X,Y)$, и рассмотрим следующую таблицу истинности:

X	Y	U	U^*
0	0	α	$\neg\delta$
0	1	β	$\neg\gamma$
1	0	γ	$\neg\beta$
1	1	δ	$\neg\alpha$

Несложно заметить, что столбец значений формулы U^* представляет собой перевернутый столбец значений формулы U, снабженных отрицанием. То же справедливо и для формул, содержащих большее число пропозициональных переменных. Из этого замечания вытекает следующее утверждение.

Закон двойственности. *Формулы алгебры высказываний равносильны тогда и только тогда, когда равносильны двойственные им формулы: $U\cong V$ тогда и только тогда, когда $U^*\cong V^*$.*□

Для булевых формул закон двойственности приобретает особенно наглядную форму.

Теорема. *Если формула U булева, то двойственная формула U^* равносильна формуле $U^{\wedge\vee}$, полученной из U заменой всех конъюнкций на дизъюнкции, а дизъюнкций на конъюнкции.*

Доказательство. Воспользуемся индукцией по длине формулы. Предположим сначала, что формула U состоит всего

из одного символа. Это означает, что формула имеет вид $U=X$, где X – некоторая пропозициональная переменная. Ясно, что для такой формулы $U^*\cong U$ и $U^{\wedge\vee}=U$, так что утверждение теоремы справедливо. Предположим теперь, что утверждение теоремы справедливо для всех формул длины меньше n и покажем, что оно справедливо и для произвольной формулы $U=U(X,\ldots,Y)$ длины n. В соответствии с определением формула U имеет вид

$$\text{а) } U=\neg V;\ \text{б) } U=V\wedge W \text{ или в) } U=V\vee W,$$

где V и W – некоторые формулы. Ясно, что в любом случае формула U содержит по крайней мере на один знак больше, чем формулы V и W. Значит, длина V меньше n, и длина W меньше n. Поэтому к формулам V и W применимо заключение теоремы, то есть

$$V^*\cong V^{\wedge\vee} \text{ и } W^*\cong W^{\wedge\vee}.$$

С учетом этого рассмотрим каждый из трех возможных случаев.

а) $U^* = \neg(\neg V(\neg X,\ldots,\neg Y)) = \neg V^*$, $U^{\wedge\vee} = \neg V^{\wedge\vee}$, откуда $U^*\cong U^{\wedge\vee}$.

б) $U^* = \neg(V(\neg X,\ldots,\neg Y) \wedge W(\neg X,\ldots,\neg Y))$, откуда по первой формуле де Моргана $U^* \cong \neg V(\neg X,\ldots,\neg Y)\vee\neg W(\neg X,\ldots,\neg Y))\cong V^*\vee W^*$. С другой стороны, $U^{\wedge\vee} = V^{\wedge\vee}\wedge W^{\wedge\vee}$, и, значит, $U^*\cong U^{\wedge\vee}$.

в) $U^* = \neg(V(\neg X,\ldots,\neg Y) \vee W(\neg X,\ldots,\neg Y))$, откуда по второй формуле де Моргана $U^* \cong \neg V(\neg X,\ldots,\neg Y)\vee\neg W(\neg X,\ldots,\neg Y))\cong V^*\wedge W^*$. С другой стороны, $U^{\wedge\vee} = V^{\wedge\vee}\vee W^{\wedge\vee}$, и, значит, $U^*\cong U^{\wedge\vee}$.

В соответствии с принципом математической индукции утверждение теоремы верно для формул любой длины, то есть для всех формул.□

Обычно закон двойственности применяют к булевым формулам и в этом случае называют двойственной к формуле U формулу $U^{\wedge\vee}$. Следуя этой традиции, мы тем не менее сохраним за двойственной формулой обозначение U^*.

В списке основных равносильностей идущие парами равносильности получаются друг из друга по закону двойственности (или, короче, по двойственности).

Пример. Формулы $X(\neg Y \vee Y)$ и $X \vee (\neg YY)$ двойственны, поэтому равносильность

$$X(\neg Y \vee Y) \cong X$$

получается из равносильности

$$X \vee (\neg YY) \cong X$$

по двойственности.□

1.5. Тождественно истинные формулы

Один класс равносильных логических формул играет особенно важную роль. Это класс формул, которые принимают значение 1 при любой оценке их переменных. Такие формулы называют *тождественно истинными*.

Примеры. Формулы

$$X \vee \neg X, \qquad \neg(X \wedge \neg X),$$

$$(X\wedge(X\to Y))\to Y,$$

$$((\neg X\to Y)\wedge(\neg X\to\neg Y))\to X$$

тождественно истинны. В этом несложно убедиться, построив таблицы истинности.□

Тождественно истинные формулы остаются истинными независимо от того, какими высказываниями заменены входящие в них переменные. Они соответствуют, в определенном смысле, некоторым универсальным логическим законам. Так, первая формула из предыдущего примера выражает так называемый *закон исключенного третьего*: из двух противоположных утверждений хотя бы одно истинно, Вторая формула– *закон противоречия*: два противоположных утверждения не могут быть истинными одновременно. Третья формула представляет собой *правило заключения*: из истинности посылки и импликации вытекает истинность заключения. Четвертая формула соответствует принципу *доказательства от противного*: утверждение верно, если из его отрицания следует одновременно некоторое заключение вместе со своим отрицанием.

Обычно логическое рассуждение проводится по следующей схеме: если верны посылки U_1, U_2, …, U_n, то верно заключение V. Чтобы проверить правильность рассуждения, достаточно установить тождественную истинность формулы $(U_1\wedge U_2\wedge\ldots\wedge U_n)\to V$. Например, логическая схема «из $X\to Y$

следует $Y \to X$» (вместе с любым заключением верно и обратное к нему) является неверной. В этом можно убедиться, проверив, что формула $(X \to Y) \to (Y \to X)$ не тождественно истинна.

1.6. Система натурального вывода

Основываясь на применяемых в математике способах рассуждения, можно сформулировать так называемые *правила естественного вывода*. Обычно логическое рассуждение имеет вид

Γ влечет U (или из Γ следует U),

где U – формула (утверждение), а Γ – некоторое множество формул (утверждений). Рассуждение такого вида мы будем представлять записью $\Gamma \Rightarrow U$ (не приписывая пока знаку $\Rightarrow$ какого бы то ни было смысла). Элементы множества Γ будем называть гипотезами, U – заключением. Правила вывода устанавливают, как от одних рассуждений можно переходить к другим, основываясь только на их логической форме.

Прежде чем сформулировать правила, условимся об обозначениях. Далее Γ будет обозначать некоторое множество формул. Если U – формула, вместо $\{U\}$ будем писать просто U; вместо $\Gamma \cup \{U\}$ будем писать Γ, U. Правила мы будем записывать в виде двухэтажных выражений: над чертой (в «числителе») – исходные рассуждения, под чертой (в «знаменателе») – рассуждение, к которому от них можно перейти.

Следующие два *базисных правила* формализуют принцип монотонности рассуждений:

$$\frac{\varnothing}{\Gamma, U \Rightarrow U}$$

$$\frac{\Gamma \Rightarrow U}{\Gamma, V \Rightarrow U}$$

Содержательно их можно понимать так: первое – всегда допустимо (выводится из «ничего») рассуждение, в котором заключение является одной из гипотез; второе – если некоторый набор гипотез позволяет прийти к некоторому заключению, то и более широкий набор гипотез позволяет прийти к тому же заключению.

Теперь выпишем *правила введения логических связок*:

$$\frac{\Gamma \Rightarrow U; \Gamma \Rightarrow V}{\Gamma \Rightarrow U \wedge V}$$

$$\frac{\Gamma \Rightarrow U}{\Gamma \Rightarrow U \vee V}$$

$$\frac{\Gamma \Rightarrow V}{\Gamma \Rightarrow U \vee V}$$

$$\frac{\Gamma, U \Rightarrow V}{\Gamma \Rightarrow U \rightarrow V}$$

$$\frac{\Gamma, U \Rightarrow V;\ \Gamma, U \Rightarrow \neg V}{\Gamma \Rightarrow \neg U}$$

Наконец, приведем *правила удаления логических связок*:

$$\frac{\Gamma \Rightarrow U \wedge V}{\Gamma \Rightarrow U}$$

$$\frac{\Gamma \Rightarrow U \wedge V}{\Gamma \Rightarrow V}$$

$$\frac{\Gamma \Rightarrow U \vee V;\ \Gamma, U \Rightarrow W;\ \Gamma, V \Rightarrow W}{\Gamma \Rightarrow W}$$

$$\frac{\Gamma \Rightarrow U \rightarrow V}{\Gamma, U \Rightarrow V}$$

$$\frac{\Gamma \Rightarrow U;\ \Gamma \Rightarrow \neg U}{\Gamma \Rightarrow V}$$

$$\frac{\Gamma \Rightarrow \neg\neg U}{\Gamma \Rightarrow U}$$

Перечисленные правила составляют *систему натурального вывода*. Рассуждение выводимо в системе натурального вывода, если его можно получить из «ничего» (пустого рассуждения), применяя конечное число подходящих правил.

Будем говорить, что формула логики высказываний U *логически следует* из гипотез Γ, если формула U принимает значение «истина» для любой оценки переменных, для которой значение «истина» принимают все формулы из Γ. Правила натурального вывода согласуются с логическим следованием. Если понимать $\Rightarrow$ как логическое следование, то верный «числитель» приводит к верному «знаменателю». Более того, система правил натурального вывода полна: если U логически следует из Γ, к этому можно прийти с помощью натурального вывода.

Пример. Приведем обоснование в системе натурального вывода метода доказательства разбором случаев:

из U, $U \to V_1 \vee V_2$, $V_1 \to W$, $V_2 \to W$ *логически следует* W

Доказательство. Обозначим для краткости набор гипотез через Γ. Имеем:

(1) $\Gamma, U \to V_1 \vee V_2 \Rightarrow U \to V_1 \vee V_2$	базисное правило
(2) $\Gamma \Rightarrow U \to V_1 \vee V_2$	базисное правило
(3) $\Gamma, U \Rightarrow V_1 \vee V_2$	(2), удаление $\to$
(4) $\Gamma \Rightarrow V_1 \vee V_2$	базисное правило
(5) $\Gamma, V_1 \to W \Rightarrow V_1 \to W$	базисное правило
(6) $\Gamma \Rightarrow V_1 \to W$	базисное правило
(7) $\Gamma, V_1 \Rightarrow W$	(6), удаление $\to$
(8) $\Gamma, V_2 \to W \Rightarrow V_2 \to W$	базисное правило
(9) $\Gamma \Rightarrow V_2 \to W$	

(10) $\Gamma, V_2 \Rightarrow W$ (9), удаление $\rightarrow$

(11) $\Gamma \Rightarrow W$ (4), (7), (10), удаление $\vee$□

1.7. Принцип резолюций

Будем говорить, что множество формул логики высказываний Γ *выполнимо*, если существует такая оценка переменных, входящих в формулы из Γ, при которой все формулы из Γ принимают значение «истина»; в противном случае будем говорить, что множество формул Γ *невыполнимо.*

Формула логики высказываний называется *элементарной дизъюнкцией* (*дизъюнктом*), если она представляет собой дизъюнкцию нескольких пропозициональных переменных и/или их отрицаний. Например, $\neg X \vee Y$, $X \vee Y \vee \neg Z$, X, $\neg X$ дизъюнкты. Любой дизъюнкт, содержащий хотя бы одну переменную, выполним. *Пустой дизъюнкт* (обозначим его через Λ) – единственный невыполнимый дизъюнкт. *Конъюнктивной нормальной формой* (*КНФ*) называется конъюнкция конечного числа дизъюнктов.

Для любой формулы логики высказываний можно получить равносильную ей КНФ с помощью следующего алгоритма:

– сначала из формулы исключаются все импликации (используется равносильность $U \rightarrow V \cong \neg U \vee V$);

– необходимое число раз применяются законы де Моргана до тех пор, пока отрицания не будут относиться только к

пропозициональным переменным; при этом снимаются двойные отрицания;

– необходимое число раз по дистрибутивности раскрываются скобки; дизъюнкты, содержащие переменную вместе с ее отрицанием, тождественно истинны и могут быть опущены; могут быть также сокращены повторы переменных в дизъюнктах.

Пример. Приведем к КНФ формулу

$$(X \to Y) \to (Z \to (X \wedge Y)).$$

Имеем

$$(X \to Y) \to (Z \to (X \wedge Y)) \cong \neg(\neg X \vee Y) \vee (\neg Z \vee (X \wedge Y)) \cong$$

$$\cong (\neg\neg X \wedge \neg Y) \vee (\neg Z \vee (X \wedge Y)) \cong (X \wedge \neg Y) \vee (\neg Z \vee (X \wedge Y)) \cong$$

$$\cong (X \wedge \neg Y) \vee ((\neg Z \vee X) \wedge (\neg Z \vee Y)) \cong$$

$$\cong (X \vee \neg Z \vee X) \wedge (\neg Y \vee \neg Z \vee X) \wedge (X \vee \neg Z \vee Y) \wedge (\neg Y \vee \neg Z \vee Y) \cong$$

$$\cong (X \vee \neg Z) \wedge (X \vee \neg Y \vee \neg Z) \wedge (X \vee Y \vee \neg Z). \square$$

Двойственным образом определяются *дизъюнктивные нормальные формы*. Элементарной конъюнкцией называется конъюнкция нескольких пропозициональных переменных и/или их отрицаний. Дизъюнктивной нормальной формой (ДНФ) называется дизъюнкция конечного числа элементарных конъюнкций.

Следующее правило называется *правилом резолюций*.

Пусть U и V дизъюнкты, а X – пропозициональная переменная. Тогда из формул $X \vee U$ и $\neg X \vee V$ логически следует формула $U \vee V$.

Дизъюнкт $U \vee V$ называется *резольвентой* дизъюнктов $X \vee U$ и $\neg X \vee V$.

На правиле резолюций основывается метод доказательства невыполнимости набора дизъюнктов Γ (*метод резолюций*):

последовательно составляется список дизъюнктов, в котором каждый из дизъюнктов либо входит в набор Γ, *либо является резолюцией выписанных ранее дизъюнктов*; *появление в списке пустого дизъюнкта свидетельствует о невыполнимости множества формул* Γ.

Пример. Покажем, используя метод резолюций, что из формул $X \vee Y$, $X \vee Z$, $\neg Y \vee \neg Z$ логически следует X. Доказываемое утверждение равносильно невыполнимости набора формул

$$X \vee Y,\ X \vee Z,\ \neg Y \vee \neg Z,\ \neg X.$$

Составим соответствующий список дизъюнктов (около резолюций в скобках указаны номера дизъюнктов, из которых они получены):

(1) $X \vee Y$; (2) $X \vee Z$; (3) $\neg Y \vee \neg Z$; (4) $\neg X$;

(5) Y (1,4); (6) Z (2,4); (7) $\neg Y$ (3,6); (8) Λ (5,7).□

Без доказательства приведем следующую теорему.

Теорема. *Пусть* Γ *– множество дизъюнктов (возможно, бесконечное и содержащее бесконечное множество*

пропозициональных переменных). Если множество Г невыполнимо, это может быть установлено методом резолюций: существует конечная последовательность дизъюнктов, заканчивающаяся пустым дизъюнктом, в которой каждый дизъюнкт либо содержится в Г, либо получен из предыдущих по правилу резолюций.□

2. Логика предикатов

2.1. Понятие предиката

Наряду с высказываниями в математике приходится иметь дело с высказывательными формами, которые превращаются в высказывания при замене в них переменных именами предметов. Например, записи $x>5$ нельзя приписать значение истинности, пока вместо x не подставлено число. Подставив вместо x число 7, мы получим истинное высказывание, подставив 3 – ложное. Подобные высказывательные формы называют *предикатами*. Дадим более точное определение.

Будем говорить, что на множестве X задан *предикат* $P(x_1,x_2,\ldots,x_n)$ от переменных $x_1, x_2, \ldots, x_n$, если каждому набору значений этих переменных из множества X поставлено в соответствие значение истинности: 1 (истина) или 0 (ложь). Предикаты от одной переменной называют одноместными; от двух переменных – двухместными и т.д. Вообще, n-местный предикат можно рассматривать как отображение X^n в $\{0,1\}$.

Для обозначения предикатов используются заглавные латинские буквы, дополненные списком переменных, от которых зависит предикат. Переменные в предикатах называют *предметными*, а множество, в котором они принимают значения, называют иногда *предметной областью*. Например, $P(x,y)$ – предикат P, зависящий от предметных переменных x и

y. Для обозначения высказываний, которые получаются после замены переменных конкретными значениями, используются стандартные функциональные обозначения, например $P(2,3)$ и т.п. Некоторые предикаты, часто используемые в математической практике, имеют свои специфические обозначения. Например, $x=y$, $x>y$ – предикаты от двух переменных.

Высказывания можно трактовать как *нульместные* предикаты, то есть постоянные предикаты, не зависящие от переменных.

Одноместный предикат $P(x)$ на множестве X может трактоваться как *свойство*. Предмет x обладает свойством P, если $P(x)$ истинно, и не обладает свойством P, если $P(x)$ ложно.

Двухместный предикат $P(x,y)$ на множестве $X\times Y$ может трактоваться как *соответствие*. Предмет y соответствует предмету x в том и только том случае, когда $P(x,y)$ истинно. При $X=Y$ предикат $P(x,y)$ может трактоваться как *бинарное отношение*: предметы x и y находятся в отношении P, если истинно $P(x,y)$.

Пусть P – n-местный предикат на множестве X. Обозначим через D_P множество всех тех наборов из X^n, для которых этот предикат истинен. Множество $D_P \subset X^n$ называется *областью истинности предиката P*.

Пример. Уравнение или неравенство с одной неизвестной величиной является предикатом на своей области определения.

Область истинности такого предиката – множество решений. Например, неравенство $P(x)$: $\lg x>3$ – это одноместный предикат на множестве положительных действительных чисел; $D_P = (1000; +\infty)$.□

Одноместные предикаты можно в некотором смысле отождествить с характеристическими функциями. Пусть X – произвольное множество, и $A \subset X$ – некоторое его подмножество. Областью истинности одноместного предиката $x \in A$ на множестве X является A. Так что значения истинности предиката $x \in A$ совпадают со значениями характеристической функции подмножества A. Обратно, всякий одноместный предикат P на множестве X принимает те же значения, что и предикат $x \in D_P$.

Иногда бывает удобно считать, что предметные переменные принимают свои значения в разных множествах. Например, для предиката $P(x,l)$: «точка x лежит на прямой l», – удобно считать, что переменная x пробегает множество точек X, а переменная l – множество прямых L. В такой ситуации говорят, что предикат P определен на $X \times L$ и рассматривают его как отображение множества $X \times L$ в $\{0,1\}$.

Предикат $P(x_1,x_2,\ldots,x_n)$ на множестве X называется:

а) *тождественно истинным* (*ложным*), если он принимает значение «истина» («ложь») для любого набора значений его предметных переменных;

б) *выполнимым* (*опровержимым*), если существует хотя бы один набор значений предметных переменных, для которого предикат P принимает значение «истина» («ложь»).

Пример. Предикат $x^2+y^2\geq 0$ тождественно истинен на множестве действительных чисел; предикат $x^2+y^2<0$ – тождественно ложен; предикат $x^2+y^2>0$ – одновременно выполним и опровержим.□

Непосредственно из определений вытекает справедливость следующих утверждений.

Предикат $P(x_1,x_2,\ldots,x_n)$ *на множестве* X *тождественно истинен (ложен) тогда и только тогда, когда* $D_P=X^n$ (*соотв.* $D_P=\varnothing$).

Предикат $P(x_1,x_2,\ldots,x_n)$ *на множестве* X *выполним (опровержим) тогда и только тогда, когда* $D_P\neq\varnothing$ (*соотв.* $D_P\neq X^n$).

2.2. Логические операции над предикатами

Операции отрицания, конъюнкции, дизъюнкции, импликации естественным образом распространяются на предикаты.

Отрицание. Отрицанием предиката P называется предикат, который определен на том же множестве, что и P, и принимает значение «ложь», когда P истинен, и значение «истина», когда P ложен. Отрицание предиката P обозначается через $\neg P$ или

через $\overline{P}$. Областью истинности предиката $\neg P$ служит дополнение области истинности предиката P:

$$D_{(\neg P)}=\overline{D_P}\,.$$

Пример. Отрицанием одноместного предиката P: $x>5$, определенного на множестве действительных чисел, служит предикат $\neg P$: $x\le 5$. Области истинности этих двух предикатов суть

$$D_P=(5;+\infty) \text{ и } D_{(\neg P)}=(-\infty;5].\square$$

Отрицание тождественно истинного предиката тождественно ложно, и обратно.

Конъюнкция.

Пусть $P(x_1,x_2,\ldots,x_n)$ – n-местный предикат, определенный на $X_1\times\ldots\times X_n$, а $Q(y_1,y_2,\ldots,y_m)$ – m-местный предикат, определенный на $Y_1\times\ldots\times Y_m$. Конъюнкцией предикатов P и Q, называется $(n+m)$-местный предикат, который определен на множестве $X_1\times\ldots\times X_n\times Y_1\times\ldots\times Y_m$ и истинен в том и только том случае, когда истинны оба предиката P и Q. Конъюнкция предикатов P и Q обозначается через $P\wedge Q$. Более точно:

$$(P\wedge Q)(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n)=P(x_1,x_2,\ldots,x_n)\wedge Q(y_1,y_2,\ldots,y_n).$$

Операцию конъюнкции можно применять к предикатам, имеющим общие переменные (пусть их число равно k). В этом случае число переменных в предикате $P\wedge Q$ равно $n+m-k$. Например, конъюнкцией предикатов $P(x,y)$ и $Q(y,z)$ является трехместный предикат $P(x,y)\wedge Q(y,z)$.

В частности, предикаты P и Q могут быть определены для одних и тех же переменных. В этом случае областью истинности предиката $P \wedge Q$ служит пересечение областей истинности предикатов P и Q:

$$D_{P \wedge Q} = D_P \cap D_Q.$$

Пример. Пусть P и Q – двухместные предикаты на множестве действительных чисел, определенные уравнениями:

$$P: x+y=3; \quad Q: x-y=1.$$

Тогда конъюнкция $P \wedge Q$ – это система двух уравнений. Ясно, что $D_{P \wedge Q} = \{(2;1)\}$. Область истинности предиката $P \wedge Q$ представляет собой точку пересечения прямых, определенных уравнениями $x+y=3$, $x-y=1$, которые, в свою очередь, служат областями истинности предикатов P и Q.□

Дизъюнкция.

Определение дизъюнкции аналогично определению конъюнкции. Дизъюнкцией n-местного предиката $P(x_1,x_2,\ldots,x_n)$ и m-местного предиката $Q(y_1,y_2,\ldots,y_m)$ называется $(n+m)$-местный предикат, определенный формулой

$$(P \vee Q)(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_m)=P(x_1,x_2,\ldots,x_n) \vee Q(y_1,y_2,\ldots,y_m).$$

Операцию дизъюнкции можно применять к предикатам, имеющим общие переменные. В частности, если предикаты P и Q определены для одних и тех же переменных, областью истинности предиката $P \vee Q$ служит объединение областей истинности предикатов P и Q:

$$D_{P\vee Q} = D_P \cup D_Q.$$

Примеры. Одноместный предикат S, определенный на множестве действительных чисел неравенством $x^2+5x+6>0$, является дизъюнкцией предикатов P: $x< -3$ и Q: $x> -2$. Имеем:

$$D_P = (-\infty; -3);\ D_Q = (-2;+\infty);$$

$$D_S = D_P \cup D_Q = (-\infty; -3) \cup (-2;+\infty).$$

Двухместный предикат $x\le y$ является дизъюнкцией предикатов $x<y$ и $x=y$.□

Импликация.

Импликацией от n-местного предиката $P(x_1,x_2,\ldots,x_n)$ к m-местному предикату $Q(y_1,y_2,\ldots,y_m)$ называется $(n+m)$-местный предикат, определенный формулой

$$(P\to Q)(x_1,x_2,\ldots,x_n,y_1,y_2,\ldots,y_n)=P(x_1,x_2,\ldots,x_n)\to Q(y_1,y_2,\ldots,y_m).$$

Импликация $P\to Q$ тождественно истинна в том и только том случае, если Q принимает значение «истина» всякий раз, когда значение «истина» принимает P.

Для предикатов, определенных для одних и тех же переменных, тождественная истинность импликации $P\to Q$ означает, что $D_P\subset D_Q$.

Если импликация $P\to Q$ тождественно истинна, говорят, что предикат Q является *следствием* предиката P. В этом случае мы будем писать $P\Rightarrow Q$. Если $P\Rightarrow Q$ и $Q\Rightarrow P$, предикаты P и Q называются *равносильными*. Для равносильных предикатов мы будем писать $P\Leftrightarrow Q$.

Пример. На множестве действительных чисел имеем:

$$x>2 \Rightarrow x^2>4;\ x>2 \Leftrightarrow (x^2>4 \wedge x>0).$$

Свойства логических операций, сформулированные для высказываний, переносятся на операции с предикатами. Например,

$$(P \to Q) \Leftrightarrow (\neg Q \to \neg P);\ \neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q),$$

и т. п.

2.3. Кванторы

Квантор существования.

Всякому одноместному предикату $P(x)$ на множестве X поставим в соответствие высказывание, обозначаемое через $\exists x P(x)$ (читается «существует x такой, что $P(x)$»). Высказывание $\exists x P(x)$ истинно, если область истинности предиката P не пуста, и ложно в противном случае. Таким образом, $\exists x P(x)$ истинно, если в множестве X найдется хотя бы один элемент a, для которого $P(a)$ истинно. Знак $\exists$ называется квантором существования. Про переменную x в высказывании $\exists x P(x)$ говорят, что она связана квантором существования.

Примеры. Высказывания

$$\exists x(x^2+1=0),\ \exists x(2^x<0)$$

ложны; высказывания

$$\exists x(x^2+5x+6=0),\ \exists x(2^x>1000)$$

истинны (мы считаем уравнения и неравенства предикатами на множестве действительных чисел).□

Кванторы существования применяются не только к одноместным предикатам. Например, пусть $P(x,y)$ – двухместный предикат на множестве X. Зафиксируем значение $y=b$. Тогда, считая $P(x,b)$ одноместным предикатом от переменной x, можно составить высказывание $\exists x P(x,b)$. Сопоставляя каждому b значение истинности этого высказывания, мы получаем одноместный предикат, зависящий от переменной y. Этот предикат обозначается через $\exists x P(x,y)$. В этом предикате переменная x считается связанной, а переменная y – свободной. Аналогично определяется $\exists y P(x,y)$. Подобные определения можно распространить и на предикаты большего числа переменных.

Пример. Рассмотрим на множестве действительных чисел трехместный предикат

$$x^2+px+q=0.$$

Предикат

$$\exists x\,(x^2+px+q=0)$$

двухместный, он зависит от переменных p и q. Значения p и q, при которых уравнение имеет решения, превращают его в истинное высказывание. Этот предикат равносилен предикату $p^2-4q\geq 0$, так что можно записать

$$\exists x\,(x^2+px+q=0) \Leftrightarrow p^2-4q\geq 0.\square$$

Квантор общности.

Всякому одноместному предикату $P(x)$ на множестве X поставим в соответствие высказывание, обозначаемое через $\forall x P(x)$ (читается «для любого x $P(x)$»). Высказывание $\forall x P(x)$ истинно, если область истинности предиката P совпадает с множеством X, и ложно в противном случае. Таким образом, $\forall x P(x)$ истинно, если $P(a)$ истинно для всех элементов a из множества X. Знак $\forall$ называется квантором общности. Про переменную x в высказывании $\forall x P(x)$ говорят, что она связана квантором общности.

Примеры. Относительно действительных чисел высказывания

$$\forall x\,(x^2+1>0), \qquad \forall x\,(x^2-1=(x-1)(x+1))$$

истинны; высказывания

$$\forall x\,(x^2+5x+6=0), \qquad \forall x\,(2^x>1000)$$

ложны.□

Так же, как и кванторы существования, кванторы общности применяются не только к одноместным предикатам. Например, пусть $P(x,y)$ – двухместный предикат на множестве X. Тогда $\forall x P(x,y)$ – это одноместный предикат. Он принимает значение «истина» для $y=b$, если истинно высказывание $\forall x P(x,b)$.

Применяя к предикату $P(x,y)$ кванторы в разном порядке, можно получить следующие высказывания:

$$\forall x \forall y P(x,y),\ \forall y \forall x P(x,y),\ \forall x \exists y P(x,y),\ \forall y \exists x P(x,y),$$

$$\exists x\exists Py(x,y),\ \exists y\exists xP(x,y),\ \exists x\forall yP(x,y),\ \exists y\forall xP(x,y).$$

Первые два высказывания в каждой строчке имеют одинаковые значения истинности:

$$[\forall x\forall yP(x,y)] = [\forall y\forall xP(x,y)], \quad [\exists x\exists yPy(x,y)] = [\exists y\exists xP(x,y)].$$

Значения истинности высказываний $\forall x\exists yP(x,y)$ и $\exists y\forall xP(x,y)$ (так же, как и высказываний в оставшейся паре), вообще говоря, различны.

Пример. Для предиката $y>x^2$ на множестве действительных чисел имеем:

$$[\forall x\forall y\ y>x^2]=0;\ [\exists x\exists y\ y>x^2]=1;$$

$$[\forall x\exists y\ y>x^2]=1;\ [\exists y\forall x\ y>x^2]=0.\square$$

Пусть $P(x)$ – произвольный предикат на конечном множестве X, состоящем, например, из двух элементов a и b. Тогда

$$\forall xP(x)\cong P(a)\wedge P(b);\quad \exists xP(x)\cong P(a)\vee P(b).$$

Применяя отрицание и воспользовавшись законами де Моргана, получаем:

$$[\neg(\forall xP(x))] = [\neg(P(a)\wedge P(b))] = [\neg P(a)\vee\neg P(b)] = [\exists x(\neg P(x))];$$

$$[\neg(\exists xP(x))] = [\neg(P(a)\vee P(b))] = [\neg P(a)\wedge\neg P(b)] = [\forall x(\neg P(x))].$$

Нетрудно видеть, что подобные равенства верны для предикатов на произвольном множестве X (не обязательно конечном):

$$[\neg(\forall xP(x))] = [\mathrm{x}\exists x(\neg P(x))];\ [\neg(\exists xP(x))] = [\forall x(\neg P(x))].$$

Эти равенства называют законами де Моргана для кванторов.

В математической практике распространены так называемые *ограниченные кванторы*.

Ограниченный квантор существования. Запись $\exists Q(x)P(x)$ служит сокращением для $\exists x(Q(x)\wedge P(x))$. Высказывание $\exists Q(x)P(x)$ истинно, если среди объектов, обладающих свойством Q, найдется объект, обладающий свойством P. Например, утверждение «существует отрицательное число, квадрат которого больше двух» может быть записано в виде $\exists x<0\ x^2>2$.

Ограниченный квантор общности. Запись $\forall Q(x)P(x)$ служит сокращением для $\forall x(Q(x)\to P(x))$. Высказывание $\forall Q(x)P(x)$ истинно, если $P(x)$ истинно для всех x, обладающих свойством Q. Например, утверждение «квадрат любого числа из промежутка $[-2;2]$ не превосходит четырех» может быть записано в виде $\forall x\in[-2;2]\ x^2\le 4$. Равносильным образом это может быть записано так же, как $\forall|x|\le 2\ x^2\le 4$.

2.4. Формулы логики предикатов и логические законы

Подобно тому, как определялись формулы логики высказываний, можно определить формулы логики предикатов. Не вдаваясь в детали (точные определения будут даны в следующей лекции), скажем только, что эти формулы содержат предикатные символы $P(x)$, $Q(x,y)$ и т.п. с указанием числа и

имен предметных переменных, логические операции и кванторы.

Некоторые формулы являются равносильными (или связаны отношением следования) в силу самой их формы, независимо от того, как они будут *проинтерпретированы*, то есть какова выбранная предметная область, какой «смысл» придан предикатным символам (то есть, какие предикаты подставлены в формулы вместо предикатных символов), какие предметы будут подставлены вместо предметных переменных. Подобного рода равносильности и следования выражают логические законы. В качестве примера можно привести рассмотренные в предыдущем пункте законы де Моргана для кванторов. Особый интерес представляют формулы, которые остаются истинными при любой интерпретации (такие формулы называют *общезначимыми*). Для формул логики высказываний тождественную истинность формулы можно проверить с помощью таблиц истинности. В случае формул логики предикатов общей процедуры установления общезначимости формулы нет, для каждой формулы приходится подбирать свой метод проверки.

Важной проблемой логики вообще, и в частности логики предикатов, является поиск универсального алгоритма, позволяющего отличать истинные суждения от ложных. Эту проблему в различных ее формулировках называют *проблемой разрешения*. Для логики предикатов проблема разрешения

решается отрицательно. Американским математиком А. Черчем установлено, что не существует общего алгоритма для определения того, что произвольная формула логики предикатов общезначима.

В приводимых ниже формулах использование предикатного символа без указания предметных переменных означает, что соответствующий предикат не зависит от указанных явно предметных переменных. Мы используем знаки $\Leftrightarrow$ и $\Rightarrow$ для указания на то, что формулы равносильны или что одна формула следует из другой при любой интерпретации.

Законы пронесения кванторов через конъюнкцию и дизъюнкцию:

$$\forall x(P(x)\wedge Q(x)) \Leftrightarrow \forall xP(x)\wedge\forall xQ(x);$$

$$\forall x(P(x)\vee Q) \Leftrightarrow \forall xP(x)\vee Q;$$

$$\exists x(P(x)\vee Q(x)) \Leftrightarrow \exists xP(x)\vee\exists xQ(x);$$

$$\exists x(P(x)\wedge Q) \Leftrightarrow \exists xP(x)\wedge Q.$$

Законы пронесения кванторов через импликацию:

$$\forall x(P(x)\to Q) \Leftrightarrow \exists xP(x)\to Q;$$

$$\exists x(P(x)\to Q) \Leftrightarrow \forall xP(x)\to Q;$$

$$\forall x(Q\to P(x)) \Leftrightarrow Q\to\forall xP(x);$$

$$\exists x(Q\to P(x)) \Leftrightarrow Q\to\exists xP(x).$$

Законы удаления квантора общности и введения квантора существования:

$$\forall x P(x) \Rightarrow P(y);\ P(y) \Rightarrow \exists x P(x).$$

Законы коммутативности для кванторов:

$$\forall x \forall y P(x,y) \Leftrightarrow \forall y \forall x P(x,y)$$

$$\exists x \exists y P(x,y) \Leftrightarrow \exists y \exists x P(x,y)$$

$$\exists y \forall x P(x,y) \Rightarrow \forall x \exists y P(x,y)$$

В качестве примера проведем доказательство того, что *формулы* $\forall x(P(x) \to Q)$ *и* $\exists x P(x) \to Q$ *равносильны*.

Доказательство. Пусть P – произвольный предикат на некотором множестве X, а Q – некоторое утверждение. Рассмотрим два случая: $[Q]=0$ и $[Q]=1$. Пусть сначала $[Q]=0$. При подстановке $a \in X$ вместо x высказывание $P(a) \to Q$ истинно, если $P(a)$ ложно, и ложно в противном случае. Таким образом, высказывание $\forall x(P(x) \to Q)$ истинно в том и только том случае, когда $P(a)$ ложно для всех $a \in X$. Высказывание $\exists x P(x) \to Q$ истинно, если ложно высказывание $\exists x P(x)$, то есть если $P(a)$ ложно для всех $a \in X$. Следовательно, высказывания $\forall x(P(x) \to Q)$ и $\exists x P(x) \to Q$ имеют одинаковое значение истинности при $[Q]=0$.

Пусть теперь $[Q]=1$. При подстановке $a \in X$ вместо x высказывание $P(a) \to Q$ истинно независимо от того, каково значение истинности высказывания $P(a)$. Таким образом, высказывание $\forall x(P(x) \to Q)$ истинно. Но и высказывание

$\exists x P(x) \to Q$ также истинно (независимо от того, истинно ли высказывание $\exists x P(x)$), то есть если $P(a)$ ложно для всех $a \in X$. Следовательно, и при $[Q]=1$ высказывания $\forall x(P(x) \to Q)$ и $\exists x P(x) \to Q$ имеют одинаковое значение истинности.□

Проведем еще одно доказательство.

Формулы $\forall x(P(x) \vee Q(x))$ *и* $\forall x P(x) \vee \forall x Q(x)$ *не равносильны.*

Доказательство. Для доказательства достаточно привести контрпример. На множестве целых чисел рассмотрим предикаты «x – четное число» и «x – нечетное число» и подставим их вместо соответственно $P(x)$ и $Q(x)$. Имеем:

$[\forall x((x$ – четное число$) \vee (x$ – нечетное число$))]=1;$

$[\forall x(x$ – четное число$) \vee \forall x(x$ – нечетное число$)] =$

$= [\forall x(x$ – четное число$)] \vee [\forall x(x$ – нечетное число$)] = 0 \vee 0 = 0.$

В рассмотренной интерпретации формулы $\forall x(P(x) \vee Q(x))$ и $\forall x P(x) \vee \forall x Q(x)$ имеют разные значения истинности. Следовательно, эти формулы не равносильны.□

2.5. Выполнимые формулы и проблема разрешения

Формула логики предикатов называется *выполнимой* на множестве X, если она превращается в истинное высказывание при некоторой интерпретации ее на этом множестве. Формула общезначима, если ее отрицание невыполнимо ни на одном множестве. Это простое замечание показывает, что проблема разрешения может рассматриваться применительно к выполнимым формулам.

Несмотря на отрицательное решение общей проблемы, тем не менее, сужая проблему, иногда удается найти соответствующие алгоритмы (например, построение таблиц истинности для формул, которые содержат только высказывания).

Ограничиваясь интерпретацией формул на конечных множествах, можно указать алгоритм для установления выполнимости формул. Мы проиллюстрируем применение алгоритма на примере.

Пример. Проверим выполнимость формулы

$$\forall x \exists y (\neg P(y,y) \wedge P(x,y))$$

на двухэлементном множестве $\{a,b\}$. Имеем:

$$[\forall x \exists y (\neg P(y,y) \wedge P(a,y))] =$$

$$= [\exists y (\neg P(y,y) \wedge P(a,y))] \wedge [\exists y (\neg P(y,y) \wedge P(b,y))] =$$

$$= ([(\neg P(a,a) \wedge P(a,a))] \vee [(\neg P(b,b) \wedge P(a,b))]) \wedge$$

$$\wedge ([(\neg P(a,a) \wedge P(b,a))] \vee [(\neg P(b,b) \wedge P(b,b))]).$$

Полагая

$$A=P(a,a),\ B=P(a,b),\ C=P(b,a),\ D=P(b,b),$$

получаем

$$[\forall x \exists y (\neg P(y,y) \wedge P(a,y))] =$$

$$= ([\neg A \wedge A] \vee [\neg D \wedge B]) \wedge ([\neg A \wedge C] \vee [\neg D \wedge D]).$$

Тем самым вопрос о выполнимости формулы логики предикатов сводится к соответствующему вопросу о формуле логики высказываний, для поиска ответа на который можно

воспользоваться стандартными методами. После очевидных упрощений достаточно построить таблицу истинности для формулы

$$\neg D \wedge B \wedge \neg A \wedge C.$$

Если в итоговом столбце встречается хотя бы один раз значение 1, исходная формула логики предикатов выполнима. В данном случае легко убедиться, что это так.□

Проблема разрешения может быть решена, если ограничиться формулами, содержащими только одноместные предикаты. Это вытекает из следующей теоремы, которую мы приводим без доказательства.

Теорема. *Если формула логики предикатов, содержащая только одноместные предикатные символы, выполнима, то она выполнима на конечном множестве, содержащем не более* 2^n *переменных, где n – число различных предикатных символов, входящих в рассматриваемую формулу*.

В заключение приведем пример формулы, которая *выполнима на бесконечном множестве и невыполнима ни на каком конечном множестве*. Существование подобной формулы имеет помимо прочего философское значение: язык логики предикатов позволяет различить конечное и бесконечное.

Пример. Рассмотрим формулу

$$(\forall x \exists y P(x,y)) \wedge (\forall x(\neg P(x,x)) \wedge (\forall x \forall y \forall z((P(x,y) \wedge P(y,z)) \rightarrow P(x,z)).$$

Предикат $P(x,y)$ можно трактовать как упорядочение (x предшествует y). Второй и третий конъюнктивные члены говорят о том, что упорядочение антирефлексивно и транзитивно. Первый говорит о том, что для каждого элемента существует следующий за ним. Если интерпретировать $P(x,y)$ как $x<y$ на множестве натуральных чисел, рассматриваемая формула станет истинной. Значит, она выполнима на бесконечном множестве.

Нетрудно показать, что формула не выполнима ни на каком конечном множестве. Предположим, что формула выполнима на некотором непустом множестве X, и $P(x,y)$ – некоторый предикат на этом множестве, который превращает формулу в истинное высказывание. Пусть $a \in X$. Существует $b \in X$ такое, что $P(a,b)$. Так как $P(a,a)$ и $P(b,b)$ должны быть ложны, a отлично от b. В свою очередь для b найдется такое $c \in X$, отличное от b, что $P(b,c)$. По транзитивности заключаем, что $P(a,c)$. Но тогда a и c различны. Продолжая подобные построения, можно продолжить цепочку $a,b,c, \ldots$, состоящую из различных элементов сколь угодно далеко. Если множество X конечно, сделать это невозможно.□

2.6. Логика предикатов и математическая практика

В математической практике обычно применяется смесь естественного языка и формул, образующая своеобразный математический «жаргон» (математическое арго). В принципе,

математические теории могут быть записаны на полностью формализованном язык. Однако их восприятие человеком (да и создание – тоже) будет крайне затруднено, если вообще возможно. Применение естественного языка существенно облегчает восприятие математических текстов. При этом возникает, однако, опасность неоднозначного понимания. Всякий текст ориентирован на определенную категорию читателей. Уровень его формализации должен быть таков, чтобы текст достаточно легко воспринимался читателем, и компетентности читателя хватало для устранения возможной неоднозначности понимания.

Например, определение предела последовательности может быть дано так: «Число a называется пределом последовательности $\{a_n\}$, если a_n становится сколь угодно близким к a для достаточно больших n». Эта формулировка может быть уточнена: «Число a называется пределом последовательности $\{a_n\}$, если для любого положительного числа ε существует такой номер n_0, начиная с которого все члены последовательности отличаются от a по модулю меньше, чем на ε». Наконец, то же определение может быть записано на языке логики предикатов:

(a есть предел $\{a_n\}$) $\Leftrightarrow \forall \varepsilon>0\ \exists n_0 \in N\ \forall n\ (n>n_0 \rightarrow |a_n - a|<\varepsilon)$.

Записи типа последней, если они оказываются не слишком сложны, часто используют для введения новых понятий. Например, пусть P и Q – двухместные предикаты на множестве

X. Трактуя их как бинарные отношения, композицию PQ можно определить формулой

$$(PQ)(x,z)=\exists y(P(x,y)\wedge Q(y,z)).$$

Желая подчеркнуть, что формула является определением, иногда используют стилизованный знак равенства:

$$(PQ)(x,z):= \exists y(P(x,y)\wedge Q(y,z)).$$

То же определение может быть записано и в такой форме:

$$(PQ)(x,z) \overset{опр}{\Leftrightarrow} \exists y(P(x,y)\wedge Q(y,z)).$$

Обычно теоремы формулируются в виде утверждений типа: *если* $P(x)$, *то* $Q(x)$. Их следует понимать так: если истинно $P(x)$, то истинно $Q(x)$. Такая теорема может быть представлена формулой

$$[\forall x(P(x)\rightarrow Q(x))]=1,$$

хотя более принятой является форма

$$P(x) \Rightarrow Q(x).$$

Говорят, что $P(x)$ – *достаточное* условие для $Q(x)$, а $Q(x)$ – *необходимое* условие для $P(x)$. Утверждение $Q(x)\Rightarrow P(x)$ называют *обратным* к утверждению $P(x)\Rightarrow Q(x)$. Запись

$$P(x) \Leftrightarrow Q(x)$$

соответствует утверждению: $P(x)$ *тогда и только тогда, когда* $Q(x)$.

3. Формальные теории

3.1. Формализация в математике

Формализация в математике необходима для более точного обоснования методов построения математических теорий. Стимулом для формализации служит появлений противоречий в теориях, построенных на основе «неформализованных» интуитивных представлений. Примером здесь может служить парадокс Рассела. Обнаружение парадокса (противоречия в «наивной» теории множеств) вынудило пересмотреть основания теории множеств и формализовать многие понятия и построения, представлявшиеся до этого очевидными и не нуждающимися в формальных описаниях.

Необходимость формализации возникает также тогда, когда требуется доказать, что некоторый объект не существует.

Рассмотрим такой объект как математическое доказательство. Рассуждение становится доказательством в результате, по выражению Ю.И. Манина, «социального акта "принятия доказательства"». Несколько упрощая, можно сказать что доказательство становится доказательством, когда таковым его признает математическое сообщество. Доказательство публикуется, обсуждается математической общественностью и принимается или отвергается в зависимости от того, насколько оно соответствует принятым критериям

доказательности. Это справедливо применительно не только к математике, но и к другим наукам. Критерии доказательности в математике практически всегда (по крайней мере, со времен Евклида) были достаточно высоки. В математической теории без доказательства принимаются аксиомы. Из них по явно сформулированным правилам выводятся теоремы. Чтобы доказать теорему, достаточно предъявить некоторый текст, который удовлетворяет определенным требованиям, позволяющим принять его в качестве доказательства. Хотя требования к доказательствам со временем эволюционировали (в направлении повышения уровня строгости), тем не менее основа оставалась более или менее неизменной. Ситуация изменилась, когда возникла необходимость доказать отсутствие доказательства. Без точно зафиксированного определения сделать это невозможно. Поясним это таким примером. Предположим, исследуется проблема присутствия на Земле инопланетян. Если кто-то сумеет предъявить сторукого обитателя летающей тарелки, это будет признано положительным решение проблемы. Давать при этом точное определение того, что такое инопланетянин, не потребуется. Для доказательства отсутствия инопланетян точное определение необходимо. К примеру, определение «инопланетянин – существо, прилетевшее на Землю из космоса» не сработает: под него подпадут космонавты.

Уточнение определения можно продолжить, однако ясно, что выработка точного определения – дело не простое.

Еще один пример доставляет нам понятие алгоритма. Предположим, что исследуется вопрос о существовании алгоритма для решения некоторого класса уравнений. Чтобы доказать существование алгоритма, достаточно предъявить описание процедуры отыскания корней. Интуитивного представления об алгоритме обычно бывает достаточно, чтобы понять, является ли предъявленная процедура алгоритмом или нет. Например, не требуется точного определения алгоритма, чтобы понимать, что традиционный школьный метод решения квадратных уравнений является таковым. Если же нужно доказать, что алгоритма не существует, без предельно точного и однозначно понимаемого определения не обойтись.

Необходимый уровень уточнения понятий (например, доказательства и алгоритма) достигается в рамках соответствующих формализованных систем. Обычно построение таких систем производится на основе принципа индукции в его расширенном понимании.

Пусть, например, требуется дать точное определение некоторого понятия или, что равносильно, точно описать класс объектов $\boldsymbol{C}$, составляющий содержание рассматриваемого понятия. Прежде всего фиксируется математический язык, на котором будет дано описание – набор знаков (алфавит) и правила их комбинации (синтаксис). Объекты

формализованной теории – это определенные языковые конструкции. Далее указываются примитивы и правила построения объектов класса ***C***. Все примитивы принадлежат классу ***C*** по определению. Правила построения имеют следующий вид: объект O может быть построен из объектов O_1, O_2, …,O_k. При этом класс ***C*** считается замкнутым относительно правильных построений: если все объекты O_1, O_2, …, O_k содержатся в классе ***C***, то и объект O содержится в классе ***C***. Таким образом, в классе ***C*** содержатся все примитивы; объекты, которые могут быть построены из примитивов; объекты, которые могут быть построены из объектов, построенных из примитивов, и т.д. Никаких других объектов класс ***C*** не содержит. Объект O принадлежит классу ***C*** тогда и только тогда, когда имеется конечная цепочка объектов

$$O_1, O_2, \ldots, O_n$$

такая, что $O_n=O$, и каждый объект в цепочке является примитивом или может быть построен из некоторых предшествующих ему объектов. Такое определение класса ***C*** называется рекурсивным.

При формализации понятия доказательства объектами считаются утверждения, записанные на языке логики (с использованием, быть может, специальных математических символов). В качестве класса ***C*** берется класс теорем. Роль примитивов играют аксиомы, а роль правил построения объектов – так называемые правила вывода. Цепочка

утверждений, показывающая принадлежность утверждения X классу теорем, называется доказательством (или выводом). Получающиеся в результате таких построений теории называют формальными теориями или исчислениями.

При формализации понятия алгоритмической вычислимости объектами считаются функции, описываемые на языке какой-нибудь математической теории (например, арифметики). Роль примитивов играют функции, вычислимость которых не вызывает сомнений. Правилами построения служат некоторые точно описанные алгоритмические конструкции.

Далее в этой лекции мы рассмотрим исчисление высказываний, исчисление предикатов и теории первого порядка (в частности формальную арифметику). В следующей лекции будет рассмотрена формализация понятий алгоритма и эффективной вычислимости.

3.2. Исчисление высказываний

Язык исчисления высказываний тот же, что и язык логики высказываний. Напомним, что *алфавит* состоит из символов пропозициональных переменных X, Y, …, знаков логических операций $\neg$, $\wedge$, $\vee$, $\rightarrow$ и скобок (,). *Формулы* определяются рекурсивно:

любая пропозициональная переменная есть формула;

если U и V – формулы, то $(\neg U)$, $(U \wedge V)$, $(U \vee V)$, $(U \rightarrow V)$ *формулы*.

Произвольное слово (последовательность символов алфавита) W является формулой тогда и только тогда, когда имеется конечная цепочка слов

$$U_1, U_2, \ldots, U_n$$

такая, что $U_n=W$, и каждое слово в цепочке является пропозициональной переменной или получено из некоторых предшествующих ему слов с помощью логических операций. Так же как и ранее, мы принимаем соглашения о сокращенной записи формул (отбрасывание внешних скобок и т.п.).

Следующие формулы считаются *аксиомами*:

($A1$) $X\to(Y\to X)$;

($A2$) $(X\to(Y\to Z))\to((X\to Y)\to(X\to Z))$;

($A3$) $(X\wedge Y)\to X$;

($A4$) $(X\wedge Y)\to Y$;

($A5$) $(X\to Y)\to((X\to Z)\to(X\to(Y\wedge Z)))$;

($A6$) $X\to(X\vee Y)$;

($A7$) $Y\to(X\vee Y)$;

($A8$) $(X\to Z)\to((Y\to Z)\to((X\vee Y)\to Z))$;

($A9$) $(X\to Y)\to(\neg Y\to\neg X)$;

($A10$) $\neg\neg X\to X$;

($A11$) $X\to\neg\neg X$.

Если формула U содержит в своей записи пропозициональную переменную X, а V – произвольная формула, условимся обозначать через $U(X/V)$ формулу,

полученную из U заменой всех вхождений переменной X формулой V. Если формула U переменной X не содержит, будем считать, что $U(X/V)$ совпадает с U.

Укажем теперь *правила вывода* (правила построения выводимых формул). Формулы, которые являются исходными для построения, будем записывать слева от знака "|–", а формулу, которая строится, – справа:

(*S*) $U \vdash U(X/V)$ *для любых формул* U, V *и пропозициональной переменной* X;

(*MP*) U, $U \to V \vdash V$ *для любых формул* U *и* V.

Правило (*S*) называется *правилом подстановки*; правило (*MP*) – *правилом заключения* (Modus Ponens).

Будем говорить, что формула $U(X/V)$ непосредственно выводима из формулы U, а формула V непосредственно выводима из формул U и $U \to V$. *Выводом* формулы W из формул $U_1, U_2, \ldots, U_k$, называется последовательность формул

$$V_1, V_2, \ldots, V_n,$$

такая, что $V_n = W$, а любая формула V_i, $i = 1,2,\ldots,n$ есть либо аксиома, либо одна из формул $U_1, U_2, \ldots, U_k$, либо непосредственно выводима из некоторых предшествующих ей формул $V_1, V_2, \ldots, V_{i-1}$.

Если существует вывод формулы W из формул $U_1, U_2, \ldots, U_k$, то говорят, что формула W *выводима* из формул $U_1, U_2, \ldots, U_k$ и пишут

$$U_1, U_2,\ldots, U_k \vdash W.$$

В этой ситуации формулы U_1, $U_2,\ldots$, U_k называют *гипотезами* или *посылками*. Формула, выводимая из аксиом, называется *доказуемой* или *выводимой*. Выводимая формула выводима не только из аксиом, но и из пустого множества формул (данное выше определение вывода позволяет включить в цепочку вывода все аксиомы). В соответствии с этим, если формула W выводима, пишут $\vdash W$.

Приведем два примера.

Теорема. *Формула* $(X\wedge Y)\to(Y\wedge X)$ *выводима*.

Доказательство. Приведем вывод:

(1) $(X\to Y)\to((X\to Z)\to(X\to(Y\wedge Z)))$;

(2) $((X\wedge Y)\to Y)\to(((X\wedge Y)\to Z)\to((X\wedge Y)\to(Y\wedge Z)))$;

(3) $((X\wedge Y)\to Y)\to(((X\wedge Y)\to X)\to((X\wedge Y)\to(Y\wedge X)))$;

(4) $(X\wedge Y)\to Y$;

(5) $((X\wedge Y)\to X)\to((X\wedge Y)\to(Y\wedge X))$;

(6) $(X\wedge Y)\to X$

(7) $(X\wedge Y)\to(Y\wedge X)$.

Комментарии: (1) – аксиома; (2) непосредственно выводится из (1) подстановкой $X\wedge Y$ вместо X; (3) непосредственно выводится из (2) подстановкой $X\wedge Y$ вместо Z; (4) – аксиома; (5) непосредственно выводится из (3) и (4) по правилу заключения; (6) – аксиома; (7) непосредственно выводится из (5) и (6) по правилу заключения.□

Теорема. *Формула $V\to W$ выводима, какова бы ни была выводимая формула W.*

Доказательство. Пусть W_1, W_2,…, $W_n=W$– вывод формулы W. Формула $W\to(Y\to W)$ непосредственно выводится из аксиомы ($A1$) подстановкой W вместо X; формула $Y\to W$ непосредственно выводится из W и $W\to(Y\to W)$ по правилу заключения. Таким образом, последовательность формул

$$W_1, W_2,\ldots, W_n, (A1), W\to(Y\to W), Y\to W$$

является выводом формулы $Y\to W$.□

Из этих примеров видно, что доказательства даже относительно несложных формул оказываются довольно громоздкими. Следующая теорема позволяет устанавливать выводимость формул гораздо более простым способом, чем непосредственное построение вывода.

Теорема о дедукции. *Пусть Γ – некоторое конечное множество формул (гипотез), U* и *V – произвольные формулы, такие, что V выводима из совокупности формул Γ и U. Тогда формула $U\to V$ выводима из формул Γ.*□

Коротко утверждение теоремы о дедукции записывают в следующей форме:

$$\frac{\Gamma, U \vdash V}{\Gamma \vdash U\to V}$$

Эту запись следует понимать так: если верно то, что записано над чертой, то верно и записанное под чертой. В такой форме записывают и другие подобные утверждения, которые называют *производными правилами вывода*.

В качестве примера применения теоремы дедукции установим справедливость следующего правила.

Теорема (*правило силлогизма*):

$$\frac{\vdash U\to V,\ \vdash V\to W}{\vdash U\to W}$$

Доказательство. Формулу W можно вывести из формул $U\to V,\ V\to W,\ U$, применив дважды правило заключения. Тогда, по теореме дедукции, формула $U\to W$ выводима из формул $U\to V,\ V\to W$.□

Легко проверить (например, по таблицам истинности), что все аксиомы исчисления высказываний являются тождественно истинными формулами. Очевидно, что формулы, непосредственно выводимые из тождественно истинных формул, также тождественно истинны. Таким образом, все выводимые формулы тождественно истинны. Оказывается, что верно и обратное.

Следующая теорема дает для исчисления высказываний положительное решение так называемой *проблемы полноты*.

Теорема. *Исчисление высказываний полно: всякая тождественно истинная формула алгебры высказываний выводима в исчислении высказываний.*□

3.3. Исчисление предикатов

Алфавит исчисления предикатов состоит из предметных переменных x, y, … (возможно, с индексами); предикатных символов P, Q, … ; знаков логических операций $\neg$, $\wedge$, $\vee$, $\rightarrow$; кванторов $\forall$, $\exists$; скобок (,).

Для предметных переменных и предикатов могут использоваться индексы. Для каждого предикатного символа указано число мест для аргументов. Например, можно считать, что каждый n-местный предикатный символ задается комбинацией знаков типа $P(\ ,\ ,\ldots,\ )$, в которой число аргументов указывается числом промежутков между запятыми. Чтобы не загромождать обозначений, мы будем иногда опускать указание на число аргументов.

Дадим определение *формулы*. Множество формул определяется рекурсивно. Оно является наименьшим подмножеством выражений, удовлетворяющим следующим условиям.

1) *Если* $P(\ ,\ ,\ldots,\ )$ *– n-местный предикатный символ, а* $x_1,x_2,\ldots,x_n$ *– предметные переменные, то* $P(x_1,x_2,\ldots,x_n)$ *– формула, причем все вхождения в нее предметных переменных свободны.*

2) *если U и V – формулы, то* $(\neg U)$, $(U \wedge V)$, $(U \vee V)$, $(U \to V)$ – *формулы; все вхождения предметных переменных, свободные в исходных формулах, остаются свободными и в построенных*.

3) *если U – формула, содержащая свободное вхождение переменной x,* то $\forall x U$, $\exists x U$ – *формулы; в этих формулах все вхождения переменной x связаны, вхождения остальных переменных свободны или связаны так же, как в формуле U*; *формулу U называют областью действия квантора*.

В этом рекурсивном определении формулы дано также определение свободного и связанного вхождения переменой и области действия квантора. Например, в формуле

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

все вхождения переменной y свободны; вхождение переменной x в первый дизъюнктивный член связано, во второй – свободно. Областью действия квантора является формула $P(x,y) \to Q(y)$.

Аксиомы исчисления предикатов содержат все аксиомы исчисления высказываний и следующие две аксиомы:

($P1$) $\forall x U \to U(x/y)$;

($P2$) $U(x/y) \to \exists x U$.

Предполагается, что формула U содержит свободные вхождения переменной x, причем ни одно из них не находится в области действия квантора по y; через $U(x/y)$ обозначается формула, полученная из U заменой всех свободных вхождений x на y. В дальнейшем мы будем использовать упрощенные обозначения. Мы будем писать $U(x)$, если формула U содержит

свободные вхождения переменной x, а вместо $U(x/y)$ будем писать $U(y)$.

Предположения о вхождениях переменных существенны. Отказ от них может привести к формулам, которые нельзя признать логически верными. Рассмотрим, например, формулу $\exists y P(x,y)$. По аксиоме ($P1$) мы получим формулу $\forall x \exists y P(x,y) \to \exists y P(y,y)$, допускающую интерпретации, в которых она не является истинной.

Правила вывода:

(MP) *правило заключения – то же, что и в исчислении высказываний;*

(G) *если формула* $V(x)$ *содержит свободные вхождения переменной x, а формула U их не содержит, то*

$$U \to V(x) \mid\!- U \to \forall x V(x);$$

(E) *если формула* $U(x)$ *содержит свободные вхождения переменной x, а формула V их не содержит, то*

$$U(x) \to V \mid\!- \exists x U(x) \to V.$$

Правило (G) называется *правилом обобщения* или $\forall$-введения, правило (E) – правилом $\exists$-*введения*.

В качестве примера вывода в исчислении предикатов докажем правило переименования связанных переменных.

Теорема. *Если формула* $U(x)$ *не содержит свободных вхождений переменной y и содержит свободные вхождения*

переменной x, не попадающие в область действия квантора по y, то из формулы $\forall x U(x)$ *выводится формула* $\forall y U(y)$.

Доказательство. Укажем вывод:

(1) $\forall x U(x)$;

(2) $\forall x U(x) \to U(y)$;

(3) $\forall x U(x) \to \forall y U(y)$;

(4) $\forall y U(y)$.

Комментарии: (1) – гипотеза; (2) – аксиома ($P1$); (3) – получено из (2) по правилу обобщения; (4) – получено из (1) и (3) по правилу заключения.□

Как и для исчисления высказываний, нетрудно убедиться в том, что любая выводимая формула исчисления предикатов *общезначима* (истинна при любой ее интерпретации), и тем самым выражает собой некоторый логический закон.

Следующая теорема, доказательство которой существенно отличается от доказательства аналогичной теоремы для исчисления высказываний (и значительно сложнее), устанавливает полноту исчисления предикатов.

Теорема. *Исчисление предикатов полно: всякая общезначимая предикатная формула выводима в исчислении предикатов.*□

3.4. Теории первого порядка. Формальная арифметика

Исчисление предикатов, рассмотренное в предыдущем пункте, называют *чистым*. Этим подчеркивают его

исключительно логический характер. При формализации конкретных математических теорий, таких как теория множеств или арифметика, применяют *прикладные* исчисления предикатов. В прикладных исчислениях используются специфические для соответствующей предметной области предикаты, константы, функциональные символы. Важнейший класс формальных языков, на которых происходит формализация математических теорий, – *языки первого порядка* (слова «первого порядка» отражают тот факт, что в этих теориях связывать кванторами можно только предметные переменные; применять кванторы к предикатам недопустимо). Теории, формализованные с использованием языков первого порядка, называют *теориями первого порядка*. Мы дадим описание языков первого порядка и параллельно, в качестве иллюстрации, опишем два важных языка: язык теории множеств Цермело–Френкеля и язык арифметики Пеано, и укажем аксиомы арифметики в рамках формальной теории.

Алфавит любого языка первого порядка разбивается на шесть попарно непересекающихся подмножеств.

Знаки логических операций: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\forall$, $\exists$.

Переменные: x, y, ….(возможно с индексами).

Скобки: (,).

Эти знаки являются общими для всех языков первого порядка.

Константы: a, b, … (возможно с индексами).

В языке теории множеств имеется одна константа ∅ (пустое множество).

В языке арифметики имеются две константы: 0 и 1.

Операции: f, g, … (возможно с индексами) с указанием числа аргументов.

В языке теории множеств операций нет.

В языке арифметики имеются две двухместные операции: сложение "+" и умножение "·".

Предикаты: P, Q, … (возможно с индексами) с указанием числа аргументов.

В языке теории множеств имеются: два двухместных предиката: ∈ (быть элементом) и = (равенство).

В языке арифметики имеется один двухместный предикат = (равенство).

Выражения языка первого порядка делятся на два типа: *термы* и *формулы*. Те и другие определяются индуктивно.

Множество термов – это наименьшее подмножество выражений, удовлетворяющее двум условиям:

1) *переменные и константы являются термами (атомарными);*

2) *если f – n-местная операция, а t_1, t_2, …, t_n – термы, то $f(t_1,t_2,\ldots,t_n)$ – терм.*

В языке теории множеств неатомарных термов нет; термами являются знаки переменных и ∅.

Для записи арифметических термов будет использоваться общепринятая форма: вместо +(11) мы будем писать 1+1 и аналогично в других случаях. Кроме того вводятся производные константы, которые служат сокращениями некоторых термов: знак 2 служит сокращением для 1+1; знак 3 – сокращением для 2+1, и т.д.. Далее, x^2 служит сокращением для $x \cdot x$; x^3 – сокращением для $x \cdot x \cdot x$ и т. д. С учетом этих обозначений термами в языке арифметики являются стандартно понимаемые арифметические выражения.

Множество формул – это наименьшее подмножество выражений, удовлетворяющее двум условиям:

если P – n-местный предикат, а t_1, t_2, …, t_n – *термы, то $P(t_1,t_2,\ldots,t_n)$ – формула (атомарная);*

выражения, полученные из формул с помощью логических операций, являются формулами.

Примеры атомарных формул в языке теории множеств: $x \in y$, $x=y$, $x \in \varnothing$ (естественно, мы пишем $x \in y$ вместо $\in(xy)$). Формула

$$\forall z(z \in x \rightarrow z \in y)$$

при неформальной интерпретации означает, что множество x является подмножеством множества y. Для этой формулы используется сокращенная запись $x \subset y$. Формула

$$\forall x \forall y \exists u \forall z(((z \in x \vee z \in y) \rightarrow z \in u) \wedge (z \in u \rightarrow (z \in x \vee z \in y)))$$

при неформальной интерпретации означает, что, каковы бы ни были множества x и y, существует множество u, являющееся их

объединением. Используя $X \leftrightarrow Y$ как сокращение для $(X \rightarrow Y) \wedge (Y \rightarrow X)$, эту формулу можно переписать так:

$$\forall x \forall y \exists u \forall z ((z \in x \vee z \in y) \leftrightarrow z \in u).$$

Примеры формул в языке арифметики: $2+2=4$, $2 \cdot 2=5$, $x+y=x+z$. Формула

$$\forall x \forall y ((2x+y=0 \wedge x+2y=0) \leftrightarrow (x=0 \wedge y=0))$$

при неформальной интерпретации означает, что система уравнений $2x+y=0$; $x+2y=0$ имеет единственное решение $x=0$, $y=0$.

При построении теории первого порядка некоторые формулы объявляются *аксиомами*. Правила вывода остаются теми же, что и в исчислении предикатов. Формула считается *теоремой*, если можно построить цепочку формул, заканчивающуюся этой формулой, такую, что каждая формула в этой цепочке либо аксиома, либо непосредственно выводима по правилам вывода из некоторых предшествующих ей формул.

К числу аксиом относятся, во-первых, все аксиомы исчисления предикатов. При этом в аксиомы ($P1$) и ($P2$) вносится поправка и они принимают следующий вид:

($P1'$) $\forall x U(x) \rightarrow U(t)$;

($P2'$) $U(t) \rightarrow \exists x U(x)$,

где $U(t)$ получается в результате подстановки в формулу U терма t вместо всех свободных вхождений переменной x, при

этом терм t не должен содержать переменных, связанных кванторами в формуле U.

Далее, если язык первого порядка содержит предикат равенства, то в число аксиом включатся *аксиомы равенства*:

(E1) $\forall x(x=x)$;

(E2) $\forall x(x=y)\to(U(x,x)\to U(x,y))$, где U – произвольная формула, а через $U(x,y)$ обозначена формула, полученная из U заменой некоторых свободных вхождений x на y (при условии, что вхождение y остается свободным).

На самом деле (E2) представляет собой не одну аксиому, а схему аксиом (по одной для каждой формулы). В теории первого порядка с равенством несложно установить стандартные свойства равенства. Выводимы следующие формулы:

$$x=y \to y=x;$$

$$(x=y \wedge y=z) \to x=z.$$

Наконец, в число аксиом теории первого порядка включаются *специальные аксиомы*.

Приведем один из вариантов системы специальных *аксиом арифметики*.

Аксиомы сложения:

$x+0=x$; $x+y=y+x$; $(x+y)+z=x+(y+z)$; $x+z=y+z \to x=y$.

Аксиомы умножения:

$x\cdot 0=0$; $x\cdot 1=x$; $x\cdot y=y\cdot x$; $(x\cdot y)\cdot z=x\cdot(y\cdot z)$.

Аксиома дистрибутивности:

$$x\cdot(y+z) = x\cdot y+x\cdot z.$$

Аксиома индукции (схема аксиом):

$$U(0) \wedge \forall x(U(x)\rightarrow U(x+1)) \rightarrow \forall x U(x),$$

где U – любая формула языка арифметики.

Теория первого порядка называется *непротиворечивой*, если в ней невозможно вывести какую-нибудь формулу U вместе с ее отрицанием $\neg U$. Из формулы $U\wedge\neg U$ (противоречие) вместе с логическими аксиомами можно вывести любую формулу. Поэтому теория непротиворечива тогда и только тогда, когда в ней существуют невыводимые формулы. Следующие теоремы Геделя показывают, насколько непросто обстоит дело даже в такой, казалось бы, простой теории, как формальная арифметика.

Теорема (*первая теорема Геделя о неполноте*). *Любая формальная теория, содержащая формальную арифметику, неполна: в ней существует и может быть эффективно построена формула U, не содержащая свободных переменных, такая, что U истинна, но не выводима*.□

Теорема (*вторая теорема Геделя о неполноте*). *Для любой непротиворечивой формальной теории, содержащей формальную арифметику, формула, выражающая непротиворечивость теории, недоказуема*.□

Эти две знаменитые теоремы имеют большое методологическое значение. Первая говорит о том, что для достаточно богатых теорий не существует адекватных и полных формализаций. Вторая утверждает, что непротиворечивость теории не может быть установлена средствами самой этой теории. Заметим, однако, что вторая теорема Геделя не отрицает возможности установить непротиворечивость теории. Например, непротиворечивость формальной арифметики может быть доказана (это сделано Генценом), правда, методами, не формализуемыми в формальной арифметике.

4. Алгоритмы и вычислимость

4.1. Мощность множества

Напомним, что для конечного множества A мы обозначаем через $|A|$ число его элементов. Будем называть число n *мощностью* множества A. Мощности конечных множеств A и B совпадают в том и только том случае, когда между элементами этих множеств можно установить взаимно однозначное соответствие. Если $f:A\to B$ – отображение, то $|f(A)|\le|A|$ (некоторые элементы множества A могут «склеиться»). Отображение f инъективно тогда и только тогда, когда $|f(A)|=|A|$ («склеек» не происходит). Для конечных множеств отображение f сюръективно тогда и только тогда, когда $|f(A)|=|B|$.

Предположим, что A и B – конечные множества одинаковой мощности, $|A|=|B|$, а $f:A\to B$ – некоторое отображение. Тогда следующие условия равносильны:

f инъективно;

f сюръективно;

f биективно (является взаимно однозначным соответствием).

В случае бесконечных множеств ситуация оказывается более сложной. Например, формулой $f(n)=2n$ определяется отображение f множества натуральных чисел в себя, которое инъективно, но не сюръективно.

В общем случае говорят, что множества A и B *равномощны* и пишут $|A|=|B|$, если между элементами этих множеств можно установить взаимно однозначное соответствие. Если существует инъективное отображение множества A в множество B, то говорят, что мощность A не превосходит мощности B и пишут $|A|\le|B|$.

Теорема Кантора–Бернштейна. *Если существуют инъективные отображения* $f:A\to B$ *и* $g:B\to A$, *то множества* A *и* B *равномощны. Иными словами: если* $|A|\le|B|$ *и* $|B|\le|A|$, *то* $|A|=B|$.

Доказательство. Положим $A_0=A$ и $A_1=g(B)$. Поскольку g устанавливает взаимно однозначное соответствие между элементами множеств B и $A_1=g(B)$, достаточно показать, что имеется взаимно однозначное соответствие между элементами множеств A и A_1.

Рассмотрим отображение $h:A\to A$, равное композиции отображений f и g. Как композиция инъективных отображений, оно инъективно. Определим индуктивно последовательность множеств $A_0, A_1,\ldots$, полагая

$$A_0=A;\ A_1=g(B);\ A_{i+2}=h(A_i),\ i=0,1,2,\ldots$$

Очевидно, $A_0\supset A_1$. Далее, $A_1=g(B)\supset g(f(A))=A_2$. Поэтому

$$A_2=h(A_0)\supset h(A_1)=A_3,\ A_3=h(A_1)\supset h(A_2)=A_4,\ \ldots$$

Таким образом,

$$A_0\supset A_1\supset A_2\supset\ \ldots\ \supset A_i\supset A_{i+1}\supset\ldots$$

Положим

$$C_i=A_i\setminus A_{i+1},\ i=0,1,\ldots;\ C=\bigcap_{i=0}^{\infty}A_i\ .$$

Отображение h устанавливает взаимно однозначное соответствие между элементами множеств C_i и C_{i+2} для всех $i=0,1,2,\ldots$.

Множества C, C_i, $i=0,1,2,\ldots$ образуют разбиение множества A, то есть они попарно не пересекаются, а их объединение составляет все множество A:

$$A=C\cup C_0\cup C_1\cup C_2\cup C_3\cup\ldots\ .$$

Точно так же множества C, C_i, $i=1,2,\ldots$ образуют разбиение множества A_1:

$$A_1=C\cup C_1\cup C_2\cup C_3\cup\ldots\ .$$

Перепишем эти разложения в следующем виде:

$$A=(C\cup C_1\cup C_3\cup\ldots)\cup\ (C_0\cup C_2\cup C_4\cup\ldots);$$

$$A_1=(C\cup C_1\cup C_3\cup\ldots)\cup\ (C_2\cup C_4\cup\ldots).$$

Отображение $\varphi:A\to A_1$, при котором

$$\varphi(x)=x,\ \text{если}\ x\in C\cup C_1\cup C_3\cup\ldots;$$

$$\varphi(x)=h(x),\ \text{если}\ x\in C_0\cup C_2\cup C_4\cup\ldots,$$

устанавливает взаимно однозначное соответствие между элементами множеств A и A_1.□

Следующие две теоремы приведем без доказательства.

Теорема Цермело. *Для любых множеств A и B выполняется одно из трех условий:* $|A|<|B|$, $|B|<|A|$, $|A|=|B|$.

Теорема. *Если существует сюръективное отображение множества A на множество B, то* $|A|\geq|B|$.

Последние три теоремы показывают, что сравнение по мощности бесконечных множеств обладает «привычными» свойствами сравнения по мощности конечных множеств.

В заключение покажем, что существуют множества сколь угодно больших мощностей.

Теорема Кантора. *Каково бы ни было множество A, множество всех его подмножеств* 2^A *имеет мощность строго большую, чем само множество A, то есть* $|A|<|2^A|$.

Доказательство. Соответствие $x\to\{x\}$, при котором каждому элементу x множества A сопоставлено одноэлементное подмножество $\{x\}$, задает инъективное отображение A в 2^A. Следовательно, $|A|\leq|2^A|$. Покажем теперь, что $|A|\neq|2^A|$. Предположим противное, то есть, что существует биективное отображение $f:A\to 2^A$. Положим

$$D=\{x\in A \mid x\notin f(x)\}.$$

Тогда

$$x\in D\Leftrightarrow x\notin f(x)$$

Поскольку f биективно, существует такой элемент $d\in A$, что $f(d)=D$. Подстановка d вместо x в предыдущую формулу приводит к противоречию:

$$d \in D \Leftrightarrow d \notin D. \square$$

4.2. Счетные множества

Начальный отрезок натурального ряда $[0;n-1]=\{1,2,\ldots,n-1\}$ конечен и содержит n элементов. Сам же натуральный ряд $\boldsymbol{N}=\{0,1,2,\ldots\}$ бесконечен. Поэтому не может быть инъективным никакое отображение $\boldsymbol{N}$ в $[0;n-1]$. Следовательно, $|\boldsymbol{N}|>n$, то есть мощность натурального ряда превосходит любое натуральное число. Множества, равномощные натуральному ряду, называются *счетными*. Для обозначения мощности счетных множеств используется символ $\aleph_0$ (читается «алеф ноль»). Если множество A конечно или счетно, его элементы могут быть занумерованы, то есть расположены в виде списка

$$a_0, a_1, a_2, a_3, \ldots ,$$

так, что всякий элемент множества A рано или поздно встретится в этом списке. Если множество A конечно, то и список конечен; в противном случае список оказывается бесконечным. Ясно, что при таких обозначениях отображение $i \to a_i$ – это и есть та самая биекция начального отрезка или всего натурального ряда на множество A, которая устанавливает конечность или счетность множества A.

Пример. Множество четных чисел счетно; их можно представить списком $0,2,4,6,\ldots$. Соответствие очевидно: $n \leftrightarrow 2n$.

Точно так же счетно и множество нечетных чисел 1,3,5,… . Здесь можно положить $n \leftrightarrow 2n+1$.□

Пример. Множество рациональных чисел счетно. Напомним, что всякое рациональное число однозначно записывается в виде несократимой дроби p/q, где p и q – взаимно простые целые числа и $q>0$. Составим список, содержащий все рациональные числа, в порядке возрастания величины $|p|+q$:

$$0;\ -1/1;\ 1/1;\ -2/1;\ -1/2;\ 1/2;\ 2/1;\ \ldots$$

Ясно, что любая дробь p/q появится в этом списке через конечное число шагов и получит свой номер.□

Укажем некоторые свойства счетных множеств.

1. *Всякое подмножество счетного множества конечно или счетно.*

Доказательство. Достаточно доказать справедливость утверждения для множества натуральных чисел: всякое подмножество A множества натуральных чисел конечно или счетно. Составим список элементов множества A в порядке их возрастания. Если этот список конечен – множество A конечно; если бесконечен – счетно.□

Из предыдущего предложения вытекает, что счетные множества являются наименьшими по мощности бесконечными множествами: если $|A| \le \aleph_0$, то A конечно или счетно.

2. *Образ счетного множества относительно произвольного отображения является конечным или счетным множеством*.

Доказательство. Пусть множество B является образом счетного множества A относительно некоторого отображения. Тогда, по теореме из предыдущего пункта, $|B|\le|A|$ и, значит, B конечно или счетно.□

Если элементы множества A представлены списком с повторениями

$$a_0, a_1, a_2, a_3, \dots ,$$

то есть списком, в котором некоторые элементы могут попадаться многократно, это означает, что отображение $i\to a_i$ сюръективно (но не инъективно). Таким образом, множество A является образом натурального ряда, и потому конечно или счетно.

3. *Всякое бесконечное множество содержит счетное подмножество.*

Доказательство. Пусть A – бесконечное множество. Тогда $|A|\ge\aleph_0$. Но это неравенство означает, что существует инъективное отображение множества натуральных чисел в A. Образ этого отображения – счетное подмножество множества A.□

4. *Объединение любого конечного (непустого) или счетного семейства счетных множеств счетно.*

Доказательство. Пусть счетные множества A_0, A_1, … представлены списками своих элементов:

$$A_0 = \{a_{00}, a_{01}, a_{02}, a_{03}, \dots\};$$

$$A_1 = \{a_{10}, a_{11}, a_{12}, a_{13}, \dots\};$$

$$A_2 = \{a_{20}, a_{21}, a_{22}, a_{23}, \dots\};$$

$$A_3 = \{a_{30}, a_{31}, a_{32}, a_{33}, \dots\};$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

Составим список объединения этих множеств A, располагая элементы объединения в порядке возрастания суммы индексов:

$$A = \{ a_{00}, a_{01}, a_{10}, a_{02}, a_{11}, a_{20}, a_{03}, \dots\}.$$

(если некоторые из множеств имеют общие элементы, в этом списке возможны повторения). Множество A бесконечно, и, значит, счетно.□

Из предыдущего утверждения вытекает, что объединение счетного числа конечных множеств конечно или счетно.

5. *Декартово произведение конечного числа счетных множеств счетно.*

Доказательство. Пусть

$$A = \{ a_0, a_1, a_2, a_3, \dots\}, B = \{ b_0, b_1, b_2, b_3, \dots\}$$

– счетные множества. Покажем, что счетно декартово произведение $A\times B$. Составим список его элементов подобно тому, как составлялся список рациональных чисел:

$$(a_0,b_0), (a_0,b_1), (a_1,b_0), (a_0,b_2), (a_1,b_1), (a_2,b_0), \dots .$$

Если счетны множества A, B, C, то счетно $A\times B$, а вместе с ним и $A\times B\times C = (A\times B)\times C$ как произведение двух счетных

множеств. Аналогично устанавливается счетность любого конечного семейства счетных множеств.□

6. *Пусть* $L = \{a,b, \ldots, \}$ *счетный алфавит. Тогда множество слов над алфавитом* L *(то есть конечных упорядоченных наборов символов алфавита) счетно.*

Доказательство. Множество n-буквенных слов можно естественным образом отождествить с L^n, счетность которого следует из утверждения 5. Теперь достаточно сослаться на утверждение 4: множество всех слов представляет собой объединение счетного семейства счетных множеств: слов из одной буквы; слов из двух букв, и т. д.□

4.3. Диагональный метод Кантора

В соответствии с теоремой Кантора из п. 4.1, множество всех подмножеств натурального ряда имеет мощность большую, чем $\aleph_0$, и, значит, не является счетным. Мы воспроизведем доказательство (с небольшими модификациями) для этого случая, чтобы подчеркнуть лежащую в основе доказательства важную идею диагонализации.

Сопоставим каждому множеству $A \subset \boldsymbol{N}$ его характеристическую последовательность из нулей и единиц

$$\alpha_0, \alpha_1, \alpha_2, \ldots$$

так, что $\alpha_i=1$, если $i \in A$, и $\alpha_i=0$, если $i \notin A$. Всякая последовательность из нулей и единиц является

характеристической для множества, элементы которого – номера мест, содержащих единицы. Таким образом между последовательностями из нулей и единиц и подмножествами множества $\boldsymbol{N}$ устанавливается взаимно однозначное соответствие. Пусть A_0, A_1, A_2, … – произвольный список подмножеств множества $\boldsymbol{N}$. Покажем, что в $\boldsymbol{N}$ найдется подмножество, не попавшее в этот список. Рассмотрим список множеств A_0, A_1, A_2, … вместе с их характеристическими последовательностями:

$$A_0 = \alpha_{00}, \alpha_{01}, \alpha_{02}, \alpha_{03}, \ldots ;$$

$$A_1 = \alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \ldots ;$$

$$A_2 = \alpha_{20}, \alpha_{21}, \alpha_{22}, \alpha_{23}, \ldots ;$$

$$A_3 = \alpha_{30}, \alpha_{31}, \alpha_{32}, \alpha_{33}, \ldots ;$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Составим «антидиагональную» последовательность

$$1-\alpha_{00}, 1-\alpha_{11}, 1-\alpha_{22}, 1-\alpha_{33}, \ldots .$$

Эта последовательность отличается, по крайней мере, первым элементом от первой последовательности списка, вторым элементом – от второй, третьим элементом – от третьей, и т.д. Следовательно, «антидиагональная» последовательность, а вместе с ней и соответствующее ей множество, не содержатся в списке. Приведенное рассуждение показывает, что невозможно составить список, включающий все подмножества

множества $\boldsymbol{N}$, и, значит, множество всех подмножеств множества $\boldsymbol{N}$ не является счетным.

Используя диагональный метод, покажем, что *множество действительных чисел отрезка* [0;1] *не является счетным*.

Доказательство. Всякое действительное число a из отрезка [0;1] может быть записано в виде бесконечной десятичной дроби

$$a = 0,\alpha_0\alpha_1\alpha_2\ldots .$$

Для чисел, представимых конечными десятичными дробями, такая запись неоднозначна. Например, записи 0,1000… и 0,0999… представляют одно и то же число. Условимся не использовать записи второго вида, в которых, начиная с некоторого места, идут одни девятки. Тогда представление чисел десятичными дробями окажется однозначным. Пусть a_0, a_1, a_2, … – произвольный список действительных чисел из отрезка [0;1]. Покажем, что на отрезке [0;1] найдется число, не попавшее в этот список. Рассмотрим список чисел a_0, a_1, a_2, … вместе с их десятичными представлениями:

$$a_0 = 0,\alpha_{00}\alpha_{01}\alpha_{02}\alpha_{03}\ldots ;$$

$$a_1 = 0,\alpha_{10}\alpha_{11}\alpha_{12}\alpha_{13}\ldots ;$$

$$a_2 = 0,\alpha_{20}\alpha_{21}\alpha_{22}\alpha_{23}\ldots ;$$

$$a_3 = 0,\alpha_{30}\alpha_{31}\alpha_{32}\alpha_{33}\ldots ;$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Положим $\beta_i=1$, если, $\alpha_{i,i}=2$, и $\beta_i=2$, если, $\alpha_{ii}\neq 2$. Число

$$\beta = 0,\beta_0\beta_1\beta_2\beta_3\ldots .$$

лежит на отрезке [0;1] и отличается, по крайней мере, первой цифрой после запятой от первого числа из списка, второй цифрой – от второго числа, третьей цифрой – от третьего и т.д. Следовательно, число β не содержится в списке. Таким образом, невозможно составить список, включающий все числа отрезка [0;1], и, значит, множество всех действительных чисел отрезка [0;1] несчетно.□

Мощность множества чисел отрезка [0;1] называется *континуум*; множества, имеющие ту же мощность, называются *континуальными*. Континуальными являются: множество всех действительных чисел, множество точек прямой, множество точек плоскости, множество последовательностей действительных чисел и многие другие множества, встречающиеся в математической практике.

Проблема существования несчетных множеств, меньших по мощности, чем континуум (так называемая *континуум-гипотеза*), возникла в тории множеств практически с момента появления этой теории. Гедель доказал, что предположение об отрицательном решении континуум-гипотезы не противоречит аксиоматике теории множеств. Позднее Коэн установил, что этой аксиоматике не противоречит и предположение о положительном решении континуум-гипотезы. Наличие в теории множеств проблемы, которая, казалось бы, должна

иметь решение типа «да» или «нет», но не имеет такового, в значительной степени стимулировало ту формализацию математики, о которой говорилось в предыдущей лекции.

4.4. Уточнение понятия алгоритма

В широком смысле слова алгоритм – это текст, который в определенных обстоятельствах может привести к однозначному развитию событий – процессу выполнения алгоритма. Анализ типичных алгоритмов позволяет выделить ряд их характерных свойств.

Каждый алгоритм служит для решения некоторого класса задач. Задачи должны быть записаны на некотором языке. Результат применения алгоритма – решение задачи– также должен быть записан на вполне определенном языке. Таким образом, в процессе выполнения алгоритма текст задачи преобразуется в текст ее решения. Процесс алгоритмического решения задачи должен быть дискретным. Он распадается на элементарные шаги и представляет собой цепочку преобразований вида

$$T_0 \to T_1 \to \ldots \to T_k,$$

где T_0 – текст, представляющий задачу, а T_k – текст, дающий ее решение. Преобразование текста на каждом шаге производится по предписаниям, которые берутся из конечного и фиксированного раз и навсегда списка.

Как было показано в п. 4.2, тексты (слова над конечным алфавитом) могут быть занумерованы. При этом цепочка текстов «задача – решение» превратится в числовую цепочку их номеров:

$$n_0 \to n_1 \to \ldots \to n_k.$$

Мы получаем числовую функцию $y=f(x)$, $n_0 \to n_k$, определенную на множестве номеров задач $X \subset \boldsymbol{N}$ и принимающую значения в $\boldsymbol{N}$. Алгоритм описывает не только саму функцию $f(x)$, но и способ ее пошагового вычисления.

Простейшее, но достаточно универсальное уточнение понятия алгоритма, позволяет считать, что алгоритм предписывает способ вычисления функции, заданной на некотором подмножестве множества $\boldsymbol{N}$ и принимающей значения в $\boldsymbol{N}$. Вычисление представляет собой конечную комбинацию элементарных вычислений из некоторого фиксированного набора. Точное описание элементарных вычислений и способов их комбинирования приводит к определению понятия алгоритма. Чтобы такое определение было удовлетворительным, необходимо выполнение следующего условия: любая функция, вычислимая каким бы то ни было алгоритмическим способом, может быть представлена как конечная комбинация зафиксированных элементарных вычислений. Последнее требование не может быть проверено математически и, являясь по существу естественно-научным, должно подтверждаться экспериментально.

На сегодняшний день известно несколько уточнений понятия алгоритма, приспособленных для решения определенных задач, в основе которых лежат различающиеся концепции: машины Тьюринга, машины Поста, нормальные алгоритмы Маркова, рекурсивные функции и др. Для каждого из них имеется свое определение алгоритмической вычислимости. Однако все эти уточнения понятия алгоритма в определенном смысле эквивалентны: справедлива теорема, утверждающая, что классы функций, вычислимых по Тьюрингу, по Посту, по Маркову, и класс рекурсивных функций совпадают.

Применительно к упомянутым уточнениям понятия алгоритма принимается следующая гипотеза.

Тезис Черча. *Числовая функция тогда и только тогда алгоритмически вычислима, когда она рекурсивна (или, что равносильно, вычислима по Тьюрингу, по Посту или по Маркову).*

4.5. Рекурсивные функции

Если не сделано специальных оговорок, мы будем предполагать, что рассматриваемые функции $y=f(x_1,x_2,\ldots,x_n)$ являются числовыми, их значения и аргументы принадлежат множеству натуральных чисел $\boldsymbol{N}=\{0,1,2,\ldots\}$. Областью определения функции $y=f(x_1,x_2,\ldots,x_n)$ может быть как все множество $\boldsymbol{N}^n$, так и некоторая его часть. Допуская

возможность того, что функция определена не на всем $\boldsymbol{N}^n$, мы будем называть функцию частичной.

Далее мы определим *простейшие функции* и *элементарные операции* над функциями.

Простейшие функции:

1) $S(x)=x+1$ (*функция следования*);

2) $O(x)=0$ (*тождественный ноль*);

3) $Pr[n;i](x_1,x_2,\ldots,x_n)=x_i$, $n\geq 1$ (*проекции*).

Заметим, что проекции $Pr[n;i]$ составляют бесконечное семейство функций.

Элементарные операции над частичными функциями.

1. *Суперпозиция* (или *композиция*).

Пусть даны частичная функция

$$g(x_1,x_2,\ldots,x_m)$$

и частичные функции

$$f_1(x_1,x_2,\ldots,x_n),\ \ldots,f_m(x_1,x_2,\ldots,x_n).$$

Суперпозицией функций g и $f_1,\ldots,f_m$ называется частичная функция

$$h(x_1,x_2,\ldots,x_n)=g(f_1(x_1,x_2,\ldots,x_n),\ldots,f_m(x_1,x_2,\ldots,x_n)),$$

которая задается на наборе $(x_1,x_2,\ldots,x_n)$ указанной формулой, если определены все значения $y_1=f_1(x_1,x_2,\ldots,x_n)$, …, $y_m=f_m(x_1,x_2,\ldots,x_n)$ и значение $g(y_1,y_2,\ldots,y_m)$. В противном случае функция $h(x_1,x_2,\ldots,x_n)$ считается неопределенной. Для функции

h, полученной суперпозицией функций g и $f_1,\ldots,f_m$, будем использовать обозначение $h=Cn[g;f_1,\ldots,f_m]$.

Примеры.

$Cn[S;S](x)=S(S(x))=S(x+1)=x+2$;

$Cn[S;Cn[S;S]](x)=x+3$;

$Cn[O;Pr[n;1]](x_1,x_2,\ldots,x_n)=O(Pr[n;1](x_1,x_2,\ldots,x_n))=O(x_i)=0$.□

2. *Рекурсия*.

Начнем с частных случаев.

Пусть заданы функция $g(y,z)$ и число a. Уравнения:

$$h(0)=a;\ h(y+1)=g(y,h(y))$$

однозначно определяют функцию $h(y)$. Последовательно вычисляя, находим:

$$h(1)=g(0,a);\ h(2)=g(1,h(1));\ \ldots$$

Пример. При $a=1$, $g(y,z)=y\cdot z$ уравнения

$$h(0)=1;\ h(y+1)=(y+1)h(y)$$

определяют функцию

$$h(y)=y!=1\cdot 2\cdot 3\cdot\ldots\cdot y.$$□

Пусть даны функции $f(x)$ и $g(x,y,z)$. Говорят, что функция $h(x,y)$ получается из функций f и g (*примитивной*) *рекурсией*, если функция h удовлетворяет уравнениям:

$$h(x,0)=f(x);\ h(x,y+1)=g(x,y,h(x,y)).$$

Ясно, что функция h определена однозначно. Имеем:

$$h(x,1)=g(x,0,h(x,0))=g(x,0,f(x));$$

$$h(x,2)=g(x,1,h(x,1));\ \ldots\ .$$

Для функции $h(x,y)$, полученной рекурсией из функций f и g, будем использовать обозначение $h=Rc[f;g]$.

Примеры. Пусть $f(x)=x$ (то есть $f=Pr[1;1]$) и $g(x,y,z)=z+1$ (то есть $g=Cn[S;Pr[3,3]]$). Тогда функция $\text{sum}=Rc[f;g]$ определяется уравнениями

$$\text{sum}(x,0)=x; \quad \text{sum}(x,y+1) = g(x,y,\text{sum}(x,y)) = \text{sum}(x,y)+1.$$

Имеем:

$$\text{sum}(x,1)=\text{sum}(x,0)+1=x+1;$$

$$\text{sum}(x,2)=\text{sum}(x,1)+1=(x+1)+1=x+2, \ldots$$

и, вообще, $\text{sum}(x,y)=x+y$.

Пусть $g(x,y,z)=z+x$ (то есть $g=Cn[\text{sum};Pr[3;3],Pr[3;1]]$). Определим функцию $\text{prod}(x,y)$ как $\text{prod}=Rc[O;g]$. Тогда h удовлетворяет уравнениям

$$\text{prod}(x,0)=0; \ \text{prod}(x,y+1)=h(x,y)+x.$$

Получаем:

$$\text{prod}(x,1)=h(x,0)+x=0+x=x;$$

$$\text{prod}(x,2) = h(x,1)+x = x+x = x\cdot 2; \ \ldots,$$

и, вообще, $\text{prod}(x,y)=xy$.□

Вообще говоря, в определении по рекурсии $h=Rc[f;g]$ можно считать, что x представляет собой набор аргументов $(x_1,x_2,\ldots,x_n)$. Тогда рекурсия по функциям $f(x_1,x_2,\ldots,x_n)$, $g(x_1,x_2,\ldots,x_n y,z)$ определяет функцию $h(x_1,x_2,\ldots,x_n,y)$.

Функции, которые могут быть получены из простейших функций операциями суперпозиции и рекурсии, называются *примитивно рекурсивными*.

3. *Минимизация*.

Пусть $f(x_1,x_2,\ldots,x_n,y)$ всюду определенная функция. Определим функцию $h(x_1,x_2,\ldots,x_n,z)$ условием:

если имеются значения y такие, что $f(x_1,x_2,\ldots,x_n,y)=z$, то $h(x_1,x_2,\ldots,x_n,z)$ есть наименьшее из таких значений; в противном случае $h(x_1,x_2,\ldots,x_n,z)$ не определено.

Для так определенной функции h будем писать $h=Mn[f]$.

Если функция $f(x_1,x_2,\ldots,x_n,y)$ частичная, то $h=Mn[f]$ определяется следующими условиями:

$h(x_1,x_2,\ldots,x_n,z)=y$, если $f(x_1,x_2,\ldots,x_n,y)=z$, причем $f(x_1,x_2,\ldots,x_n,t)$ определено и отлично от z для всех $t<y$; в противном случае $h(x_1,x_2,\ldots,x_n,z)$ не определено.

Пример. Рассмотрим функцию $h=Mn$[sum]. Имеем

$$h(x,z)=\min\{y \mid x+y=z\}.$$

Если $x\le z$, то $h(x,z)=z-x$, в противном случае $h(x,z)$ не определено. Обозначим эту функцию через dif.□

Частичные функции, которые могут быть получены из простейших с помощью конечного числа операций суперпозиции, рекурсии и минимизации, называются *рекурсивными* (или *частично рекурсивными*). Всюду определенные частично рекурсивные функции называются *общерекурсивными*. Запись частично рекурсивной функции с помощью простейших функций и операций будем называть *рекурсивной схемой*. Рекурсивная схема фактически задает *алгоритм вычисления функции*. По рекурсивной схеме функции

f может быть построено ее *рекурсивное описание*: конечная последовательность частичных функций $f_0, f_1, \ldots, f_n$ такая, что $f_n=f$, и каждая функция в этой последовательности либо является простейшей, либо получается применением одной из элементарных операций к некоторым из предшествующих ей функций. Одна и та же функция может быть определена с помощью разных рекурсивных схем. Это согласуется с представлением о том, что одну и ту же функцию можно вычислять по-разному.

Пример. Имеем следующую рекурсивную схему для функции dif из предыдущего примера:

$$\text{dif}=Mn[Rc[Pr[1;1]; Cn[S;Pr[3,3]]]].$$

Из этой формулы без труда можно получить рекурсивное описание функции dif:

$$Pr[1;1], Pr[3,3], S, Cn[S;Pr[3,3]], Rc[Pr[1;1]],$$
$$Mn[Rc[Pr[1;1]; Cn[S;Pr[3,3]]]]=\text{dif}.$$

Рекурсивная схема представляет собой слово над счетным алфавитом, содержащим в качестве символов натуральные числа, обозначения для простейших функций, элементарных операций, скобки, запятую и точку с запятой. Следовательно, *множество рекурсивных схем счетно*. Вместе с ним *счетно и множество частично рекурсивных функций.*

4.6. Вычислимость и разрешимость

Можно показать, подобно тому, как это делалось в п. 4.4, что традиционно считающиеся вычислимыми функции имеют рекурсивные описания и, значит, частично рекурсивны. Обычно используемые вычислительные схемы также реализуются с помощью простейших функций и элементарных операций. Все это и ряд других соображений приводит к следующей формулировке.

Тезис Черча. *Числовая функция тогда и только тогда алгоритмически вычислима, когда она частично рекурсивна*.

Построим пример *невычислимой функции*. Начнем с некоторых общих определений и замечаний.

Подмножество множества натуральных чисел $M \subset \boldsymbol{N}$ называется *разрешимым*, если его характеристическая функция

$$\chi_M(x)=1 \text{ при } x \in M,\ \chi_M(x)=0 \text{ при } x \notin M$$

рекурсивна. Содержательно разрешимость множества M означает, что существует алгоритм, позволяющий по любому числу x определить за конечное число шагов, принадлежит это число множеству M или нет.

Подмножество множества натуральных чисел $M \subset \boldsymbol{N}$ называется *перечислимым*, если оно является областью значений некоторой общерекурсивной функции f. Перечислимость множества M означает, что его элементы могут быть последовательно выписаны (возможно с повторениям) с помощью некоторой эффективной процедуры.

Всякое непустое разрешимое множество M является перечислимым.

Доказательство. Несложно определить перечисляющую функцию f. Пусть m – произвольный элемент множества M. Определяем по рекурсии:

$$f(0)=m; \qquad f(x+1)=\chi_M(x)(x+1)+(1-\chi_M(x+1))f(x),$$

то есть $f(x+1)=x+1$, если $x+1\in M$, и $f(x+1)=f(x)$, если $x+1\notin M$.□

Обратное, вообще говоря, неверно. Не всякое перечислимое множество является разрешимым. *Перечислимое множество разрешимо лишь в том случае, когда перечислимо также и его дополнение.*

В конце п. 4.4 было показано, что частично рекурсивные функции можно эффективно перенумеровать, используя их рекурсивные описания. Некоторые номера соответствуют общерекурсивным функциям. Обозначим множество таких номеров через M и покажем, что множество M неперечислимо.

Теорема. *Множество номеров общерекурсивных функций не перечислимо.*

Доказательство. Предположим противное. Пусть $\varphi(x)$ – общерекурсивная функция, множеством значений которой является M. Тогда последовательность $\varphi(0)$, $\varphi(1)$, $\varphi(2)$,… содержит номера всех общерекурсивных функций, и только их. Следуя диагональному методу, определим функцию $g(x)$ формулой

$$g(x)=f_{\varphi(x)}(x)+1.$$

Это определение дает алгоритм вычисления значений функции $g(x)$. В соответствии с тезисом Черча, функция $g(x)$ частично рекурсивна, и, значит, общерекурсивна, поскольку функция $g(x)$ определена для любого x. Значит, функция $g(x)$ должна получить свой номер при перечислении с помощью $\varphi(x)$. Пусть этот номер равен n, то есть $g(x)=f_{\varphi(n)}(x)$. Но тогда $g(n)=f_{\varphi(n)}(n)+1=g(n)+1$, что невозможно.□

Вообще неперечислимые и неразрешимые семейства функций – это не «экзотика», а, скорее, норма.

Приведем без доказательства следующую теорему.

Терема (Райс). *Никакое нетривиальное семейство вычислимых функций не является алгоритмически разрешимым.*

Иными словами, если C – некоторое семейство вычислимых функций такое, что есть функции, входящие в это семейство, а есть и не входящие в него, то множество номеров функций из C неразрешимо. Не существует алгоритма, который бы позволял по номеру функции сказать, входит она в C или нет.

Так, по номеру функции нельзя узнать, является ли она монотонной, периодической и т.п. Заметим, что, нумеруя частично рекурсивные функции, мы на самом деле нумеровали их рекурсивные описания, то есть вычисляющие их алгоритмы. Теорема Райса утверждает, что по номеру алгоритма нельзя

узнать, периодична ли, например, функция, вычисляемая в соответствии с этим алгоритмом.

5. Булевы функции

5.1. Двоичные векторы

Любое положительное целое число имеет единственное двоичное представление (в виде суммы неповторяющихся степеней числа 2). Например:

$$7=1+2+4;\ 35=32+2+1.$$

В общем случае, чтобы получить двоичное представление целого числа $x>0$, можно воспользоваться следующим соотношением:

$$x = \alpha_0+2(\alpha_1+2(\alpha_2+\ldots+2(\alpha_{n-2}+2\alpha_{n-1})\ldots),$$

где α_0 – остаток от деления x на 2 (то есть $\alpha_0=0$, если x четно, и $\alpha_0=1$, если x нечетно); α_1 – остаток от деления на 2 числа $x_1=(x-\alpha_0)/2$; α_2 – остаток от деления на 2 числа $x_2=(x_1-\alpha_1)/2$; и т.д. Тогда

$$x = \alpha_{n-1}\cdot 2^{n-1}+\alpha_{n-2}\cdot 2^{n-2}+\ldots+\alpha_1\cdot 2+\alpha_0.$$

Числа α_0, α_1,…, α_{n-1} называют *двоичными цифрами* числа x, а последовательность из нулей и единиц

$$\alpha_{n-1}\alpha_{n-2}\ldots\alpha_1\alpha_0$$

– *двоичной записью* числа x. Пишут также

$$x = (\alpha_{n-1}\alpha_{n-2}\ldots\alpha_1\alpha_0)_2.$$

Пример.

$$25=1+2\cdot 12=1+2\cdot(0+2\cdot 6)=1+2\cdot(0+2\cdot(0+2\cdot 3))=$$
$$=1+2\cdot(0+2\cdot(0+2\cdot(1+2\cdot 1)),$$

откуда

$$25=1\cdot 1+0\cdot 2+0\cdot 4+1\cdot 8+1\cdot 16.\square$$

Самое большое число, которое можно записать с помощью n двоичных цифр, содержит в свой двоичной записи одни единицы. Это число равно

$$2^{n-1}+2^{n-2}+\ldots+2+1=2^n-1.$$

Декартову степень $\{0,1\}^n$, $n\geq 1$, составляют всевозможные упорядоченные последовательности из нулей и единиц длины n. Мы будем называть такие последовательности n-мерными *двоичными векторами*.

Произвольному n-мерному двоичному вектору можно сопоставить неотрицательное целое число, двоичными цифрами которого служат компоненты вектора

$$(\alpha_1,\alpha_2,\ldots,\alpha_n)\to \alpha_1\cdot 2^{n-1}+\alpha_2\cdot 2^{n-2}+\ldots+\alpha_{n-1}\cdot 2+\alpha_n.$$

Этим устанавливается взаимно однозначное соответствие между множеством всех n-мерных двоичных векторов и множеством неотрицательных целых чисел, меньших 2^n. Таким образом, общее число n-мерных двоичных векторов равно 2^n, то есть $|\{0,1\}^n|=2^n$.

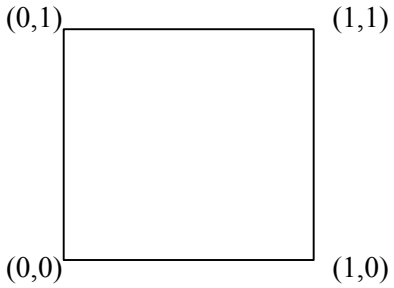
Пример. При $n=3$ имеем:

$$(0,0,0)\leftrightarrow 0;\qquad (0,0,1)\leftrightarrow 1;\qquad (0,1,0)\leftrightarrow 2;\qquad (0,1,1)\leftrightarrow 3;$$

$(1,0,0) \leftrightarrow 4$; $(1,0,1) \leftrightarrow 5$; $(1,1,0) \leftrightarrow 6$; $(1,1,1) \leftrightarrow 7$.□

Пусть $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ и $\beta=(\beta_1,\beta_2,\ldots,\beta_n)$ – двоичные векторы. Будем писать $\alpha\le\beta$ (или $\beta\ge\alpha$), если $\alpha_i\le\beta_i$ для всех i=1,2,…, n. Если $\alpha\le\beta$, но $\alpha\ne\beta$, будем писать $\alpha<\beta$ (последнее означает, что $\alpha_i.\le\beta_i$ для всех i=1,2,…, n, и при этом хотя бы одно из этих неравенств строгое). Заметим, что имеются векторы α и β, для которых неверно ни $\alpha\le\beta$, ни $\beta\le\alpha$. Такие векторы будем называть несравнимыми.

Примеры. Двумерные двоичные векторы можно рассматривать как вершины единичного квадрата в двумерном евклидовом пространстве:



Векторы α и β связаны отношением $\le$, если из вершины α можно пройти в вершину β по сторонам квадрата в направлении координатных осей (направо и вверх). Аналогично, трехмерные векторы соответствуют вершинам куба; векторы α и β связаны отношением $\le$, если из вершины α можно пройти в вершину β по ребрам куба в направлении координатных осей.□

5.2. Понятие булевой функции

Пусть $U=U(X_1,X_2,\ldots,X_n)$ – произвольная формула алгебры высказываний, содержащая n переменных. Оценка переменных такой формулы – это упорядоченная последовательность из 0 и 1 длины n, то есть n-мерный двоичный вектор. Каждой оценке переменных $(x_1,x_2,\ldots,x_n)\in\{0,1\}^n$ однозначным образом сопоставляется значение истинности $u\in\{0,1\}$ высказывания, полученного из формулы U после соответствующей подстановки. Таким образом, мы получаем соответствие $(x_1,x_2,\ldots,x_n)\to u$, задающее отображение f_U: $\{0,1\}^n\to\{0,1\}$, $u=f_U(x_1,x_2,\ldots,x_n)$. Такие отображения называют *булевыми функциями*. Непосредственно из определений вытекает, что формулы алгебры высказываний $U=U(X_1,X_2,\ldots,X_n)$ и $V=V(X_1,X_2,\ldots,X_n)$ равносильны в том и только том случае, когда функции f_U и f_V совпадают.

Булевы функции представляют интерес не только в связи с их «логическим» происхождением, но и сами по себе. Оттеняя это обстоятельство, введем следующие определения.

Переменные, пробегающие множество $\{0,1\}$, мы будем называть *булевыми* и обозначать буквами x, y, z, …, x_1, x_2, … . Функция от одной или нескольких булевых переменных, принимающая значение в множестве $\{0,1\}$, называется *булевой*.

Любую булеву функцию можно задать таблицей, подобной таблице истинности. Например, следующая таблица задает булеву функцию трех аргументов:

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Чтобы задать булеву функцию от трех переменных достаточно указать в подобной таблице произвольный столбец из 0 и 1 высоты 8 (по числу наборов значений аргументов), то есть двоичный вектор размерности 8. Число всевозможных таких столбцов равно 2^8. Значит, и число различных булевых функций от трех переменных конечно и составляет 2^8. В случае функций от n переменных число строк в таблице равно 2^n , такова же и высота столбца, определяющего функцию. Следовательно, число булевых функций от n переменных равно 2^{2^n}. С увеличением числа переменных количество булевых функций быстро нарастает. Так, число булевых функций от одной переменной равно 4, от двух переменных – 16, от трех – 256, от четырех – 65536 и т. д.

5.3. Булевы функции от одной и двух переменных

Булевы функции от одной переменной – это отображения множества $\{0,1\}$ в себя. Булевы функции от одной переменной можно рассматривать как унарные операции на множестве

{0,1}. В следующей таблице приведены все четыре булевы функции от одной переменной.

x	$g_0(x)$	$g_1(x)$	$g_2(x)$	$g_3(x)$
0	0	0	1	1
1	0	1	0	1

Имеем:

$g_0(x)=0$ – функция, тождественно равная 0 (тождественный ноль);

$g_1(x)=x$ – тождественная функция;

$g_2(x)=1–x$ – эта функция соответствует отрицанию и носит то же название; в теории булевых функций отрицание принято обозначать через x', поэтому мы будем писать $g_2(x)=x$';

$g_3(x)=1$ – функция, тождественно равная 1 (тождественная единица).

Булевы функции от двух переменных можно рассматривать как бинарные операции на множестве {0,1}. В следующей таблице приведены все шестнадцать булевых функции от двух переменных (значения аргументов и функций выписаны в строках, функции перечисляются в столбце). Для некоторых функций указаны используемые обозначения и названия.

x_1	0	0	1	1	
x_2	0	1	0	1	
---	---	---	---	---	---
f_0	0	0	0	0	0 – *тождественный ноль*
f_1	0	0	0	1	$\cdot$ *умножение, конъюнкция*
f_2	0	0	1	0	
f_3	0	0	1	1	x_1
f_4	0	1	0	0	
f_5	0	1	0	11	x_2
f_6	0	1	1	0	$\oplus$ – *сложение по модулю* 2
f_7	0	1	1	1	$\vee$ – *дизъюнкция*
f_8	1	0	0	0	$\downarrow$ – *стрелка Пирса*
f_9	1	0	0	1	$\leftrightarrow$ – *эквивалентность*
f_{10}	1	0	1	0	
f_{11}	1	0	1	1	$\leftarrow$ – *обратная импликация*
f_{12}	1	1	0	0	
f_{13}	1	1	0	1	$\rightarrow$ – *импликация*
f_{14}	1	1	1	0	$\mid$ – *штрих Шеффера*
f_{15}	1	1	1	1	1 – *тождественная единица*

Комбинируя перечисленные функции (с помощью суперпозиций), можно строить более сложные булевы функции, в том числе и большего числа переменных, например, $xy\rightarrow zt$ и т.п. Булевы отрицание, конъюнкция (умножение), дизъюнкция, импликация обладают свойствами, подобными тем, которыми обладают соответствующие логические операции (с естественной заменой равносильности формул на равенство функций). Например, *законы де Моргана* принимают следующий вид (знак умножения, как это часто делается, опущен):

$$(xy)'=x'\vee y'; \qquad (x\vee y)'=x'y'.$$

Кроме того, имеем:

$$1'=0; \qquad 0'=1;$$

$$x\vee x'=1; \qquad xx'=0;$$

$$0x=0; \qquad 1x=x; \qquad 0\vee x=x; \qquad 1\vee x=x.$$

Приведем некоторые уравнения, в которых одни булевы функции выражены через другие:

$$x' = x\to 0 = x|x = x\downarrow x = 1\oplus x;$$

$$xy = (x'\vee y')' = x'\downarrow y' = (x\downarrow x)\downarrow(y\downarrow y);$$

$$x\vee y = (x'y')' = x'\to y = =(x\to y)\to y = x'|y' = (x|x)|(y|y);$$

$$x\to y = x'\vee y;$$

$$x\leftrightarrow y = (x\to y)\,(y\to x) = xy\vee x'y';$$

$$x\oplus y = xy'\vee x'y.$$

Все эти равенства легко проверяются с помощью таблиц.

Принцип двойственности естественным образом переносится на булевы функции. Приведем необходимые формулировки. *Двойственной* к булевой функции $f(x,y,\ldots,z)$ называется функция

$$f^*(x,y,\ldots,z)=f'(x',y',\ldots,z').$$

Если $f(x,y,\ldots,z)$ представлена формулой, содержащей только конъюнкции, дизъюнкции и отрицания, то двойственная функция получается заменой в этой формуле конъюнкций на дизъюнкции, а дизъюнкций на конъюнкции.

5.4. ДНФ и КНФ

Существует простой способ дать аналитическое представление функции в виде формулы, содержащей конъюнкции, дизъюнкции и отрицания, используя ее табличное задание. Например, пусть функция от трех переменных задана следующей таблицей:

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Тогда

$$f(x,y,z) = x'y'z' \vee xy'z' \vee xyz.$$

Каждый из трех дизъюнктивных членов (слагаемых) записанной формулы соответствует набору значений аргументов, для которого функция принимает значение 1. Каждое слагаемое содержит все три аргумента функции; отрицанием снабжены те из них, которые имеют значение 0 в соответствующем наборе. Так, набору (0,0,0) соответствует слагаемое $x'y'z'$, набору (1,0,0) – слагаемое $xy'z'$, набору (1,1,1) – слагаемое xyz. Каждый из дизъюнктивных членов принимает значение 1 на своем наборе значений переменных и значение 0

– на всех остальных. Дизъюнкция этих трех слагаемых принимает значение 1 лишь тогда, когда значение 1 принимает хотя бы одно из слагаемых. Таким образом, функция в правой части записанного равенства принимает значение 1 на тех же трех наборах значений аргументов, что и функция f (на остальных наборах обе эти функции принимают значение 0). Тем самым справедливость равенства установлена.

Легко видеть, что описанный способ построения формулы по таблице применим к любой функции, не равной тождественно нулю. Получаемые при этом формулы называются *совершенными дизъюнктивными нормальными формами*, сокращенно СДНФ. Считается, что СДНФ тождественного нуля – это «пустая» дизъюнкция, не содержащая ни одного дизъюнктивного слагаемого.

Двойственная конструкция приводит к представлению функции в так называемой *совершенной конъюнктивной нормальной форме*, сокращенно СКНФ. СКНФ рассмотренной ранее функции имеет следующий вид:

$$f(x,y,z) = (x \vee y \vee z')(x \vee y' \vee z)(x \vee y' \vee z')(x' \vee y \vee z')(x' \vee y' \vee z).$$

Каждый из пяти конъюнктивных членов (множителей) соответствует набору значений аргументов, для которого функция принимает значение 0. Каждый множитель содержит все три аргумента функции; отрицанием снабжены те из них, которые имеют значение 1 в соответствующем наборе. Так, набору (0,0,1) соответствует множитель xyz', набору (0,1,0) –

множитель $xy'z$, и т. д. Каждый из конъюнктивных членов принимает значение 0 на своем наборе значений переменных и значение 1 – на всех остальных. Конъюнкция этих трех множителей принимает значение 0 лишь тогда, когда значение 0 принимает хотя бы один из множителей. Таким образом, функция в правой части записанного равенства принимает значение 0 на тех же трех наборах значений аргументов, что и функция f.

Описанный выше способ построения СДНФ и СКНФ опирается на следующую теорему о разложении функции по переменной.

Теорема. *Пусть* $f(x_1,x_2,\ldots,x_n)$ *– произвольная булева функция. Тогда*

$$f(x_1,x_2,\ldots,x_n) = x_1 \cdot f(1,x_2,\ldots,x_n) \vee x_1' \cdot f(0,x_2,\ldots,x_n);$$

$$f(x_1,x_2,\ldots,x_n) = (x_1 \vee f(0,x_2,\ldots,x_n))(x_1' \vee f(1,x_2,\ldots,x_n)).$$

Доказательство. Докажем первую формулу. Чтобы не загромождать выкладки индексами и многоточиями, ограничимся случаем функции от двух переменных. Доказываемая формула принимает следующий вид:

$$f(x,y) = x \cdot f(1,y) \vee x' \cdot f(0,y).$$

При любом y подстановка в правую часть x=1 и x=0 дает соответственно

$$1 \cdot f(1,y) \vee 1' \cdot f(0,y) = f(1,y) \vee 0 \cdot f(0,y) = f(1,y) \vee 0 \cdot = f(1,y);$$

$$0 \cdot f(1,y) \vee 0' \cdot f(0,y) = 0 \vee 1 \cdot f(0,y) = 1 \cdot f(0,y) = f(0,y).$$

Таким образом, левая и правая части доказываемого равенства совпадают на любом наборе значений аргументов. Следовательно, функции слева и справа от знака равенства равны. На общий случай доказательство распространяется практически без изменений. Достаточно считать, что y обозначает не одну переменную, а набор переменных. Второе равенство из формулировки теоремы доказывается аналогично (впрочем, его справедливость следует из принципа двойственности).□

Последовательно применяя несколько раз (по числу переменных) разложение из предыдущей теоремы, можно получить СДНФ булевой функции. Например,

$$f(x,y) = x\cdot f(1,y) \vee x'\cdot f(0,y) =$$
$$= x\cdot(y\cdot f(1,1) \vee y'\cdot f(1,0)) \vee x'\cdot(y\cdot f(1,1) \vee y'\cdot f(1,0)) =$$
$$= x\cdot y\cdot f(1,1) \vee x\cdot y'\cdot f(1,0) \vee x'\cdot y\cdot f(1,1) \vee x'\cdot y'\cdot f(1,0).$$

Функция $f(x,y)$ представлена в виде дизъюнкции четырех дизъюнктивных членов. Те из них, для которых коэффициент $f(\alpha,\beta)$ равен нулю, можно отбросить. В результате получится СДНФ. Например, для функции $f(x,y)=x\oplus y$ имеем $f(0,0)=f(1,1)=0$ и $f(0,1)=f(1,0)=1$, поэтому

$$x\oplus y=x\cdot y' \vee x'\cdot y.$$

Элементарной конъюнкцией (*конъюнктом*) называют конъюнкцию переменных и/или их отрицаний, в которой каждая переменная встречается не более одного раза.

Например, *x'yz*, *x'y* – конъюнкты. *Пустой конъюнкт* (в который не входит ни одна переменная) считается равным 1. *Дизъюнктивной нормальной формой* (сокращенно ДНФ) называется дизъюнкция конечного числа конъюнктов. Ясно, что любая СДНФ является ДНФ. Характеристический признак СДНФ – в каждый из ее конъюнктов входят все переменные. Например, *x'yz*∨*y'* – это ДНФ, не являющаяся совершенной. Представление булевой функции в виде СДНФ с точностью до порядка конъюнктов однозначно. При отказе от совершенности формы однозначность представления пропадает. Вообще говоря, одну и ту же булеву функцию можно представить разными способами в виде ДНФ.

Двойственным образом определяются *конъюнктивные нормальные формы* (КНФ). Элементарной дизъюнкцией (*дизъюнктом*) называют дизъюнкцию переменных и/или их отрицаний, в которой каждая переменная встречается не более одного раза. *Пустой дизъюнкт* считается равным 0. Конъюнктивной нормальной формой называется конъюнкция конечного числа дизъюнктов.

5.5. Полные системы булевых функций

Ранее было показано, что произвольная булева функция может быть выражена через конъюнкцию, дизъюнкцию и отрицание. Это означает, что конъюнкция, дизъюнкция и отрицание образуют *полную систему функций*. Вообще, система булевых функций называется *полной*, если любая булева

функция может быть выражена через функции этой системы с помощью суперпозиций.

Таким образом, в соответствии с определением система функций $\{\wedge, \vee, '\}$ полна. Поскольку дизъюнкцию можно выразить через конъюнкцию и отрицание, система функций $\{\wedge, '\}$ также полна. Точно так же полной является и система функций $\{\vee, '\}$, поскольку конъюнкцию можно выразить через дизъюнкцию и отрицание. Отрицание можно выразить через ноль и импликацию, дизъюнкцию – через импликацию и отрицание (см. п. 2.2). Следовательно, отрицание и импликация, ноль и импликация также образуют полные системы функций $\{', \rightarrow\}$, $\{0, \rightarrow\}$.

Через $\oplus$ и 1 можно выразить отрицание, так что система функций $\{1, \oplus, \cdot\}$ также является полной. Последнее означает, что любая булева функция может быть представлена в виде многочлена. При этом ненулевыми коэффициентами при одночленах служат единицы, а одночлены не содержат степеней переменных, поскольку умножение (конъюнкция) идемпотентна. Такие многочлены называют *полиномами Жегалкина.*

Пример. Вычислим полином Жегалкина для функции

$$f(x,y,z)=(x\rightarrow y)\vee(z\rightarrow y)$$

Имеем:

$$(x\rightarrow y)\vee(z\rightarrow y) = (x'\vee y)\vee(z'\vee y) = (xy')'\vee(zy')' =$$

$= (1 \oplus xy') \vee (1 \oplus zy') = (1 \oplus xy') \oplus (1 \oplus zy') \oplus (1 \oplus xy')\,(1 \oplus zy') =$

$= 1 \oplus xy' \oplus 1 \oplus zy' \oplus 1 \oplus xy' \oplus zy' \oplus xy'zy' =$

$= (1 \oplus 1) \oplus (xy' \oplus xy') \oplus (zy' \oplus zy') \oplus 1 \oplus xy'z =$

$= 0 \oplus 0 \oplus 0 \oplus 1 \oplus xy'z = 1 \oplus xy'z = 1 \oplus x(1 \oplus y)z = 1 \oplus xz \oplus xyz.$

При выводе использовались равенства $x'=1 \oplus x$, $x \oplus x=0$, $x \vee y=x \oplus y \oplus xy$ и др. (см. п. 3.2).□

Существуют полные системы, содержащие всего одну функцию. Отрицание и конъюнкцию можно выразить через стрелку Пирса (см. п. 3.2). Следовательно, стрелка Пирса составляет полную систему функций $\{\downarrow\}$. Точно так же отрицание и дизъюнкция выражаются через штрих Шеффера, так что $\{|\}$ – тоже полная система функций.

Мы видим, что установить полноту системы функций можно, показав, как через функции этой системы выражаются функции какой-нибудь системы, полнота которой уже известна. Доказательство неполноты может оказаться более изощренным.

Пример. Покажем что система функций $\{\cdot,\vee\}$ неполна. Действительно, отрицание нельзя выразить через дизъюнкцию и конъюнкцию. Допустим противное, то есть, что отрицание удалось представить в виде $x'=f(x,y,\ldots,z)$, и при этом функция f выражена через конъюнкции и дизъюнкции. Тогда

$$1=0'=f(0,y,\ldots,z) \qquad \text{и} \qquad 0=1'=f(1,y,\ldots,z).$$

Но конъюнкция и дизъюнкция монотонны по своим аргументам:

если $\alpha_1 \le \alpha_2$ и $\beta_1 \le \beta_2$ то $\alpha_1 \wedge \beta_1 \le \alpha_2 \wedge \beta_2$ и $\alpha_1 \vee \beta_1 \le \alpha_2 \vee \beta_2$.

Тем же свойством обладает и любая сложная функция, составленная из конъюнкции и дизъюнкции. Значит,

$$f(0,y,\ldots,z) \le f(1,y,\ldots,z),$$

что противоречит предполагаемому равенству.□

5.6. Важнейшие замкнутые классы булевых функций. Теорема Поста о полноте

Пусть $\boldsymbol{K}$ – некоторый класс булевых функций. *Замыканием* класса $\boldsymbol{K}$ называется множество всех тех функций, которые могут быть выражены через функции класса $\boldsymbol{K}$. Замыкание класса $\boldsymbol{K}$ будем обозначать через $[\boldsymbol{K}]$. Класс функций называется *замкнутым*, если он совпадает со своим замыканием.

Замыкание любой полной системы функций содержит все булевы функции. Для неполной системы функций это уже не так. В п. 3.4 было показано, что отрицание не входит в замыкание класса $\boldsymbol{K}=\{\wedge,\vee\}$.

Рассмотрим важнейшие замкнутые классы булевых функций.

Класс $\boldsymbol{P}_0$. Класс $\boldsymbol{P}_0$ – это *класс всех функций, сохраняющих* 0, то есть таких функций $f(x_1,x_2,\ldots,x_n)$, для которых $f(0,0,\ldots,0)=0$. В этот класс входят тождественная функция, конъюнкция, дизъюнкция, сложение по модулю 2; не входят тождественная единица, отрицание, импликация. Таблица для функции из

класса $\boldsymbol{P}_0$ в первой строке содержит 0, остальные значения могут быть какими угодно.

Класс $\boldsymbol{P}_1$. Класс $\boldsymbol{P}_1$ – это *класс всех функций, сохраняющих* 1, то есть таких функций $f(x_1,x_2,\ldots,x_n)$, для которых $f(1,1,\ldots,1)=1$. В этот класс (так же, как и в $\boldsymbol{P}_0$) входят тождественная функция, конъюнкция, дизъюнкция, сложение по модулю 2; импликация также входит в $\boldsymbol{P}_1$; тождественный ноль, отрицание в класс $\boldsymbol{P}_1$ не попадают.

Класс $\boldsymbol{S}$. Класс $\boldsymbol{S}$ – это *класс всех самодвойственных функций*, то есть таких функций f, которые совпадают со своей двойственной функцией, $f^*=f$. Простейшие примеры самодвойственных функций – x и x'. Функция $xy\vee xz\vee yz$ также самодвойственная:

$$(xy\vee xz\vee yz)^* = (x\vee y)(x\vee z)(y\vee z) = (x\vee xy\vee xz\vee yz)(y\vee z) =$$

$$= xy\vee xz\vee yz\vee xyz = xy\vee xz\vee yz.$$

Конъюнкция и дизъюнкция не самодвойственны.

В таблице самодвойственной функции значение в последней строке противоположно значению в первой строке, значение в предпоследней – значению во второй, и т.д.

Класс $\boldsymbol{L}$. Класс $\boldsymbol{L}$ – это *класс всех линейных функций*, то есть функций, представимых в виде

$$f(x_1,x_2,\ldots,x_n) = \alpha_1x_1\oplus\alpha_2x_2\oplus\ldots\oplus\alpha_nx_n,$$

где α_1, α_2, …, $\alpha_n\in\{0,1\}$ – константы. Функции x, $x'=1\oplus x$, $x\oplus y$ линейные; конъюнкция, дизъюнкция – нет.

Класс ***M***. Класс ***M*** – это *класс монотонных функций*. Функция $f(x_1,x_2,\ldots,x_n)$ называется монотонной, если $f(\alpha_1,\alpha_2,\ldots,\alpha_n)\le f(\beta_1,\beta_2,\ldots,\beta_n)$ при $(\alpha_1,\alpha_2,\ldots,\alpha_n)\le(\beta_1,\beta_2,\ldots,\beta_n)$. Конъюнкция, дизъюнкция монотонны; отрицание, импликация, сложение по модулю 2 – нет.

Теперь мы можем сформулировать один из важнейших результатов теории булевых функций – теорему Поста о полноте.

Теорема. *Класс функций* ***K*** *полон тогда и только тогда, когда он не содержится целиком ни в одном из перечисленных выше пяти классов* $\boldsymbol{P}_0$, $\boldsymbol{P}_1$, ***S***, ***L***, ***M***.□

Не приводя доказательства теоремы, поясним ее смысл. Как было показано, ни один из перечисленных пяти замкнутых классов не является полным (имеются не входящие в него булевы функции). Поэтому не может быть полным ни один класс функций, целиком содержащийся в одном из них. Имеются булевы функции, не входящие ни в один из классов $\boldsymbol{P}_0$, $\boldsymbol{P}_1$, ***S***, ***L***, ***M***. Любая такая функция в соответствии с теоремой составляет полную систему функций, то есть через эту функцию может быть выражена любая булева функция. Среди функций от двух переменных такими функциями являются стрелка Пирса и штрих Шеффера.

С помощью теоремы Поста можно установить полноту системы функций, не выписывая непосредственно выражения для булевых функций.

Пример. Покажем, что система функций $\{\rightarrow,\neg\}$ является полной. Составим таблицу, в которой символ 1 означает, что функция входит в соответствующий класс, а символ 0 – что не входит:

	P_0	P_1	S	L	M
$\rightarrow$	0	1	0	0	0
$\neg$	0	0	1	1	0

В каждом столбце таблицы имеется 0, значит, нет ни одного класса из пяти, который содержал бы обе функции. Следовательно, система функций $\{\rightarrow,\neg\}$ полна.□

6. Элементы теории кодирования

6.1. Двоичное кодирование

В информационных системах для двоичной записи целых чисел обычно используют фиксированное число двоичных разрядов (позиций для двоичных цифр) n. Если число имеет в своей записи $m \le n$ двоичных цифр, в первые $n-m$ позиций вписываются нули, а в оставшиеся m позиций цифры числа. Таким образом, используя n двоичных разрядов, можно представить все числа от 0 до 2^n-1.

Всякое сообщение, записанное с использованием символов некоторого алфавита, можно представить в виде некоторой последовательности из нулей и единиц. В самом деле, пусть $A=\{a,b,\ldots\}$ – конечный алфавит. Выберем число n так, чтобы 2^n было не меньше, чем число его символов. Перенумеруем символы алфавита (начиная нумерацию с нуля) и припишем каждому из них его двоичный код – двоичную запись номера символа с использованием n двоичных разрядов (битов). Текст $ab\ldots$, представляется последовательностью блоков

$$\alpha_{n-1}\alpha_{n-2}\ldots\alpha_1\alpha_0\beta_{n-1}\beta_{n-2}\ldots\beta_1\beta_0\ldots,$$

где $\alpha_{n-1}\alpha_{n-2}\ldots\alpha_1\alpha_0$ – двоичная запись номера символа a, $\beta_{n-1}\beta_{n-2}\ldots\beta_1\beta_0$ – двоичная запись номера символа b, и т.д.

В информатике распространены системы кодирования символов алфавита с использованием 8-разрядных блоков –

байтов. Это позволяет работать с алфавитами, содержащими до 256 символов. Обычно используемые алфавиты содержат латинские буквы, буквы национального алфавита, цифры, знаки препинания и некоторые специальные знаки.

6.2. Векторное пространство $\{0,1\}^n$

На множестве n-мерных двоичных векторов определим операцию $\oplus$ – сложение по модулю 2. Сумма двоичных векторов $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ и $\beta=(\beta_1,\beta_2,\ldots,\beta_n)$ определяется формулой

$$\alpha\oplus\beta = (\alpha_1\oplus\beta_1, \alpha_1\oplus\beta_1,\ldots, \alpha_n\oplus\beta_n).$$

Вектор $\alpha\oplus\beta$ содержит единицы на тех местах, где координаты векторов α и β различаются, и нули – на тех, где совпадают.

Примеры. $(0,1,0,1)\oplus(0,0,1,1) = (0,1,1,0)$;

$(0,1,0,1)\oplus(1,1,1,1) = (1,0,1,0)$;

$(0,1,0,1)\oplus(0,1,0,1) = (0,0,0,0)$.□

Операция $\oplus$ обладает важными свойствами обычного сложения: она коммутативна и ассоциативна, нулевой вектор является нейтральным элементом. Кроме того, $\alpha\oplus\alpha$ является нулевым вектором для любого вектора α.

Система n-мерных двоичных векторов *линейно зависима*, если сумма (по модулю 2) нескольких векторов из этой системы равна 0 (мы используем один и тот же символ «0» для обозначения числа «ноль» и нулевого вектора, когда из контекста ясно, о чем идет речь). На двоичные векторы

распространяются стандартные свойства линейной зависимости:

в пространстве $\{0,1\}^n$ *любая система, содержащая более n векторов, линейно зависима*;

любые n линейно независимых векторов образуют базис пространства $\{0,1\}^n$; *всякий вектор из* $\{0,1\}^n$ *может быть единственным образом представлен в виде суммы нескольких базисных векторов*.

Двоичные векторы (0,0,…,0,1), (0,0,…,1,0),…, (1,0,…,0,0) образуют базис пространства $\{0,1\}^n$, называемый *каноническим*.

Число единичных координат двоичного вектора $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ обозначают через $w(\alpha)$ и называют *весом* вектора α. Очевидно,

$$w(\alpha) = \alpha_1+\alpha_2+\ldots+\alpha_n.$$

Формулой

$$d(\alpha,\beta) = w(\alpha\oplus\beta)$$

определяется расстояние $d(\alpha,\beta)$ между двоичными векторами α и β, называемое *расстоянием Хемминга*. Расстояние Хемминга обладает следующими свойствами:

1) $d(\alpha,\alpha)=0$ *и* $d(\alpha,\beta)>0$ при $\alpha\neq\beta$;

2) $d(\alpha,\beta)=d(\beta,\alpha)$;

3) $d(\alpha,\beta)+d(\beta,\gamma)\geq d(\alpha,\gamma)$ (*неравенство треугольника*).

6.3. Отображения $\{0,1\}^n$ в $\{0,1\}^m$

Произвольное отображение из $\{0,1\}^n$ в $\{0,1\}^m$,

$$(x_1,x_2,\ldots,x_n) \to (y_1,y_2,\ldots,y_m),$$

задается набором булевых функций

$$y_1=f_1(x_1,x_2,\ldots,x_n),\ y_2=f_2(x_1,x_2,\ldots,x_n),\ \ldots,\ y_m=f_m(x_1,x_2,\ldots,x_n).$$

Чтобы задать такое отображение, требуется указать m двоичных векторов размерности 2^n. Таким образом, для задания произвольного отображения необходимо $m\times 2^n$ бит информации. Например, отображение из $\{0,1\}^2$ в $\{0,1\}^3$ задается вектором размерности 12 (составленным из трех векторов размерности 4). Общее число отображений из $\{0,1\}^2$ в $\{0,1\}^3$ равно $2^{12}=4096$.

Напомним, что линейной называется функция вида

$$f(x_1,x_2,\ldots,x_n) = c_1x_1 \oplus c_2x_2 \oplus \ldots \oplus c_nx_n,$$

где $c=(c_1,c_2,\ldots,c_n)$ – произвольный двоичный вектор.

Булева функция $f:\{0,1\}^n \to \{0,1\}$ *является линейной, если*

$$f(\alpha\oplus\beta)=f(\alpha)\oplus f(\beta)$$

для любых α *и* β *из* $\{0,1\}^n$.

В самом деле, так как

$$(x_1,x_2,\ldots,x_n) = x_1\cdot(1,0,\ldots,0) \oplus x_2\cdot(0,1,\ldots,0)\oplus\ldots\oplus x_n\cdot(0,0,\ldots,1),$$

то

$$f(x_1,x_2,\ldots,x_n) = x_1\cdot f(1,0,\ldots,0) \oplus x_2\cdot f(0,1,\ldots,0)\oplus\ldots\oplus x_n\cdot f(0,0,\ldots,1).$$

Вектор $c=(c_1,c_2,\ldots,c_n)$ имеет следующий вид:

$$c_1 = f(1,0,\ldots,0),\ c_2= f(0,1,\ldots,0),\ \ldots,\ c_n= f(0,0,\ldots,1).$$

Общее число линейных функций от n переменных равно числу n-мерных двоичных векторов, то есть равно 2^n.

Как видно из предыдущего, линейная функция f является суммой нескольких своих аргументов. Например, x_1 входит слагаемым в эту сумму, если $f(1,0,\ldots,0)=1$, и не входит, если $f(1,0,\ldots,0)=0$.

Пример. Перечислим все линейные функции $y=f(x_1,x_2,x_3)$ от трех переменных:

$$y=0 \text{ (тождественный 0)}; \; y=x_1; \; y=x_2; \; y=x_3;$$

$$y=x_1\oplus x_2; \; y=x_1\oplus x_3; \; y=x_2\oplus x_3; \; y=x_1\oplus x_2\oplus x_3.\square$$

Отображение $f:\{0,1\}^n \to \{0,1\}^m$ называется *линейным*, если $f(\alpha\oplus\beta)=f(\alpha)\oplus f(\beta)$ для любых α и β из $\{0,1\}^n$. Отображение

$$f:\{0,1\}^n \to \{0,1\}^m, \; (x_1,x_2,\ldots,x_n) \to (y_1,y_2,\ldots,y_m),$$

линейно тогда и только тогда, когда линейны все его компоненты

$$y_1=f_1(x_1,x_2,\ldots,x_n), \; y_2=f_2(x_1,x_2,\ldots,x_n), \ldots, \; y_m=f_m(x_1,x_2,\ldots,x_n).$$

Отсюда следует, что линейное отображение из $\{0,1\}^n$ в $\{0,1\}^m$ однозначно определяется набором, содержащим m двоичных векторов размерности n, то есть некоторой матрицей из нулей и единиц размера $m\times n$. Для задания линейного отображения необходимо $m\times n$ бит информации. Общее число линейных функций из $\{0,1\}^n$ в $\{0,1\}^m$ равно 2^{mn}.

Пример. Рассмотрим линейное отображение f из $\{0,1\}^2$ в $\{0,1\}^3$. Задать его можно, указав матрицу из нулей и единиц (c_{ij}), $i=1,2,3$, $j=1,2$:

$$y_1=c_{11}x_1\oplus c_{12}x_2, \; y_2=c_{21}x_1\oplus c_{22}x_2, \; y_3=c_{31}x_1\oplus c_{32}x_2.$$

Пусть, например,

$$y_1=x_1,\ y_2=x_2,\ y_3=x_1\oplus x_2.$$

Тогда

$$c_{11}=1,\ c_{12}=0,\ c_{21}=0,\ c_{22}=1,\ c_{31}=1,\ c_{32}=1.\square$$

Следующая таблица дает некоторое представление о росте объема информации, необходимой для задания произвольных и линейных отображений из $\{0,1\}^n$ в $\{0,1\}^m$.

		Задание отображения из $\{0,1\}^n$ в $\{0,1\}^m$ (бит)	
n	m	произвольное	линейное
1	1	2	1
1	2	4	2
2	2	8	4
2	3	12	6
3	4	32	12
8	9	2304	72
15	20	655360	300

6.4. Блочные двоичные коды

При передаче информации в каналах связи возможно появление помех. Передаваемые сигналы могут искажаться. Чтобы обеспечить надежную передачу информации, применяют различные методы кодирования информации. Вместе с основной информацией пересылают некоторую дополнительную, позволяющую судить об искаженности принятых сообщений. Коды делятся на два больших класса: коды с обнаружением ошибок и коды с исправлением ошибок.

Пример. *Код, обнаруживающий одиночные ошибки*. Пусть сообщения, предназначенные для передачи, представляются двоичными векторами размерности 4. Произвольное сообщение α имеет вид $\alpha=(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\in\{0,1\}^4$. Перед тем как сообщение α будет передано, его кодируют, добавляя бит проверки на четность:

$$E(\alpha)=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_1\oplus\alpha_2\oplus\alpha_3\oplus\alpha_4)\in\{0,1\}^5.$$

По каналу связи пересылается сообщение $E(\alpha)$. В пересылаемом сообщение число единичных битов четно:

$$\alpha_1\oplus\alpha_2\oplus\alpha_3\oplus\alpha_4\oplus(\alpha_1\oplus\alpha_2\oplus\alpha_3\oplus\alpha_4)=0.$$

Предположим, что при пересылке ошибка может произойти не более, чем в одном бите. Пусть $\beta=(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5)$ – принятое сообщение. Тогда, если ошибка произошла, то $\beta_1\oplus\beta_2\oplus\beta_3\oplus\beta_4\oplus\beta_5=1$, если нет – $\beta_1\oplus\beta_2\oplus\beta_3\oplus\beta_4\oplus\beta_5=0$.□

Пример. *Код Хемминга, исправляющий одиночные ошибки*. Сообщение $\alpha=(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ при кодировании дополняется тремя битами:

$$E(\alpha)=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7),$$

где

$$\alpha_5=\alpha_2\oplus\alpha_3\oplus\alpha_4;$$

$$\alpha_6=\alpha_1\oplus\alpha_3\oplus\alpha_4;$$

$$\alpha_7=\alpha_1\oplus\alpha_2\oplus\alpha_4.$$

Сообщение $E(\alpha)\in\{0,1\}^7$ передается по каналам связи. Пусть $\beta=(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7)$ – принятое сообщение. Вычислим следующие суммы:

$$\sigma_1=\beta_4\oplus\beta_5\oplus\beta_6\oplus\beta_7;$$

$$\sigma_2=\beta_2\oplus\beta_3\oplus\beta_6\oplus\beta_7;$$

$$\sigma_3=\beta_1\oplus\beta_3\oplus\beta_5\oplus\beta_7.$$

Если сообщение передано без ошибки, то все три суммы нулевые. В самом деле, при безошибочной передаче $\beta_i=\alpha_i$ для i=1,2,…,7. Легко видеть, что после замены α_5, α_6, α_7 их выражениями через α_1, α_2, α_3 и α_4, каждая из сумм σ_1, σ_2, σ_3 содержит четное число слагаемых α_i , i=1,2,3,4, и потому равна 0. Верно и обратное. Если все три суммы нулевые, сообщение передано без ошибки. В противном случае число j, $1\le j\le 7$, с двоичной записью $\sigma_1\sigma_2\sigma_3$ указывает номер позиции, в которой произошла ошибка. Пусть, например, ошибка произошла в первой позиции. Тогда $\beta_1=1\oplus\alpha_1$ и $\beta_i=\alpha_i$ при i=2,3,…,7. Имеем

$$\sigma_3 = 1\oplus\alpha_1\oplus\alpha_3\oplus\alpha_5\oplus\alpha_7 =$$

$$= 1\oplus\alpha_1\oplus\alpha_3\oplus(\alpha_2\oplus\alpha_3\oplus\alpha_4)\oplus(\alpha_1\oplus\alpha_2\oplus\alpha_4) = 1.$$

Так как в вычислении σ_1 и σ_2 ошибочный бит не участвует, то эти суммы равны 0. Значит, $j=001_2=1$.

Для исправления ошибки в принятом сообщении β, нужно заменить β_j на $1\oplus\beta_j$ и отбросить последние три бита. Первые

четыре бита исправленного сообщения дают исходное сообщение α. Этот алгоритм реализует функцию декодирования $\alpha = D(\beta)$.□

В общем случае (n,m)-*блочный двоичный код* определяется двумя функциями: функцией кодирования $E: \{0,1\}^n \to \{0,1\}^m$ и функцией декодирования $D: \{0,1\}^m \to \{0,1\}^n$, где $m \le n$. Векторы вида $E(\alpha) \in \{0,1\}^m$ называются кодовыми словами. Интуитивно ясно, что код тем лучше приспособлен к обнаружению и исправлению ошибок, чем больше различаются его кодовые слова.

Кодовым расстоянием блочного двоичного кода называется величина $d(E)$, равная наименьшему расстояние между различными кодовыми словами:

$$d(E) = \min\{d(E(\alpha),E(\beta)) \mid \alpha, \beta \in \{0,1\}^m, \alpha \neq \beta\}.$$

Пример. Вычислим кодовое расстояние для (4,5)-кода с проверкой на четность. Имеется 16 кодовых слов:

00000;	00011;	00101;	00110;
01001;	01010;	01100;	01111;
10001;	10010;	10100;	10111;
11000;	11011;	11101;	11110.

Нетрудно проверить, что нет ни одной пары кодовых слов, для которых расстояние равнялось бы 1. В то же время имеются кодовые слова, расстояние между которыми равно 2.

Следовательно, кодовое расстояние для рассматриваемого кода равно 2.□

Пример. Найдем кодовое расстояние для рассмотренного ранее (4,7)-кода Хемминга. Имеется 16 кодовых слов (проверочные биты записаны через пробел):

0000 000; 0001 111; 0010 110; 0011 001;

0100 101; 0101 010; 0110 011; 0111 100;

1000 011; 1001 100; 1010 101; 1011 010;

1100 110; 1101 001; 1110 000; 1111 111.

Легко обнаружить кодовые слова, расстояние между которыми равно 3. Несколько сложнее проверяется, что кодовых слов, расстояние между которыми равно 2 или 1, нет. Значит, кодовое расстояние рассматриваемого кода равно 3.□

Теорема. 1) *Код позволяет обнаруживать ошибки в k* (*или менее*) *позициях тогда и только тогда*, *когда его кодовое расстояние превышает k*.

2) *Код позволяет обнаруживать и исправлять ошибки в k* (*или менее*) *позициях тогда и только тогда*, *когда его кодовое расстояние превышает* 2*k*.

Доказательство. Мы ограничимся доказательством второй части теоремы. Первая доказывается аналогично.

Необходимость. Предположим, что кодовое расстояние меньше, чем 2*k*. Тогда найдутся два слова α и γ такие, что $d = d(E(\alpha), E(\gamma)) \le 2k$. В слове $E(\alpha) \oplus E(\gamma)$ заменим часть единиц

нулями: $d/2$ единиц, если d четно, и $(d-1)/2$ единиц, если d нечетно, и обозначим полученное так слово через δ. Заметим, что

$$w(\delta)\le k \text{ и } w(\delta\oplus E(\alpha)\oplus E(\gamma)) \le k.$$

Положим $\beta=E(\alpha)\oplus\delta$. Тогда

$$d(E(\alpha),\beta) = w(E(\alpha)\oplus E(\alpha)\oplus\delta) = w(\delta) \le k,$$

$$d(E(\gamma),\beta) = w(E(\gamma)\oplus E(\alpha)\oplus\delta) \le k.$$

Следовательно, слово β может появиться в результате ошибочной передачи (с числом ошибок, не превосходящим k) как слова α, так и слова β. Такую ошибку исправить невозможно.

Достаточность. Предположим, что при передаче слова $E(\alpha)$ ошибки произошли в $r\le k$ битах и на выходе было получено слово β. Поскольку $E(\alpha)\oplus\beta$ – вектор ошибок, то

$$d(E(\alpha),\beta) = w(E(\alpha)\oplus\beta) = r.$$

Так как кодовое расстояние превышает $2k$, то для произвольного кодового слова $E(\gamma)$, отличного от $E(\alpha)$, имеем $d(E(\alpha),E(\gamma))>2k$. Используя неравенство треугольника, получаем

$$d(E(\alpha),\beta) + d(\beta,E(\gamma)) \ge d(E(\alpha),E(\gamma)) > 2k,$$

$$d(\beta,E(\gamma)) \ge 2k - d(E(\alpha),\beta) = 2k-r > k.$$

Следовательно, слово β может получиться при передаче слова $E(\gamma)$ только в том случае, когда сделано более k ошибок. Это позволяет по слову β однозначным образом восстановить

$E(\alpha)$ как ближайшее к нему кодовое слово, единственное, которое может привести к появлению слова β в результате не более, чем k ошибок.□

6.5. Коды Хемминга

Начнем с нескольких определений и конструкций общего характера.

Если функция кодирования блочного кода $E:\{0,1\}^n \to \{0,1\}^m$ линейна, то код называется *линейным*. В дальнейшем мы рассматриваем только линейные коды. Назовем *проверочным* такое линейное отображение $S:\{0,1\}^m \to \{0,1\}^k$, что $S(\beta)=0$ тогда и только тогда, когда β является кодовым словом. Для произвольного $\beta \in \{0,1\}^m$ вектор $S(\beta)$ называется *синдромом*. Нулевой синдром имеют кодовые слова, и только они.

Предположим, что в зашумленном канале передаваемое кодовое слово $E(\alpha)$ исказилось, к нему добавился вектор ошибок δ, так что на выходе принято слово $\beta=\delta \oplus E(\alpha)$. Тогда

$$S(\beta)=S(\delta \oplus E(\alpha))=S(\delta) \oplus S(E(\alpha))=S(\delta).$$

Для того чтобы правильно декодировать передаваемое сообщение, нужно уметь определять вектор ошибок по его синдрому. Если вектор ошибок определен, то исправить их несложно: $E(\alpha)=\delta \oplus \beta$. Ограничившись случаем одиночных ошибок, можно привести сравнительно несложное построение кода, исправляющего ошибки.

Вектор одиночной ошибки имеет всего одну ненулевую координату, то есть является одним из векторов канонического базиса пространства $\{0,1\}^m$. Линейный код позволяет исправлять все одиночные ошибки тогда и только тогда, когда синдромы всех векторов из канонического базиса пространства $\{0,1\}^m$ отличны от нуля и друг от друга. Поскольку пространство $\{0,1\}^k$ содержит всего 2^k-1 ненулевых векторов, используя проверочное отображение $S:\{0,1\}^m\to\{0,1\}^k$, можно исправлять одиночные ошибки лишь в том случае, когда длины кодовых слов ограничены числом 2^k-1, то есть $m\le 2^k-1$. Оказывается, что можно построить коды с исправлением ошибок, в которых $m=2^k-1$. В таких кодах их «исправляющие» возможности используются с максимальной эффективностью. К их числу относятся рассматриваемые ниже коды Хемминга.

Перейдем к описанию кода Хемминга. Пусть $m=2^k-1$. Среди m позиций кодового слова k позиций являются контрольными, а $n = 2^k-k-1$ – информационными. Матрица H (размерности $k\times(2^k-1)$), задающая проверочное отображение, содержит в качестве столбцов все ненулевые векторы пространства $\{0,1\}^k$. Порядок столбцов не важен, но технически удобнее считать, что в каждом столбце записан его номер в двоичном формате. Строки матрицы H определяют коэффициенты системы из k однородных линейных уравнений с 2^k-1 неизвестными. Множество кодовых слов совпадает с множеством решений этой системы. Выражая последние k неизвестных через первые

2^k–k–1, мы получаем уравнения для вычисления контрольных битов. Вектор с нулевым синдромом является кодовым и его декодирование сводится просто к отбрасыванию контрольных битов. Если синдром отличен от нуля, он представляет собой двоичную запись номера позиции, в которой произошла ошибка. В этом случае при декодировании ошибка исправляется. Доля информационных позиций в коде Хемминга составляет

$$\frac{2^k - k - 1}{2^k - 1} = 1 - \frac{k}{2^k - 1}$$

и стремится к 1 с ростом k.

Пример. Рассмотрим случай k=3, m=7, n=4. Проверочное отображение S задается следующей матрицей:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Столбцы матрицы представляют собой образы векторов канонического базиса пространства $\{0,1\}^7$ относительно S. Для произвольного вектора $\beta=(\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7)$ синдром $S(\beta)=(\sigma_1,\sigma_2,\sigma_3)$ определяется уравнениями

$$\sigma_1=\beta_4\oplus\beta_5\oplus\beta_6\oplus\beta_7;$$

$$\sigma_2=\beta_2\oplus\beta_3\oplus\beta_6\oplus\beta_7;$$

$$\sigma_3=\beta_1\oplus\beta_3\oplus\beta_5\oplus\beta_7.$$

Кодовое слово $S(\alpha)=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7)$ должно удовлетворять системе уравнений

$$\alpha_4\oplus\alpha_5\oplus\alpha_6\oplus\alpha_7=0;$$

$$\alpha_2\oplus\alpha_3\oplus\alpha_6\oplus\alpha_7=0;$$

$$\alpha_1\oplus\alpha_3\oplus\alpha_5\oplus\alpha_7=0.$$

Решив эту систему относительно α_5, α_6, α_7, можно найти уравнения, задающие контрольные биты. Сложив первые два уравнения, получаем

$$\alpha_2\oplus\alpha_3\oplus\alpha_4\oplus\alpha_5=0,$$

откуда

$$\alpha_5=\alpha_2\oplus\alpha_3\oplus\alpha_4.$$

Подставив выражение для α_5 в третье уравнение системы, получаем

$$\alpha_7=\alpha_1\oplus\alpha_2\oplus\alpha_4.$$

Теперь подставляем выражение для α_7 во второе уравнение системы и находим

$$\alpha_6=\alpha_1\oplus\alpha_3\oplus\alpha_4.\square$$

7. Функции выбора и их логическая форма

7.1. Понятие функции выбора

В основе многих экономических моделей (потребительского спроса, конкурентного рынка и др.) лежит предположение о том, каким образом осуществляется выбор «лучших» вариантов из числа предложенных.

Рассмотрим следующую предельно упрощенную модель потребительского выбора товара. На складе имеется фиксированный набор штучных товаров Ω. Потребителю доступна совокупность товаров (ассортимент) $X \subset \Omega$, из которой он выбирает для себя любой товар (или набор товаров).

Разберем две ситуации, связанные с таким выбором. В первом случае каждый товар $x \in \Omega$ снабжен ярлыком с указанием определяющей для потребителя характеристики товара в виде числа $f(x)$. Потребитель выбирает товар, у которого эта характеристика имеет наибольшее значение. Во втором случае товары не снабжены ярлыками с указанием их ценности для потребителя. Потребитель, тем не менее, сравнивая товары, выбирает те, которые ему нравятся больше. Моделируя выбор потребителя, можно предположить, что потребитель неявным образом приписывает каждому товару некоторое число – оценку его полезности. Возникает естественный вопрос, какими свойствами должен обладать

выбор потребителя, чтобы такая модель была адекватной (правильно описывала потребительский выбор).

Возможны и другие модели, например, связанные с приписыванием товару нескольких числовых оценок его качеств и т.п. Чтобы, наблюдая поведение потребителя, предвидеть, что он выберет из нового ассортимента, нужно понять общие закономерности выбора и скрытую логику мотивации потребителя. Математическим аппаратом для изучения выбора в подобных и иных ситуациях служат функции выбора.

Пусть задано *множество вариантов* (или, как еще говорят, альтернатив) Ω. В содержательных задачах это может быть множество товаров, проектов, планов, стратегий и т.п. Будем считать, что Ω – конечное множество, содержащее не менее двух элементов. Подмножества множества Ω будем называть *предъявлениями*. Если предъявлено множество $X \subset \Omega$, то выбор из него состоит в указании множества выбранных вариантов $Y \subset X$. В случае, когда выбор пуст, $Y=\varnothing$, будем также говорить об отказе от выбора. *Функцией выбора* называется отображение C: $2^{\Omega} \to 2^{\Omega}$ такое, что $C(X) \subset X$ для всех $X \subset \Omega$. Содержательно, $C(X)$ – это множество вариантов, выбранных из предъявленного множества вариантов X. Выбор называют единичным, если из любого предъявления выбирается ровно один элемент, то есть любое множество $C(X)$ содержит ровно один элемент. Выбор

называют множественным, если хотя бы одно множество $C(X)$ содержит более одного элемента.

В некоторых случаях удобно считать, что не все предъявления допустимы. Тогда выделяется множество допустимых предъявлений, а под функцией выбора понимается отображение этого множества в 2^{Ω}. В дальнейшем, говоря о множестве предъявлений, мы обычно будем считать, что оно содержит все возможные предъявления; случаи, когда это не так, будут оговариваться специально. Впрочем, как правило, предположение о допустимости всех предъявлений несущественно, и нет нужды уточнять, совпадает ли множество допустимых предъявлений со всем множеством 2^{Ω} или является его собственной частью.

7.2. Примеры функций выбора

1. *Выбор по скалярному критерию*.

На множестве вариантов Ω определена функция $f:\Omega\to\boldsymbol{R}$ – скалярный критерий. Из предъявленного множества вариантов $X\subset\Omega$ выбираются те, для которых критерий имеет максимальное значение:

$$C(X)=\{x\in X \mid \forall x'\in X\, f(x)\geq f(x')\}.$$

Если функция $f(x)$ принимает в точке x свое максимальное значение, принято писать $x = \arg\max f(x)$. С использованием этого обозначения предыдущую формулу можно переписать так:

$$C(X)=\{x\in X \mid x = \arg\max f(x)\}.$$

2. *Выбор по Парето*.

На множестве вариантов Ω задан набор критериев $f_i(x)$, i=1,2,…,m. Сопоставляя каждому варианту x вектор

$$f(x) = (f_1(x), f_2(x), \ldots, f_m(x)),$$

получаем отображение $f:\Omega\to\boldsymbol{R}^m$, называемое векторным критерием. Будем говорить, что y предпочтительнее x, и писать $f(x)<f(y)$, если $f_1(x)\leq f_1(x)$, $f_2(x))\leq f_2(y)$, … $f_m(x)\leq f_m(y)$, причем хотя бы одно из неравенств строгое. Из предъявленного множества вариантов X выбираются те, для которых в X отсутствуют более предпочтительные варианты:

$$C(X) = \{x\in X \mid \neg(\exists y\in X\, f(x)<f(y))\}.$$

3. *Турнирный выбор*.

На множестве

$$\Omega\times\Omega = \{(x,y) \mid x, y\in\Omega\}$$

задана функция $f(x,y)$, принимающая значения 0; 1 и 2, такая, что $f(x,y)+f(y,x)=2$ для любых $x,y\in\Omega$, $x\neq y$. Кроме того, мы считаем, что $f(x,x)=0$ для любого x. Можно считать, что функция $f(x,y)$ представлена в виде турнирной таблицы, в которой значение $f(x,y)$ располагается в строке x и столбце y. При $x\neq y$ значение 2 соответствует победе (x над y), значение 0 – поражению, значение 1 – ничьей. Из предъявляемого множества вариантов X выбираются «победители» турнира, то есть

варианты, набравшие максимальное число очков. Более точно, для $X \subset \Omega$ и $x \in X$ пусть

$$h_X(x) = \sum_{y \in X} f(x,y)$$

– число очков, набранных вариантом x. Тогда

$$C(X) = \{x \in X \mid x = \arg\max h_X(x)\}.$$

Примеры 1 и 2 иллюстрируют общие способы построения функции выбора по отношению, заданному на множестве вариантов, которые мы рассмотрим ниже.

Пусть R – бинарное отношение на множестве вариантов Ω. Будем писать xRy, если $(x,y) \in R$. Для $X \subset \Omega$ положим

$$C_R(X) = \{x \in X \mid \forall y \in X \; xRy\};$$

$$C^R(X) = \{x \in X \mid \forall y \in X \; \neg(yRx)\}.$$

В случае скалярного критерия $f: \Omega \to R$ полагаем xRy, если $f(x) \geq f(y)$. Тогда $C_R(X)$ – это выбор по скалярному критерию. В случае векторного критерия $f: \Omega \to R^m$ полагаем yRx, если $f(x) < f(y)$ (y не хуже, чем x по любому критерию, а по одному из них превосходит x). Тогда, по закону де Моргана для предикатов, $C^R(X)$ – это выбор по Парето.

Между функциями вида $C_R(X)$ и $C^R(X)$ имеется тесная связь. Чтобы ее описать, введем понятие двойственного отношения. Пусть R – произвольное бинарное отношение на Ω. Двойственное к R отношение R^d определяется формулой

$$R^d = \overline{R^{-1}}.$$

Таким образом,

$$xR^d y \Leftrightarrow \neg yRx.$$

Например, если R – это отношение нестрогого порядка $\leq$ на множестве действительных чисел, то R^d – это отношение строгого порядка $>$:

$$x>y \Leftrightarrow \neg(y\leq x).$$

Ясно, что

$$R^{dd}=R.$$

Из формул де Моргана следует, что

$$(R\cap S)^d=R^d\cup S^d\ ,\ (R\cup S)^d=R^d\cap S^d.$$

Непосредственно из определений вытекает, что

$$C^R(X)=C_{R^d}(X);\ C_R(X)=C^{R^d}(X).$$

Функцию выбора C^R называют *функцией блокировки* по отношению R. Функции выбора вида C^R будем называть *нормальными*. Поскольку любая функция выбора вида C_R является функцией блокировки по двойственному отношению, любая такая функция нормальна.

Не все функции выбора нормальны.

Пример. Рассмотрим следующую функцию выбора на двухэлементном множестве $\Omega=\{x,y\}$:

$$C(\{x\})=\{x\};\ C(\{y\})=\varnothing;\ C(\{x,y\})=\{y\}.$$

Покажем, что она не является нормальной. Предположим противное, то есть, что $C=C^R$ – это функция блокировки по

некоторому отношению R. Так как $C(\{y\})=\varnothing$, то yRy. Но $y\in C(\{x,y\})$ означает, что $(\neg xRy)\wedge(\neg yRy)$, откуда $\neg yRy$. Полученное противоречие показывает, что предположение о нормальности функции неверно.□

7.3. Характеристические векторы подмножеств конечного множества

Пусть U – конечное множество и $n=|U|$ – число его элементов. Занумеруем элементы множества U числами от 1 до n и будем обозначать элементы их номерами, полагая, что $U=\{1, 2, \ldots, n\}$.

Всякое подмножество $X\subset U$ может быть описано двоичным вектором $\xi = (\xi_1,\xi_2,\ldots,\xi_n)\in\{0,1\}^n$, в котором $\xi_i=1$, если $i\in X$, и $\xi_i=0$, если $i\notin X$. По существу, это представление подмножества его характеристической функцией. Такой вектор будем называть *характеристическим*. Обратно, каждый двоичный вектор $\xi=(\xi_1,\xi_2,\ldots,\xi_n)$ может рассматриваться как характеристический вектор соответствующего подмножества X:

$$i\in X \Leftrightarrow \xi_i=1.$$

Пустому множеству соответствует нулевой вектор; характеристический вектор множества U состоит из одних единиц. Очевидно, число элементов множества X равно весу его характеристического вектора ξ, $|X|=w(\xi)$.

Пример. Пусть $U=\{1,2,3\}$. Тогда

$\varnothing\leftrightarrow(0,0,0)$; $\{1\}\leftrightarrow(1,0,0)$; $\{2\}\leftrightarrow(0,1,0)$; $\{3\}\leftrightarrow(0,0,1)$;

$\{1,2\}\leftrightarrow(1,1,0)$; $\{1,3\}\leftrightarrow(1,0,1)$; $\{2,3\}\leftrightarrow(0,1,1)$; $\{1,2,3\}\leftrightarrow(1,1,1)$.

□

Пусть $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ и $\beta=(\beta_1,\beta_2,\ldots,\beta_n)$ – двоичные векторы. Мы пишем $\alpha\le\beta$ (или $\beta\ge\alpha$), если $\alpha_i\le\beta_i$ для всех $i=1,2,\ldots, n$.

Определим на множестве векторов операции конъюнкции и дизъюнкции, выполняя их покоординатно. Например, для дизъюнкции имеем:

$$\alpha\vee\beta = (\alpha_1\vee\beta_1, \alpha_2\vee\beta_2, \ldots, \alpha_n\vee\beta_n).$$

Очевидно, $\alpha\le\beta$ тогда и только тогда, когда $\alpha\vee\beta=\beta$ (равносильно, $\alpha\wedge\beta=\alpha$). Дизъюнкцию двух или большего числа векторов будем называть их верхней гранью. Так, $\alpha\vee\beta$ – верхняя грань векторов α и β; $\alpha\vee\beta\vee\gamma$ – верхняя грань векторов α, β и γ и т.п. Каждый вектор является верхней гранью не превосходящих его векторов канонического базиса.

Пусть ξ и η – характеристические векторы подмножеств $X, Y\subset U$. Тогда условие $X\subset Y$ равносильно условию $\xi\le\eta$. Характеристическим вектором множества $X\cup Y$ является вектор $\xi\vee\eta$, а множества $X\cap Y$ – вектор $\xi\wedge\eta$.

Пусть V – конечное множество, содержащее m элементов, $V=\{1,2,\ldots,m\}$, и $f:U\to V$ – произвольное отображение. Для множества $X\subset U$ обозначим через ξ его характеристический вектор, а через $F(\xi)$ – характеристический вектор множества $f(X)\subset V$. Этим определяется отображение $F:\{0,1\}^n\to\{0,1\}^m$.

Непосредственно из определений вытекает, что отображение F обладает следующими свойствами:

1) $F(\xi)=0$ тогда и только тогда, когда $\xi=0$;

2) $w(F(\xi))\le w(\xi)$ для любого вектора ξ;

3) $F(\xi\vee\eta)=F(\xi)\vee F(\eta)$ для любой пары векторов ξ и η.

Обратно, всякое отображение $F:\{0,1\}^n\to\{0,1\}^m$, обладающее перечисленными свойствами, порождается некоторым однозначно определенным отображением $f:U\to V$. В самом деле, если ξ – вектор канонического базиса, то $F(\xi)\ne 0$ и $w(F(\xi))\le w(\xi)=1$. Следовательно, $w(F(\xi))=1$, то есть $F(\xi)$ – вектор канонического базиса. Но векторы канонического базиса являются характеристическими векторами одноточечных множеств. Таким образом, сужение F на канонический базис дает отображение $f:U\to V$.

Назовем матрицу *двоичной*, если все ее элементы нули или единицы. Определим *булево умножение* двоичных матриц подобно тому, как определяется произведение числовых матриц с заменой суммы дизъюнкцией. Пусть $A=(a_{ij})$ и $B=(b_{jk})$ – двоичные матрицы размера $m\times n$ и $n\times p$. Их булевым произведением называется матрица $C=(c_{ik})$ размера $m\times p$, элементы которой определяются формулами

$$c_{ik}=a_{i1}b_{1k}\vee a_{i2}b_{2k}\vee\ldots\vee a_{in}b_{1n}.$$

Пример.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.\square$$

Пусть R – некоторое соответствие из множества $U=\{1,2,\ldots,n\}$ в множество $V=\{1,2,\ldots,m\}$. Положим $a_{ij}=1$, если $(i,j)\in R$ и $a_{ij}=0$ в противном случае. Назовем двоичную матрицу $A=(a_{ij})$, $i=1,2,\ldots n$, $j=1,2,\ldots m$, *характеристической матрицей* соответствия R. Пусть $\xi=(\xi_1,\xi_2,\ldots,\xi_n)$ – характеристический вектор некоторого множества $X\subset U$ (рассматриваемый как двоичная матрица размера $1\times n$). Тогда двоичный вектор $\eta=\xi A$ определяется уравнениями

$$\eta_k=\xi_1 a_{1k}\vee\xi_2 a_{2k}\vee\ldots\vee\xi_n a_{nk},\ k=1,2,\ldots,n,$$

и является характеристическим вектором множества $R(X)\subset V$.

7.4. Логическое представление функций выбора

Пусть n – число элементов множества Ω. Занумеруем варианты числами от 1 до n, и будем обозначать варианты их номерами, полагая, что $\Omega=\{1, 2, \ldots, n\}$.

С учетом предыдущего функцию выбора C можно считать отображением множества $\{0,1\}^n$ в себя, $C:\{0,1\}^n\to\{0,1\}^n$. Так как $C(X)\subset X$ для любого предъявления X, то $C(\xi)\le\xi$ для любого $\xi\in\{0,1\}^n$. Обратно, всякая функция $C:\{0,1\}^n\to\{0,1\}^n$, $C(\xi)\le\xi$, является функцией выбора.

Для $\xi=(\xi_1,\xi_2,\ldots,\xi_n)\in\{0,1\}^n$ пусть

$$C(\xi) = ((C_1(\xi), C_2(\xi), \ldots, C_n(\xi)).$$

Тогда $C_i(\xi)=1$ означает, что вариант i попадет в число выбранных из предъявления с характеристическим вектором ξ. Для всех векторов ξ с $\xi_i=0$ значение $C_i(\xi)$ постоянно и равно 0. Поэтому, по теореме о разложении булевой функции по аргументу, функция $C_i(\xi)$, $i=1,2,\ldots,n$, имеет вид

$$C_i(\xi) = \xi_i : f_i(\xi),$$

где

$$f_1(\xi)=C_1(1,\xi_2,\ldots,\xi_n), f_2(\xi)=C_2(\xi_1,1,\ldots,\xi_n), \ldots, f_n(\xi)=C_n(\xi_1,\xi_2,\ldots,1).$$

Таким образом, каждой функции выбора C отвечает набор функций $f=(f_1,f_2,\ldots,f_n)$, про который говорят, что он дает *логическое представление функции выбора* C. Обратно, произвольный набор булевых функций $f=(f_1, f_2,\ldots,f_n)$, в котором функция $f_i(\xi)$ не зависит от ξ_i, $i=1,2,\ldots n$, однозначно определяет функцию выбора C, для которой составляет ее логическое представление. Логическое представление $f=(f_1, f_2,\ldots,f_n)$ можно рассматривать как отображение $:\{0,1\}^n \to \{0,1\}^m$, полагая

$$f(\xi)=(f_1(\xi),f_2(\xi),\ldots,f_n(\xi)).$$

Пример. Пусть $\Omega=\{1,2,3,4\}$. Будем считать, что варианты занумерованы в порядке убывания их привлекательности для потребителя: вариант с меньшим номером лучше (предпочтительнее) варианта с большим номером. Выбор осуществляется в соответствии со следующими правилами:

1) потребитель никогда не отказывается от выбора и никогда не выбирает более двух вариантов;

2) при предъявлении двух или трех вариантов потребитель отбрасывает худший вариант.

Из непустоты выбора следует, что при предъявлении одного варианта потребитель его и выбирает. При предъявлении всех вариантов потребитель выбирает первые два.

Функция выбора задается следующей таблицей:

ξ	$C(\xi)$	ξ	$C(\xi)$
0000	0000	1000	1000
0001	0001	1001	1000
0010	0010	1010	1000
0011	0010	1011	1010
0100	0100	1100	1000
0101	0100	1101	1100
0110	0100	1110	1100
0111	0110	1111	1100

Дадим явные аналитические выражения для функций C_i. Легко видеть, что

$$f_1(\xi)=1;\ C_1(\xi)=\xi_1\ 1.$$

Функция $f_2(\xi)=C_2(\xi_1,1,\xi_3,\xi_4)$ принимает значение 0 только на одном наборе (1,1,0,0); имеем:

$$f_2(\xi) = \xi_1' \vee \xi_3 \vee \xi_4;\ C_2(\xi)= \xi_2\ (\xi_1' \vee \xi_3 \vee \xi_4).$$

Функция $f_3(\xi)=C_3(\xi_1,\xi_2,1,\xi_4)$ принимает значение 1 на четырех наборах (0,0,1,0), (0,0,1,1), (0,1,1,1), (1,0,1,1). Записав ее в виде ДНФ, получаем:

$$f_3(\xi) = \xi_1'\xi_2' \vee \xi_1'\xi_2\xi_4 \vee \xi_1\xi_2'\xi_4;\ C_3(\xi) = \xi_3(\xi_1'\xi_2' \vee \xi_1'\xi_2\xi_4 \vee \xi_1\xi_2'\xi_4).$$

Функция $f_4(\xi)=C_4(\xi_1,\xi_2,\xi_3,1)$ принимает значение 1 только на одном наборе (0,0,0,1); имеем:

$$f_4(\xi) = \xi_1' \vee \xi_2' \vee \xi_3';\ C_4(\xi) = \xi_4\ (\xi_1' \vee \xi_2' \vee \xi_3').$$

Теорема. *Общее число различных функций выбора на множестве вариантов из n элементов равно* $\left(2^{2^{n-1}}\right)^n$.

Доказательство. Соответствие функций выбора и их логических представлений

$$C \leftrightarrow f = (f_1, f_2, \ldots, f_n)$$

является взаимно однозначным. Теперь доказываемое утверждение следует из того, что каждое логическое представление является набором из n булевых функций от n–1 переменной, а общее число булевых функций от n–1 переменной равно $2^{2^{n-1}}$. □

7.5. Основные свойства функций выбора

Ниже будут описаны некоторые свойства, которыми могут обладать функции выбора. Считается, что функции, обладающие теми или иными комбинациями этих свойств, моделируют так называемый *рациональный выбор*.

Будем говорить, что функция выбора C удовлетворяет *условию наследования* (или *обратному условию Сена*), если

$$Y \cap C(X) \subset C(Y)$$

для любого X и любого $Y \subset X$.

В соответствии с определением выбор удовлетворяет условию наследования, если варианты, выбираемые из более широкого множества (при больших возможностях для сравнения и выбора), тем более будут выбраны и в более узком.

Будем говорить, что функция выбора C удовлетворяет *условию согласия* (или *прямому условию Сена*), если

$$C(X \cup Y) \supset C(X) \cap C(Y)$$

для любых X и Y. Потребительский выбор, удовлетворяющий условию согласия, можно описать так: если два ассортимента содержат общие товары, выбираемые потребителем из каждого из этих ассортиментов, то они будут выбраны и при предъявлении ему объединенного ассортимента. Заметим, что условие согласия можно формулировать не для двух, а для любого конечного числа множеств. Если функция выбора удовлетворяет условию согласия, то, например, для трех множеств X,Y,Z имеем

$$C(X \cup Y \cup Z) \supset C(X \cup Y) \cap C(Z) \supset C(X) \cap C(Y) \cap C(Z).$$

Будем говорить, что функция выбора C независима от отвергнутых вариантов, если

$$C(X \setminus Y) = C(X)$$

в случае, когда $Y \subset X \setminus C(X)$.

Выбор независим от отвергнутых вариантов, если отбрасывание некоторых (или всех) вариантов, не выбранных из исходного предъявления, не меняет выбора.

Следующая теорема описывает свойства функций выбора в терминах их логических представлений.

Теорема. *Пусть набор булевых функций* $f=(f_1,f_2,\ldots,f_n)$ *служит логическим представлением функции выбора* C.

1) *Функция* C *удовлетворяет условию наследования тогда и только тогда, когда отображение* $f:\{0,1\}^n \to \{0,1\}^n$ *антимонотонно*:

$$\xi \le \eta \Rightarrow f(\xi) \ge f(\eta)$$

2) *Функция* C *удовлетворяет условию согласия тогда и только тогда, когда*

$$f(\xi) \wedge f(\eta) \le f(\xi \vee \eta)$$

для любых $\xi,\eta \in \{0,1\}^n$.

3) *Функция* C *независима от отвергнутых альтернатив тогда и только тогда, когда выполняется следующее условие*:

$$\eta \wedge f(\eta) \le \xi \le \eta \Rightarrow \eta \wedge f(\eta) = \xi \wedge f(\xi).$$

□

Мы не приводим доказательства, которое получается простой переформулировкой определений.

Теорема Сена. *Функция выбора нормальна тогда и только тогда, когда одновременно удовлетворяет условиям наследования и согласия*.

Доказательство. *Необходимость*. Предположим, что функция выбора C нормальна, то есть имеет вид $C=C^R$ для некоторого бинарного отношения R на множестве альтернатив Ω:

$$C(X) = \{ x \in X \mid \forall y \in X \neg(yRx)\}.$$

Покажем, что функция C удовлетворяет условию наследования. Пусть $Y \subset X$. Возьмем произвольный элемент $x \in Y \cap C(X)$. Так как $x \in C(X)$, то yRx не выполняется ни для одного $y \in X$ и, значит, тем более ни для одного $y \in Y$. Но тогда $x \in C(Y)$. Следовательно, $Y \cap C(X) \subset C(Y)$.

Покажем теперь, что функция C удовлетворяет условию согласия. Возьмем произвольный элемент $x \in C(X) \cap C(Y)$. Тогда yRx не выполняется ни для одного $y \in X$ и ни для одного $y \in Y$. Значит, yRx не выполняется ни для одного $y \in X \cup Y$ и потому $x \in C(X \cup Y)$. Следовательно, $C(X) \cap C(Y) \subset C(X \cup Y)$.

Достаточность. Предположим теперь, что функция C удовлетворяет условиям наследования и согласия. Определим бинарное отношение R на множестве альтернатив условием

$$xRy \Leftrightarrow y \notin C(\{x,y\}).$$

Тогда

$$C^R(X)=\{x \in X \mid \forall y \in X \neg(yRx)\} = \{x \in X \mid \forall y \in X\, x \in C(\{x,y\})\}.$$

Последнее равенство можно переписать так:

$$x \in C^R(X) \Leftrightarrow x \in X \cap (\cap_{y \in X} C(\{x,y\})).$$

В силу условия согласия при $x \in X$ получаем

$$\cap_{y \in X} C(\{x,y\}) \subset C(\cup_{y \in X} \{x,y\}) = C(X).$$

Но тогда $C^R(X) \subset C(X)$. Докажем обратное включение. Пусть $x \in C(X)$. Тогда для любого $y \in X$, в силу условия наследования, имеем

$$x \in \{x,y\} \cap C(X) \subset C(\{x,y\}),$$

то есть $x \in C^R(X)$.□

Приведем без доказательства еще одну теорему.

Теорема. *Функция выбора C на множестве вариантов* Ω *является выбором по Парето относительно некоторого векторного критерия тогда и только тогда*, *когда функция C удовлетворяет условиям наследования и согласия*, *независима от отвергнутых вариантов и дает непустой выбор для непустых предъявлений*.□

7.6. Логическое представление нормальных функций выбора

В соответствии с определением функции блокировки C^R множество $C^R(X)$ получается из X отбрасыванием всех тех вариантов x, для которых найдется $y \in X$ такой, что yRx, то есть отбрасыванием всех вариантов из $R(X)$. Таким образом,

$$C^R(X) = X \setminus R(X).$$

На языке характеристических векторов это равенство означает, что

$$C^R(\xi) = \xi \wedge (\xi A)'.$$

Отсюда находим функции

$$f_1(\xi) = a_{11}'(\xi_2' \vee a_{21}')(\xi_3' \vee a_{31}') \cdot \ldots \cdot (\xi_n' \vee a_{n1}');$$

$$f_2(\xi) = (\xi_1' \vee a_{12}')a_{22}'(\xi_3' \vee a_{32}') \cdot \ldots \cdot (\xi_n' \vee a_{n2}');$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f_n(\xi) = (\xi_1' \vee a_{1n}')(\xi_2' \vee a_{2n}')(\xi_3' \vee a_{3n}') \cdot \ldots \cdot a_{nn}',$$

дающие логическое представление функции выбора C^R.

Пример. Пусть $\Omega=\{1,2,3,4\}$, а R – это отношение предпочтения, при котором варианты 1 и 2 несравнимы, 2 и 3 тоже несравнимы, а во всех остальных случаях вариант с меньшим номером предпочтительнее, чем вариант с большим номером. Тогда $a_{12}=0$, и $a_{ij}=1$ при $i<j$, $a_{ij}=0$ при $i \geq j$ во всех остальных случаях. Для функции выбора C^R получаем следующее логическое представление:

$$f_1(\xi) = 1; f_2(\xi) = 1; f_3(\xi) = \xi_1'; f_4(\xi) = \xi_1' \cdot \xi_2' \cdot \xi_3'. \square$$

7.7. Логическое представление турнирных функций выбора

Начнем с некоторых общих замечаний относительно монотонных булевых функций.

Булева функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ называется *монотонной* по первому аргументу, если $f(0,\xi_2,\ldots,\xi_n) \leq f(1,\xi_2,\ldots,\xi_n)$ для любого

вектора $(\xi_1,\xi_2,\ldots,\xi_n)$, и *антимонотонной* по первому аргументу, если выполняется противоположное неравенство. Аналогично определяется монотонность и антимонотонность по остальным аргументам. Функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ антимонотонна по ξ_1 в том и только том случае, когда функция $f(\xi_1',\xi_2,\ldots,\xi_n)$ монотонна по ξ_1. Функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ монотонна, если она монотонна по всем своим аргументам.

Если функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ монотонна по ξ_1, она допускает следующее разложение по переменной ξ_1.

$$f(\xi_1,\xi_2,\ldots,\xi_n)=f(0,\xi_2,\ldots,\xi_n)\vee f(1,\xi_2,\ldots,\xi_n)\xi_1.$$

В справедливости этого тождества несложно убедиться непосредственно, подставив $\xi_1=0$ и $\xi_1=1$:

$$f(0,\xi_2,\ldots,\xi_n)=f(0,\xi_2,\ldots,\xi_n)\vee f(1,\xi_2,\ldots,\xi_n)\cdot 0;$$

$$f(1,\xi_2,\ldots,\xi_n)=f(0,\xi_2,\ldots,\xi_n)\vee f(1,\xi_2,\ldots,\xi_n)\cdot 1$$

(второе верно в силу монотонности, поскольку $f(0,\xi_2,\ldots,\xi_n) \le f(1,\xi_2,\ldots,\xi_n)$).

Если функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ монотонна еще и по переменной ξ_2, то разложение можно продолжить. В случае, когда функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ монотонна по всем аргументам, последовательно применяя указанное разложение, мы придем к ДНФ функции $f(\xi_1,\xi_2,\ldots,\xi_n)$, не содержащей отрицаний переменной. Если функция $f(\xi_1,\xi_2,\ldots,\xi_n)$ по некоторым переменным монотонна, а по некоторым антимонотонна, ее можно представить в виде

ДНФ, в которую первые переменные входят без отрицания, а вторые – только с отрицанием.

В качестве примера рассмотрим так называемы пороговые функции, которые определяются условиями вида

$$f(\xi_1,\xi_2,\ldots,\xi_n) = 1 \Leftrightarrow k_1\xi_1+k_2\xi_2+\ldots+k_n\xi_n \geq s,$$

где k_1, k_2, …, k_n, s – действительные коэффициенты. Пороговая функция монотонна по тем переменным, которые входят в сумму с положительным коэффициентом и антимонотонна по тем переменным, которые входят в сумму с отрицательным коэффициентом.

Пример. Пусть $f(\xi_1,\xi_2,\xi_3)$ определяется условием

$$f(\xi_1,\xi_2,\xi_3)=1 \Leftrightarrow 3\xi_1-5\xi_2+\xi_3\geq -1.$$

Тогда

$$f(\xi_1,\xi_2,\xi_3)= \xi_1\xi_3\vee\xi_2'.$$

Чтобы получить эту формулу, можно выписать СДНФ и провести в ней сокращения, используя законы поглощения.□

Рассмотрим теперь турнирный выбор. Для множества участников (игроков) $\Omega=\{1,2,\ldots n\}$ задана турнирная таблица $T=(t_{ij})$, в которой клетка t_{ij} содержит 2, если i победил j; 0, если j победил i; 1, если i и j сыграли вничью. Все клетки t_{ii} содержат единицы.

Пусть X – некоторое множество участников турнира. По определению турнирного выбора из X отбираются победители, то есть игроки, набравшие максимальное число во встречах с

игроками из X. Для $i \in X$ обозначим через $l_i(X)$ разность между числом побед и числом поражений игрока i во встречах с игроками из X. Ясно, что победителями являются те игроки, для которых $l_i(X)$ принимает наибольшее значение. Таким образом,

$$i \in C(X) \Leftrightarrow \forall j \in X\, l_i(X) \geq l_j(X).$$

Пусть $\xi = (\xi_1,\xi_2,\ldots,\xi_n)$ характеристический вектор множества X и $(C_1(\xi),C_2(\xi),\ldots,C_n(\xi))$ – характеристический вектор $C(X)$. Для $i \in X$ имеем

$$l_i(X) = \xi_1 \cdot (t_{i1} - 1) + \xi_2 \cdot (t_{i2} - 1) + \ldots + \xi_n \cdot (t_{in} - 1).$$

Обозначим через $g_{ij}(\xi)$ пороговую функцию, определенную условием

$$g_{ij}(\xi) = 1 \Leftrightarrow l_i(X) - l_j(X) \geq 0,$$

(результат i не хуже, чем результат j).

Тогда условие попадания в число победителей можно переписать так:

$$C_i(\xi) = 1 \Leftrightarrow \xi_i = 1 \wedge (\xi_j = 0 \vee l_i(X) - l_j(X) \geq 0)$$

или

$$C_i(\xi) = \xi_i \cdot (\xi_1' \vee g_{i1}(\xi))(\xi_2' \vee g_{i2}(\xi)) \cdot \ldots (\xi_n' \vee g_{in}(\xi)).$$

Следовательно, логическое представление функции выбора задается функциями

$$f_i(\xi) = (\xi_1' \vee g_{i1}(\xi))(\xi_2' \vee g_{i2}(\xi)) \cdot \ldots (\xi_n' \vee g_{in}(\xi)),\ i = 1,2,\ldots,n,$$

при том, что $\xi_i = 1$.

Пример. Рассмотрим турнир с пятью участниками:

	1	2	3	4	5
1		0	2	2	1
2	2		1	2	1
3	0	1		0	2
4	0	0	2		1
5	1	1	0	1	

Имеем

$$l_1(\xi) = -\xi_2+\xi_3+\xi_4; \qquad l_2(\xi) = \xi_1+\xi_4; \qquad l_3(\xi) = -\xi_1-\xi_4+\xi_5;$$

$$l_4(\xi) = -\xi_1-\xi_2+\xi_3; \qquad l_5(\xi) = -\xi_3.$$

Проведем расчеты для участника 1:

$$g_{11}(\xi)=1;$$

$$g_{12}(\xi)=1 \Leftrightarrow -\xi_1-\xi_2+\xi_3\geq 0; \qquad g_{12}(\xi)=\xi_1'\vee\xi_2';$$

$$g_{13}(\xi)=1 \Leftrightarrow \xi_1-\xi_2+\xi_3+2\xi_4-\xi_5\geq 0;$$

$$g_{13}(\xi)=\xi_1\xi_2'\vee\xi_1\xi_3\vee\xi_1\xi_5'\vee\xi_2'\vee\xi_4\vee\xi_5';$$

$$g_{14}(\xi)=1 \Leftrightarrow \xi_1+2\xi_2+\xi_4\geq 0; \qquad g_{14}(\xi)=1;$$

$$g_{15}(\xi)=1 \Leftrightarrow -\xi_2+2\xi_3+\xi_4\geq 0; \qquad g_{15}(\xi)=\xi_2'\vee\xi_3\vee\xi_4.$$

Отсюда

$$f_1(\xi)=\xi_2'(\xi_2'\vee\xi_3\vee\xi_5'\vee\xi_2'\vee\xi_3'\vee\xi_4\vee\xi_5')(\xi_2'\vee\xi_3\vee\xi_4\vee\xi_5').$$

Раскрыв скобки и проведя упрощения, получаем:

$$f_1(\xi)=\xi_2',$$

откуда

$$C_1(\xi)=\xi_1\xi_2'.$$

Это позволяет сделать вывод, что, участник 1 окажется победителем в любом предъявлении, в которое входит он сам, а участник 2 не входит.

Аналогичным образом можно рассчитать остальные четыре компоненты функции выбора.□