Министерство образования и науки Российской Федерации
Ярославский государственный университет
им. П. Г. Демидова

Л. Ю. Белова, Ю. А. Белов

Элементы теории множеств и математической логики

Теория и задачи

Учебное пособие

Рекомендовано
Научно-методическим советом университета для студентов,
обучающихся по направлению Прикладная математика и информатика

Ярославль 2012

УДК 510.23:510.6(075.8)
ББК В12я73
Б43

Рекомендовано
Редакционно-издательским советом университета в качестве учебного издания. План 2012 года

Рецензенты:
кандидат физико-математических наук, доцент Корнилов П. А.;
кафедра теории и методики преподавания информатики Ярославского государственного педагогического университета им. К. Д. Ушинского,

Б43 **Белова, Л. Ю. Элементы теории множеств и математической логики. Теория и задачи:** учебное пособие /Л. Ю. Белова, Ю. А. Белов; Яросл. гос. ун-т им. П. Г. Демидова. – Ярославль: ЯрГУ, 2012. – 204 с.

ISBN 978-5-8397-0878-5

Пособие содержит материал по элементам теории множеств, исчислению высказываний, исчислению предикатов, булевым функциям. Приведён ряд задач, дополняющих основное содержание пособия.

Предназначено для студентов, обучающихся по направлению 010400.62 Прикладная математика и информатика (дисциплина «Дискретная математика», цикл Б3), очной формы обучения.

ISBN 978-5-8397-0878-5

УДК 510.23:510.6(075.8)
ББК В12я73

Содержание

Введение

Математика состоит из нескольких теорий - геометрии, теории чисел, алгебры и других, которые имеют похожую логическую структуру и методы и используют общий теоретико-множественный язык. Общность структуры всех математических теорий в том, что в них сначала задаются первичные (неопределяемые) понятия и основные недоказываемые утверждения о свойствах этих понятий - аксиомы. Дальнейшее развитие теории происходит чисто логически: из основных утверждений строятся различные выводы - теоремы, на основе первичных понятий определяются дальнейшие понятия. При этом математика не должна опираться на опыт, так как иначе она потеряет свою универсальную применимость. Конечно, при практическом изучении любой математической теории многие аксиомы не формулируются ради простоты в явном виде. Это связано с тем, что для первоначального изучения строго аксиоматический логический метод труден и громоздок, однако он рассматривается как принципиальный способ проверки истинности всех утверждений теории. Все же некоторые основные понятия и аксиомы теории обычно формулируются в самом начале изучения, хотя и в неполном объеме. Например, в геометрии основными понятиями являются точка, прямая, плоскость и другие, примером аксиомы может служить утверждение о том, что через две различные точки проходит не более одной прямой, или знаменитый пятый постулат (аксиома) о параллельных прямых. Примерами определяемых понятий являются луч, угол, ломаная и вообще все геометрические понятия, кроме исходных. Какие при этом возникают проблемы? Необходимо, видимо, точно определить допустимые логические приемы доказательств и уточнить теоретико-множественный язык, используемый (как отмечалось ранее) во всех математических теориях. Эти вопросы очень важны для математики, так как проясняют ее основы. Это одна из причин, почему в данном курсе будет изучаться и теория множеств, и математическая логика. Ясно также, что названные дисциплины входят в базис общей математической культуры.

1 Понятие множества

1.1 Примеры множеств

Множество - начальное, неопределяемое понятие, как точка и прямая в геометрии, натуральное число в арифметике, элемент векторного пространства в линейной алгебре. Представления о натуральном числе или прямой получаются из неформальных разъяснений и примеров: три яблока, три карандаша и т. д. с помощью абстракции дают представление о числе три. Луч света или натянутая проволока дают первоначальное представление о прямой и т. п. Далее первоначальные представления уточняются в процессе изучения свойств этих объектов. Аналогично, представление о множестве дает любое семейство или собрание объектов: слова в словаре, все положительные действительные числа, дни недели и т. п. Объекты, из которых состоит множество, называются элементами множества.

1.2 Обозначение и задание множеств

При изучении геометрии точки, прямые и другие фигуры обозначаются некоторыми идентификаторами, например точка A, прямая l, отрезок AB. Аналогичная практика символьного обозначения чисел и выражений имеется в арифметике и во всех математических теориях вообще. Множества также обозначаются некоторыми идентификаторами (обычно из прописных букв): A, B, C_1, и т. п. Элементы множеств обозначаются строчными буквами или буквами с индексами, например a, x, c_{ij} и т. д. Отметим, что для основных числовых множеств приняты такие стандартные имена:

$\mathbb{N}$ - множество натуральных чисел,

$\mathbb{Z}$ - множество целых чисел,

$\mathbb{Q}$ - множество рациональных чисел,

$\mathbb{R}$ - множество действительных чисел,

$\mathbb{C}$ - множество комплексных чисел.

Для обозначения того, что объект x является элементом множества A, применяется формальная запись $x \in A$ или $A \ni x$, которая читается так: x принадлежит A или A содержит x соответственно. Если x не принадлежит A, применяется запись $x \notin A$. Например, $0.3 \notin N$, однако $0.3 \in Q$. Для задания определенного множества A надо указать те элементы, которые ему принадлежат. Это можно сделать несколькими способами, например:

перечислением элементов: $A = \{a_1, a_2, ...a_n\}$;

заданием характеристического свойства:

$B = \{x | x \in Z, \text{ четное}\}$;

порождающей процедурой: $F = \{x_k | x_0 = 0, x_1 = 1, x_k = x_{k-2} + x_{k-1}\}$.

Отметим, что знак |, встречающийся внутри фигурных скобок в определении множеств B и F, читается как «...такие, что...». Например, определение B «дословно» читается так: B - это множество всех x таких, что x - целое и четное. Конечно, это можно сказать более естественно: B - множество целых четных чисел. Главное, чтобы при этом не искажался смысл. Ясно, что перечислением можно задавать только конечные множества. Любые множества можно задавать при помощи порождающих процедур или характеристических свойств элементов. Можно строить новые множества из имеющихся с помощью некоторых операций, подобно тому, как, например, из чисел

a и b строится число $a + b$ в арифметике. Для определения основных операций такой "арифметики"множеств (она называется алгеброй множеств) будем использовать некоторые знаки, которые пока можно считать просто стенографическими знаками для сокращения письма:

$\Rightarrow$ - если A, то B, или из A следует B;

$\Longleftrightarrow$ - A истинно тогда и только тогда, когда истинно B;

$\neg$ - не A, неверно, что A;

$\vee$ - или A или B (или оба);

$\wedge$ - и A и B;

$\forall$ для всякого ..., любой, всякий;

$\exists$ - существует, найдется такой ..., что ...;

$\exists!$ - существует и при том только один, такой ..., что ...

Все знаки, кроме трех последних, связывают какие-то утверждения, обозначенные через A и B, и называются логическими связками. Три последних знака обращаются к элементам множества и указывают «количество» элементов, имеющих некоторое свойство: все или хотя бы один – и называются кванторами (quantum - количество, сумма). Конечно, ценность этих знаков не только в сокращении письма. В дальнейшем будет показано, что (в некотором смысле) они являются полной основой языка, достаточного для записи любого математического утверждения.

1.3 Отношения между множествами и операции над множествами

Для чисел имеются такие основные операции, как сумма и произведение, а также отношения неравенства и равенства. При построении теории множеств - аналогичная картина.

Определение. Множество A называется подмножеством (частью) множества B, и это обозначается так: $A \subseteq B$, если все элементы из A являются также и элементами множества B. С использованием введенных знаков это можно записать так:

$A \subseteq B \iff \forall x(x \in A \Rightarrow x \in B)$.

Последняя запись может быть прочитана так: A является подмножеством B тогда и только тогда, когда для любого x из того, что он содержится в A, следует, что он содержится в B. Для множеств это отношение включения напоминает отношение неравенства для чисел; во всяком случае, если конечное множество A является подмножеством конечного множества B, то количество элементов в A не больше числа элементов в B. Количество элементов в **конечном** множестве A будем обозначать так: $|A|$. Назовем два множества *равными* и будем это обозначать так: $A = B$, если $A \subseteq B \wedge B \subseteq A$. Определим теперь некоторые операции над множествами.

Определения.

Объединение: $A \cup B = \{x | x \in A \vee x \in B\}$;

Пересечение: $A \cap B = \{x | x \in A \wedge x \in B\}$;

Разность: $A \backslash B = \{x | x \in A \wedge x \notin B\}$;

Симметрическая разность: $A \triangle B = (A \cup B) \backslash (A \cap B) = (A \backslash B) \cup (B \backslash A)$.

Можно дать словесные прочтения данных определений. Например, объединением множеств A и B называется множество всех элементов, принадлежащих A или B (возможно, обоим) и аналогично для оставшихся определений. В дальнейшем будет использоваться смесь естественного и формального языков. Операции объединения и пересечения обобщаются на семейства (наборы) множеств. Пусть I - некоторое множество, каждому $i \in I$ соответствует множество A_i, тогда множество

$$\bigcup_{i\in I} A_i = \{x | \exists i \in I : x \in A_i\}$$

называется объединением семейства множеств A_i (по множеству индексов I). Аналогично определяется пересечение семейства множеств:

$$\bigcap_{i\in I} A_i = \{x | \forall i \in I : x \in A_i\}.$$

Отметим, что симметрическая разность выражается через ранее определённые операции и потому может считаться неосновной. Однако эта операция очень естественна (она дает величину «несовпадения» множеств), и к тому же через нее и одну из предыдущих операций остальные тоже выражаются, как можно проверить, так что ее можно брать за начальную. Для графической иллюстрации операций с множествами используются *диаграммы Эйлера*, в которых множества условно изображаются кругами или частями кругов, а результат операции выделяется штриховкой или цветом:

На рисунке более темным цветом выделены результаты применения операций объединения - $A \cup B$, пересечения - $A \cap B$, разности $A \setminus B$ и симметрической разности $A \triangle B$ к множествам A и B. Диаграммы позволяют в ряде случаев наглядно представить результат применения к множествам и нескольких операций. Отметим, что диаграмма является лишь иллюстрацией, но не средством доказательства, как и чертеж в геометрии.

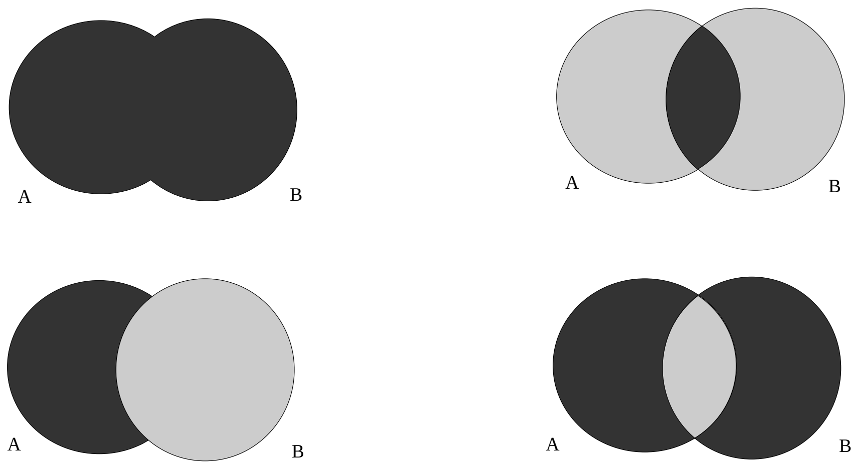

Рис. 1. Основные операции над множествами

1.4 Свойства операций над множествами

Аналогично свойствам операций над числами, таким как коммутативность и ассоциативность сложения и умножения и т. п., имеется ряд основных свойств операций над множествами.

Теорема 1. Выполняются следующие свойства операций над множествами:

1. Ассоциативность объединения и пересечения

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

2. Коммутативность объединения и пересечения

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

3. Дистрибутивность пересечения относительно объединения, дистрибутивность объединения относительно пересечения

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

4. Поглощение $(A \cap B) \cup A = A; \quad (A \cup B) \cap A = A.$

Доказательства утверждений теоремы проводятся совершенно автоматически. Приведем для примера формальное доказательство дистрибутивности пересечения относительно объединения. Отметим, что для доказательства равенства двух множеств необходимо, согласно определению, показать, что всякий элемент из одного множества содержится во втором, и наоборот, любой элемент второго содержится в первом множестве:

$$x \in A \cap (B \cup C) \Rightarrow x \in A \wedge x \in (B \cup C) \Rightarrow x \in A \wedge (x \in B \vee x \in C)$$

$$\Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Rightarrow x \in (A \cap B) \vee x \in (A \cap C)$$

$$\Rightarrow x \in (A \cap B) \cup (A \cap C).$$

Сейчас показано, что $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Обратное включение доказывается аналогично - все логические стрелки можно обратить. Отметим, что приведенные выкладки никак не являются полным доказательством, не требующим ни одного слова пояснения. Это только некоторый «конспект» или «концентрат», который должен быть дополнен устными пояснениями, отсутствующими здесь ввиду ограниченности места. Это замечание справедливо и для всего дальнейшего изложения.

В любой математической теории рассматривается некоторое основное множество объектов, а другие множества являются его подмножествами. Например, в планиметрии основным множеством можно считать плоскость, а геометрические фигуры - различные подмножества плоскости, в линейной алгебре основное множество - линейное пространство, и рассматриваются различные подмножества этого множества, и т. п. В связи с этим при рассмотрении систем подмножеств некоторого множества приняты такие обозначения: основное множество называется *универсумом* и обозначается через U, а множество всех его подмножеств называется *булеан* U и обозначется через $B(U)$. Одним из его элементов является само множество U: $U \in B(U)$, другой крайний случай - *пустое множество* $\emptyset \in B(U)$. Пустое множество $\emptyset$ - аналог нуля в арифметике, это множество, не содержащее ни одного элемента. Можно сказать, что пустое множество является подмножеством любого множества. Для элементов булеана введем еще одну операцию - *дополнение множества A внутри универсума*:

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

Конечно, и A и $\overline{A}$ являются подмножествами U и элементами булеана. Для подмножеств универсума выполнены дополнительные свойства.

Теорема 2.

1. Свойства нуля и единицы

$$A \cup \emptyset = A; \qquad A \cap \emptyset = \emptyset; \qquad A \cup U = U; \qquad A \cap U = A.$$

2. "Законы де Моргана"

$$\overline{A \cup B} = \overline{A} \cap \overline{B}; \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}; \qquad \overline{\overline{A}} = A.$$

3. Свойства дополнения и разности

$$A \cup \overline{A} = U; \qquad A \cap \overline{A} = \emptyset; \qquad A \backslash B = A \cap \overline{B}.$$

Доказательство этой теоремы такое же очевидное, как и предыдущей, и потому пропущено. В дальнейшем конец доказательства или его отсутствие будем обозначать символом •

2 Отношения и функции

2.1 Декартово произведение множеств

Определение. Пусть заданы два множества A и B. *Декартовым (прямым)* произведеним множеств A и B называется множество всевозможных упорядоченных пар вида (a, b), где $a \in A$, $b \in B$:

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

Аналогично дается определение декартова произведения нескольких множеств. Вместо пар при этом рассматриваются упорядоченные наборы *(кортежи)* элементов перемножаемых множеств. Часто отождествляют, например, произведения $(A \times B) \times C$, $A \times (B \times C)$, $A \times B \times C$. Частным случаем произведения является декартова степень множества A: $A^n = A \times ... \times A$ - n раз. Элементы множества A^n называются также *векторами длины (размерности) n с координатами из множества A*. В частности, элементы множества R^n называются арифметическими n-мерными векторами, а само множество R^n - арифметическим n-мерным векторным пространством. Для **конечных** множеств справедлива следующая теорема.

Теорема 1-«правило произведения».

$$|A \times B| = |A| \cdot |B| \bullet$$

Следствие 1

$$|A^n| = |A|^n \bullet$$

Пусть F_2 - множество из двух элементов: $F_2 = \{0, 1\}$, F_2^n - множество соответствующих векторов. Тогда получаем еще

Следствие 2. Множество всех $0 - 1$ - векторов длины n содержит 2^n элементов $\bullet$

Следствие 3. Если A - конечное множество и $|A| = k$, то $|B(A)| = 2^k$.

Доказательство. Пусть $A = \{a_1, a_2, \dots a_k\}$. Тогда каждому подмножеству B множества A можно сопоставить *характеристический вектор* $(i_1, i_2, \dots i_k)$ из нулей и единиц по правилу: $\forall i_l\ i_l = 1$, если $a_{i_l} \in B$, иначе $a_{i_l} = 0$. Легко понять, что указанный способ задает биекцию между всеми 0-1-векторами длины k и подмножествами множества A. Тогда в силу предыдущего следствия утверждение доказано $\bullet$

2.2 Отношения

Вообще говоря, декартово произведение - это еще одна операция на множествах. На его основе можно дать точные определения понятиям функции, частичного порядка, эквивалентности и другим.

Определение. Пусть A и B - два множества. *Бинарным отношением (соответствием)* G из A в B называется подмножество множества $A \times B$: $G \subseteq A \times B$.

Если $A = B$, G называется отношением на множестве A.

Примеры. Пусть $G = \{(x, y) | x, y \in R \wedge y = sin(x)\}$. Очевидно, что G является отношением на R и представляет собой график $y = sin(x)$. Пусть $G = \{(k, l) | k, l \in Z \wedge k - l \vdots 7\}$. Это отношение на Z называется отношением *сравнимости по модулю 7.* Отношения равенства или неравенства также дают примеры бинарных отношений на множестве чисел, равенство или подобие геометрических фигур - примеры бинарных отношений - на множестве фигур плоскости и многие другие.

Понятие бинарного отношения непосредственно обобщается до n-арного отношения – подмножества декартова произведения нескольких множеств:

$$G \subseteq A_1 \times \dots \times A_n = \{(a_1, a_2, ..., a_n) | \forall i\ a_i \in A_i\}.$$

Например, тернарное отношение - на множестве действительных чисел R - всевозможные тройки действительных чисел (x, y, z) такие, что $x + y = z$, на множестве векторов пространства: тройка векторов называется *компланарной*, если векторы тройки параллельны некоторой плоскости.

Определение. Для бинарных отношений вводятся следующие понятия:

Обратное отношение:

$$G^{-1} = \{(a, b)|(b, a) \in G\}.$$

Дополнительное отношение:

$$\overline{G} = \{(a, b)|(a, b) \notin G\}.$$

Тождественное отношение (при $A = B$):

$$I = \{(a, a)|a \in A\}.$$

Например, если G - приводившийся ранее график синуса, то G^{-1} - то, что иногда определяется как $y = Arcsin(x)$ - как говорят, некоторая «многозначная функция». Аналогично, взаимно обратными являются логарифм и показательная функция и т. п.

2.3 Произведение отношений

Пусть $G \subseteq A \times B$ - отношение из A в B, $H \subseteq B \times C$ - отношение из B в C. *Произведением (суперпозицией)* отношений называется отношение из A в C вида:

$$G \circ H = \{(a, c)|\exists b \in B\ (a, b) \in G \land (b, c) \in H\}.$$

Имеется следующая

Теорема 2. Справедливы следующие соотношения:

Ассоциативность суперпозиции: если F, G, H - отношения соответственно из A в B, из B в C, из C в D, то существуют и равны такие произведения:

$$(F \circ G) \circ H = F \circ (G \circ H).$$

Взятие обратного к произведению: если F и G отношения соответственно из A в B и из B в C, то существуют и равны такие произведения:

$$(F \circ G)^{-1} = G^{-1} \circ F^{-1}.$$

Нейтральность тождественного отношения: если F и I_B соответственно отношение из A в B и тождественное на B, то:

$$F \circ I_B = F.$$

Аналогично для умножения слева:

$$I_A \circ F = F.$$

Взятие второго обратного и второго дополнения:

$$(F^{-1})^{-1} = F; \qquad \overline{\overline{F}} = F.$$

Докажем, к примеру, свойство взятия обратного к произведению. Пусть F и G отношения соответственно из A в B и из B в C. Тогда по определению произведения $F \circ G$ существует и является соответствием из A в C. Тогда отношение $(F \circ G)^{-1}$ "действует"из C в A. Аналогично можно убедиться, что существует отношение $G^{-1} \circ F^{-1}$ из C в A. Для доказательства равенства, отмеченного в теореме, остается поэтому доказать два включения: $(F \circ G)^{-1} \subseteq G^{-1} \circ F^{-1}$ и $G^{-1} \circ F^{-1} \subseteq (F \circ G)^{-1}$. Докажем, например, первое.

$$(c, a) \in (F \circ G)^{-1} \Rightarrow (a, c) \in F \circ G$$

$$\Rightarrow \exists b \in B: \ (a, b) \in F \wedge (b, c) \in G$$

$$\Rightarrow (c,b) \in G^{-1} \wedge (b,a) \in F^{-1} \Rightarrow (c,a) \in G^{-1} \circ F^{-1}.$$

Так же тривиально доказывается обратное включение и остальные пункты теоремы ●

2.4 Функции

Определение. Пусть $G \subseteq A \times B$ - отношение из A в B.

Тогда:

область определения G: $D = \{a \in A | \exists b \in B : (a,b) \in G\}$;

область значений G: $E = \{b \in B | \exists a \in A : (a,b) \in G\}$.

Отношение называется *всюду определенным (тотальным)*, если $D = A$.

Отношение называется *сюръективным*, если $E = B$.

Отношение F называется *функциональным* или *однозначным*,

если $\forall a \in D \exists!\ b : (a,b) \in F$.

Отношение F называется *инъективным*,

если $\forall b \in E\ \exists!\ a : (a,b) \in F$.

Очевидно, если F - функционально, то F^{-1} - инъективно. В примере с синусом, конечно, область определения - все множество $\mathbb{R}$, область значений - отрезок $[-1,1]$, и отношение функционально, но не является сюръекцией и инъекцией.

Отношение F, являющееся тотальным и функциональным, называется *функцией* или *отображением* из A в B, и это обозначается так:

$$F : A \to B.$$

При этом используют запись $b = F(a)$ вместо $(a,b) \in F$ и b называют элементом, *соответствующим* a, что согласуется с названием *соответствие*. Для произвольных соответствий (отношений) также вместо общей теоретико-множественной записи $(a, b) \in F$ часто употребляется специальная более компактная: aFb.

Определение. Пусть $F : A \to B$ - функция из A в B. Если она инъективна и сюръективна, она называется *биекцией* A на B, или взаимно-однозначным соответствием A на B.

Собрав все понятия, использовавшиеся в определении биекции, получаем эквивалентную формулировку.

Теорема 3.

Отношение F из A в B является биекцией тогда и только тогда, когда:

$$(\forall a \in A\ \exists!\ b \in B:\ aFb) \wedge (\forall b \in B\ \exists!\ a \in A:\ aFb) \bullet$$

Следующие утверждения легко проверяются, если использовать определения и предыдущую теорему.

Теорема 4.

1. Если F функция из A в B, G - функция из B в C, то $F \circ G$ - функция из A в C.

2. Если F инъекция A в B, G - инъекция B в C, то $F \circ G$ - инъекция A в C.

3. Если F биекция A на B, G - биекция B на C, то $F \circ G$ - биекция A на C.

4. Если F - биекция A на B , то F^{-1} - биекция B на A $\bullet$

Простейшим примером биекции A на A служит тождественное отношение I_A(или просто I), биекцией также является ограничение любой функции на ее область монотонности. Дадим определение ограничения функции. Пусть $F : A \to B$ - функция из A в B и $A_1 \subseteq A$.

Ограничением F на множество A_1 называется отношение $F|_{A_1}$, определяемое так: $F|_{A_1} = F \cap (A_1 \times B)$. Ясно, что ограничение функции снова является функцией: $F|_{A_1} : A_1 \to B$. Аналогичное определение ограничения можно дать для произвольных отношений:

Пусть $G \subseteq A \times B$ - отношение из A в B и $A_1 \subseteq A$, $B_1 \subseteq B$. Тогда ограничением G на $A_1 \times B_1$ назовем $G_1 = G \cap (A_1 \times B_1)$. Например, $y = tg(x)$ задает биекцию интервала $(-\pi/2, \pi/2)$ на $\mathbb{R}$, $y = sin(x)$ - биекцию отрезка $[-\pi/2, \pi/2]$ на отрезок $[-1, 1]$.

2.5 Специальные свойства отношений на множестве

В предыдущем пункте рассматривались отношения, описывающие различные стороны функциональности. Сейчас будут перечислены свойства, которые в некоторых сочетаниях задают важные классы отношений на данном множестве.

Определение. Пусть $G \subseteq A \times A$ - отношение на множестве A. Тогда отношение называется

рефлексивным, если $I_A \subseteq G$,

антирефлексивным, если $I_A \cap G = \emptyset$,

симметричным, если $G^{-1} \subseteq G$,

антисимметричным, если $G \cap G^{-1} \subseteq I_A$,

транзитивным, если $G \circ G \subseteq G$.

Замечание. Для любого из перечисленных пяти свойств обратное отношение тоже обладает этим же свойством.

Легко проверить, что для симметричного отношения имеется равенство: $G^{-1} = G$.

На языке элементов эти свойства переформулируются следующим образом.

Предложение. Пусть G - отношение на A. Тогда

G рефлексивно $\Longleftrightarrow \forall a \in A\ aGa$,

G антирефлексивно $\Longleftrightarrow \forall a \in A\ \neg aGa$,

G симметрично $\Longleftrightarrow \forall a, b \in A\ (aGb \Rightarrow bGa)$,

G антисимметрично $\Longleftrightarrow \forall a, b \in A\ (aGb \wedge bGa \Rightarrow a = b)$,

G транзитивно $\Longleftrightarrow \forall a, b, c \in A\ (aGb \wedge bGc \Rightarrow aGc)$•

Определение. Отношение со свойствами рефлексивности и транзитивности называется отношением *квазипорядка* и обозначается приблизительно таким значком $\preceq$, а не буквой. Отношение делимости является примером квазипорядка в кольце многочленов с действительными коэффициентами $R[x]$ или в кольце целых чисел $\mathbb{Z}$:

$f \preceq g \Longleftrightarrow g \vdots f$.

Определение. Отношение со свойствами рефлексивности, транзитивности и антисимметричности называется отношением частичного порядка, а множество, на котором задано отношение частичного порядка, называется частично упорядоченным.

Элементы x и y будем называть сравнимыми, если или $x \preceq y$ или $y \preceq x$. Тривиальным примером частичного порядка на произвольном множестве A является тождественное отношение I_A. Примером частичного порядка может служить отношение включения для подмножеств данного множества U: $X \preceq Y \Longleftrightarrow X \subseteq Y$, где X и Y принадлежат $B(U)$. Конечно, примером частичного порядка служит и отношение неравенства на множестве действительных чисел, в этом случае любые два элемента сравнимы. Такой частичный порядок называется линейным, а множество - цепью.

В задачах оптимизации требуется находить в данном множестве самый маленький или самый большой элемент в смысле имеющейся частичной упорядоченности. В связи с этим рассмотрим следующие *определения*.

Пусть на множестве A определено отношение частичного порядка $\preceq$.

Элемент $x \in A$ называется минимальным, если $\forall y \in A\ (y \preceq x \Rightarrow y = x)$.

Элемент $x \in A$ называется наименьшим, если $\forall y \in A\ x \preceq y$.

Поясняя определение, можно сказать, что элемент является минимальным, если нет элементов меньше, и элемент является наименьшим, если он меньше всех. Ясно, что наименший элемент (если существует) является минимальным и он в множестве всегда единственный, а минимальных может быть много. Например, для рассматриваемого выше отношения на $B(U)$ имеется наименьший элемент - пустое множество $\emptyset$. Если же рассмотреть ограничение имеющегося отношения частичного порядка только для непустых подмножеств U, то есть для $B(U) \backslash \emptyset$, то наименьшего элемента уже не будет, а минимальными элементами в множестве $B(U) \backslash \emptyset$ будут все одноэлементные подмножества множества U.

В рассматриваемом ранее примере квазипорядка (по делимости) для множества Z рассмотрим его ограничение на множество натуральных чисел больших единицы. Легко проверить, что ограничение будет частичным порядком и множество минимальных элементов будет состоять из простых чисел.

Из замечания, сделанного выше, следует, что отношение, обратное к отношению частичного порядка, также будет отношением частичного порядка; аналогичная ситуация для квазипорядков. Обычно обратное отношение записывается не в виде $\preceq^{-1}$, а так: $\succeq$. Можно дать двойственные определения максимального элемента и наибольшего элемента, как минимального и соответственно наименьшего в обратном отношении. Все примеры и замечания также имеются в двойственных вариантах. В теории частично упорядоченных множеств большую роль играют различные условия *обрыва цепей*, убывающих или возрастающих, как некоторые условия конечности, но это уже обычно выходит за рамки того, что излагается на лекциях.

Другой важный класс отношений - отношения эквивалентности.

Определение. Отношение G на множестве A называется *отношением эквивалентности*, если оно имеет свойство рефлексивности, симметричности и транзитивности.

Хотя отношение эквивалентности от отношения порядка отличается в определении лишь одним свойством, эти классы отношений весьма далеки друг от друга. Отношение на Z - сравнимости по модулю 7, описанное ранее, является отношением эквивалентности.

Вообще, классифицирующие отношения - привычные отношения, преобладающие во всех естественных науках, таких как химия, физика, биология. В математике также отношения равенства геомерических фигур, подобия или гомеоморфности являются примерами отношений эквивалентности. Снова тривиальным примером отношения эквивалентности на A служит тождественное отношение I_A, другими словами - отношение равенства. И в общем случае отношение эквивалентности разбивает элементы множества на классы «одинаковых», или «подобных», элементов.

Определение. Разбиением множества A называется представление A в виде попарно непересекающихся подмножеств:

$$A = \bigcup_{i \in I} A_i, \ \forall i \neq j \in I : \ A_i \cap A_j = \emptyset.$$

Часто, если имеется объединеие непересекающихся множеств, используется такое обозначение:

$$A = \dot{\bigcup_{i \in I}} A_i,$$

при этом множества A_i называются классами разбиения.

Теорема 5. Пусть на множестве A определено отношение эквивалентности G. Тогда существует такое разбиение множества A на непустые подмножества, что каждый класс разбиения состоит из всех попарно сравнимых элементов. Обратно, для любого разбиения A на непересекающиеся непустые классы существует такое отношение эквивалентности на A, что классы разбиения будут классами попарно сравнимых элементов.

Доказательство. $\forall x \in A$ определим множество $A_x = \{y \in A | \ xGy\}$. Ясно, что $A_x \subseteq A \ \forall x \in A$; в силу рефлексивности G xGx и потому $x \in A_x$. Значит,

$$\bigcup_{x \in A} A_x = A.$$

Докажем, что A_{x_1} и A_{x_2} либо не пересекаются, либо совпадают. Пусть $\exists z \in A_{x_1} \cap A_{x_2}$. Тогда $x_1 G z \wedge x_2 G z$ и в силу симметричности и транзитивности G получаем, что

$x_1 G x_2$. Но тогда $\forall t \in A_{x_2}$, снова в силу транзитивности получаем: $x_2 G t \Rightarrow x_1 G t$, то есть $t \in A_{x_1}$. Это означает, что $A_{x_2} \subseteq A_{x_1}$. В силу симметричности условий для A_{x_1} и A_{x_2} обратное включение тоже верно. Таким образом, получено разбиение множества A и классы этого разбиения состоят из всех сравнимых между собой элементов.

Обратно, пусть задано разбиение множества A на непересекающиеся классы A_i. Определим отношение G следующим образом: $xGy \iff \exists i \in I : \; x, y \in A_i$, то есть два элемента сравнимы тогда и только тогда, когда они лежат в одном классе A_i. Очевидно, что полученное отношение удовлетворяет всем условиям теоремы $\bullet$

Отметим, что **множество классов** попарно сравнимых элементов называется *фактор-множеством* множества A по отношению эквивалентности G и обозначается - A/G, класс эквивалентности, в котором содержится $x \in A$, обозначают за $\overline{x}$. Конечно, $\forall x \in A \; x \in \overline{x}$ и $\forall x \in A \; \overline{x} \in A/G$. Ясно также, что вполне может быть $\overline{x}_1 = \overline{x}_2$, хотя $x_1 \neq x_2$. Если элемент $t \in \overline{x}$, то t называется *представителем* класса $\overline{x}$. Конечно, в таком случае имеем равенство: $\overline{t} = \overline{x}$.

Упоминавшееся ранее отношение сравнимости по модулю 7 на Z порождает разбиение целых чисел на семь непересекающихся классов $\overline{0}, \overline{1}, \ldots, \overline{6}$. Каждый класс $\overline{k}$ состоит из целых чисел, которые при делении на 7 дают в остатке k, - эти классы называются классами вычетов по модулю 7. Конечно, в этом примере вычеты по модулю 7 можно заменить вычетами по любому другому модулю n. Аналогичное отношение сравнимости C по модулю какого-нибудь многочлена можно определить для

$R[x]$. Например, $fCg \Longleftrightarrow (f-g)\vdots(x^2+1)$. Тогда каждый класс получившегося отношения эквивалентности состоит из всех многочленов, дающих при делении на x^2+1 один и тот же остаток $a+bx$. Можно показать, что множество классов эквивалентности, то есть фактор-множество $R[x]/C$, отождествляется с множеством комплексных чисел, класс $a+bx$ можно отождествить с числом $a+bi$.

Закончим этот раздел теоремой, в которой будут упоминаться отношения квазипорядка, частичного порядка и эквивалентности

Теорема 6. Пусть на множестве A задано отношение квазипорядка $\preceq$. Определим новое отношение $\sim$ на A и назовем его ассоциированностью: $x \sim y \Longleftrightarrow x \preceq y \wedge y \preceq x$.

Тогда ассоциированность является отношением эквивалентности на множестве A и на фактор-множестве $A/\sim$ определяется отношение частичного порядка по правилу: $\overline{x} \preceq \overline{y} \Longleftrightarrow x \preceq y$.

Доказательство. Отношение $\sim$ определяется симметрично и потому имеет свойство симметричности, так же очевидно и свойство рефлексивности. Проверим свойство транзитивности: пусть $x \sim y \wedge y \sim z$. Тогда $x \preceq y \wedge y \preceq z$, потому в силу транзитивности квазипорядка $\preceq$ получаем: $x \preceq z$. Сравнение $z \preceq x$ справедливо в силу симметричности определения отношения $\sim$. Таким образом показано, что $\sim$ является отношением эквивалентности и можно построить фактор-множество $A/\sim$ классов ассоциированных элементов. Для доказательства второго утверждения прежде всего убедимся, что определение частичного порядка, предложенного в теореме, *корректно.* Дело в том, что, как отмечалось ранее, вполне может быть $\overline{x} = \overline{x}_1$, $\overline{y} = \overline{y}_1$ хотя $x \neq x_1$, $y \neq y_1$, и возникает вопрос, будет ли $x_1 \preceq y_1$? Другими словами, определение, данное в теореме, зависит, вообще говоря, от выбора *представителей* классов. Но если $x \preceq y$ и $x_1 \in \overline{x}$, то $x_1 \preceq x$, и потому $x_1 \preceq y$ в силу транзитивности отношения квазипорядка $\preceq$. Аналогично, если $y_1 \in \overline{y}$, то $y \preceq y_1$, и потому $x_1 \preceq y_1$. Другими словами, определение не зависит от выбора представителей классов. Докажем, что отношение на классах - частичный порядок. Рефлексивность и транзитивность, очевидно, «наследуются» от квазипорядка. Докажем антисимметричность. Пусть имеем: $\overline{x} \preceq \overline{y} \wedge \overline{y} \preceq \overline{x}$. Но тогда получается: $x \preceq y \ \wedge y \preceq x$, откуда $x \sim y$, и, значит, $\overline{x} = \overline{y}$, значит, свойство антисимметричности выполнено •

3 Эквивалентность множеств

3.1 Конечные множества

В различных разделах математики множества изучаются по-разному: в топологии исследуются свойства близости точек множества, наличия в множестве «разрывов», в геометрии - форма множеств, взаимное расположение различных точек, в алгебре - свойства операций на множетве, и так далее. В теории множеств никакие дополнительные структуры на множествах не изучаются - поэтому остается изучать только «запас» точек в множестве, который для **конечного** множества A совпадает с количеством точек в множестве - $|A|$. Для сравнения множеств используется биекция.

Определение. Пусть имеются два множества: A и B. Говорят, что множество A *эквивалентно* или *равномощно* множеству B, если имеется биекция A на B. Эквивалентность множеств обозначается так: $|A| = |B|$.

Отметим, что для конечных множеств символ $|A|$ обозначал количество элементов в множестве, но два конечных множества A и B равномощны тогда и только тогда, когда количество элементов в первом и втором множестве одинаково: $|A| = |B|$, так что противоречия в обозначениях нет.

Например, как отмечалось ранее, $y = tg(x)$ задает биекцию интервала $(-\pi/2, \pi/2)$ на R, $y = sin(x)$ - биекцию отрезка $[-\pi/2, \pi/2]$ на отрезок $[-1, 1]$; легко можно показать, что любые два интервала равномощны между собой и равномощны $\mathbb{R}$ и все отрезки равномощны друг другу.

Из теоремы 4 предыдущей главы (это будем обозначать так: т. 4 гл. 2) следует

Теорема 1. Отношение равномощности обладает свойствами рефлексивности, транзитивности и симметричности •

Можно бы короче сформулировать предыдущую теорему: отношение равномощности является отношением эквивалентности, тем более что это отношение часто так и называется. Однако по определению любое отношение есть отношение на определенном множестве, а наше «отношение равномощности» мы хотим применять к любой паре множеств, то есть это отношение должно быть определено на «множестве всех множеств», а такого множества не существует - для такого объекта надо вводить понятие *класс*; например, класс всех множеств, класс всех векторных пространств и т. п. Но тогда бы возникли слишком сложные вопросы - что такое класс и чем он отличается от множества.

Таким образом, формулировка теоремы, вообще говоря, не совсем строга - нельзя употреблять термин «отношение», который занят другим точным определением. Можно считать это замечание просто пустой придиркой, но основная причина неточности в том, что все предыдущие понятия базировались на понятии множества, а сейчас мы хотим изучать сами множества, для которых (в отличие от геометрии или арифметики) нет приемлемой аксиоматики и первоначальных понятий. Поэтому наш подход к изучению элементов теории множеств называется *наивным.* Аналогично, например, излагается арифметика в школе, где изучается много теорем, хотя основы теории проясняются не до конца.

Из теоремы следует, что если множество A равномощно B, то и B равномощно A, если A равномощно C и B равномощно C, то A равномощно B.

Определение. Отрезком натурального ряда длины n назовем множество всех натуральных чисел, не превосходящих n:

$$[1, n] = \{1, 2, \dots, n\}.$$

Определение. Множество A называется конечным, если оно равномощно некоторому отрезку натурального ряда. Пустое множество также считаем отрезком натурального ряда и потому конечным.

Определение. Множество A называется бесконечным, если оно не является конечным.

Теорема 2. Любое подмножество конечного множества конечно. Объединение двух конечных множеств конечно.

Доказательство. Пусть A - конечное. По определению, существует биекция: $f : A \to [1, n]$. Отсюда, согласно т. 3 гл. 2,следует что

$$(\forall a \in A\ \exists!\ k \in [1, n] :\ k = f(a)) \wedge (\forall k \in [1, n]\ \exists!\ a \in A :\ f(a) = k).$$

Другими словами, каждому элементу из A присвоен натуральный номер и все элементы могут быть выписаны в виде конечной последовательности: $A = \{a_1, a_2, \ldots, a_n\}$. Пусть теперь $A_1 \subseteq A$. Докажем, что A_1 тоже конечное. Так как все элементы из A_1 также содержатся в приведенной конечной последовательности, просматриваем все элементы A и нумеруем те из них, которые содержатся в A_1: первому встретившемуся элементу из A_1 сопоставляем номер 1, следующему - 2 и т. д. Через n шагов все элементы из A будут просмотрены, в частности всем элементам из A_1 будут присвоены номера из некоторого отрезка натурального ряда и полученное соответствие будет биекцией.

Докажем, что $A \cup B$ конечно, если A и B конечны. Во-первых, отметим, что $A \cup B = A \dot{\cup} (B \backslash A)$, $A \cap (B \backslash A) = \emptyset$. A - конечное, $B \backslash A$ - подмножество конечного множества B и потому тоже конечно, значит, имеются биекции: $f : A \to [1, n]$ и $g : B \backslash A \to [1, l]$. Тогда можно построить биекцию h $A \cup (B \backslash A)$ на отрезок $[1, n + l]$ по правилу:

$$h(x) = f(x) \forall x \in A\ \wedge\ h(x) = g(x) + n\ \forall x \in (B \backslash A).$$

Проверка свойств биективности h проводится непосредственно $\bullet$

Следствие. Пересечение любого набора конечных множеств - конечное множество. Объединание конечного набора конечных множеств - конечное множество •

3.2 Счетные множества

Определение. Множество A называется счетным, если оно равномощно натуральному ряду $\mathbb{N}$.

Примеры. Следующие множества счетны:

множество всех целых чисел $\mathbb{Z}$;

множество всех четных чисел;

множество всех целых отрицательных чисел;

множество всех простых чисел •

Более важный пример.

Теорема 3. Множество всех рациональных чисел $\mathbb{Q}$ - счетно.

Доказательство. Всякое рациональное число однозначно записывается как несократимая дробь p/q, где $p \in Z$, $q \in N$. Назовем высотой дроби число $|p| + q$. Ясно, что дробей заданной высоты - конечное число, например, высоту 1 имеет только число $0 = 0/1$, высоту 2 - числа $1/1$ и $-1/1$ и т. д. Нумеруем рациональные числа по возрастанию высоты - сначала присвоим натуральные номера числам высоты 1 (это только 0), затем перенумеруем числа высоты 2 и т. д. Этот процесс задает биекцию $\mathbb{Q}$ на $\mathbb{N}$ •

Теорема 4. Всякое подмножество счетного множества конечно или счетно.

Доказательство. Пусть A - счетное множство. Тогда, в силу существования биекции A на $\mathbb{N}$, каждый элемент из A получает некоторый натуральный номер, и, значит, все элементы из A могут быть записаны в виде следующей бесконечной последовательности:

$$A = \{a_1, a_2, a_3, \dots, a_k, \dots\}.$$

Пусть $B \subseteq A$ - некоторое подмножество A. В силу имеющейся нумерации множества A элементы из B также получают некоторые номера: $B = \{a_{n_1}, a_{n_2}, a_{n_3}, \dots\}$. Может быть два случая: либо среди номеров $n_1, n_2, n_3, ...$ существует наибольший, либо нет, и B либо конечно, либо счетно. Биекция в обоих случаях устанавливается естественно, по возрастанию номеров: $a_{n_1} \to 1,\ a_{n_2} \to 2,\ a_{n_3} \to 3, \dots$ ●

Теорема 5. Объединение конечного или счетного множества счетных множеств является счетным множеством.

Доказательство. Пусть A_1, A_2, A_3, ... – счетные множества. Тогда элементы этих множеств можно записать в виде набора последовательностей:

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \dots\}, \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \dots\}, \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \dots\}, \\ &\ \ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \end{aligned}$$

Допустим для простоты, что все A_i попарно не пересекаются; определим биекцию $f : \cup A_i \to N$. Высотой элемента a_{kl} назовем сумму $k + l$. Нумеруем элементы по возрастанию высот, а в пределах одной высоты - лексикографически:

$$f(a_{11}) = 1,\ f(a_{12}) = 2,\ f(a_{21}) = 3,\ f(a_{13}) = 4,\ f(a_{22}) = 5, ...$$

Легко проверить, что f - биекция ●

Следствие 1. Декартово произведение двух счетных множеств является счетным множеством.

Доказательство. Пусть $C = A \times B$ - декартово произведение счетных множест A и B. Тогда C представляется в виде объединения непересекающихся множеств $A_i = \{(a_i, b_l) : b_l \in B\}$, $i = 1, 2, ...$, и из предыдущей теоремы получаем требуемое утверждение •

Следствие 2. Множество точек n-мерного пространства с рациональными координатами счетно •

Теорема 6. Во всяком бесконечном множестве M имеется такое счетное подмножество A, что $|M \backslash A| = |M|$.

Доказательство. Выделим в множестве M два счетных подмножества A и B следующим образом: так как M бесконечно, в нем существуют два различных элемента - a_1 и b_1. Множество $M \backslash \{a_1, b_1\}$ бесконечно и потому не пусто. Поэтому в нем существуют еще два элемента - a_2 и b_2, и так далее. Пусть уже выделены два подмножества: $\{a_1, a_2, \ldots a_k\}$ и $\{b_1, b_2, \ldots b_k\}$. Это конечные множества, и их объединение тоже конечно (т. 2). Так как M бесконечно, в нем найдутся еще два элемента, не совпадающие с выбранными ранее, a_{k+1} и b_{k+1}, и так далее. Таким образом, в M выделены два счетных непересекающихся подмножества: $A = \{a_1, a_2, \ldots a_k \ldots\}$ и $B = \{b_1, b_2, \ldots b_k \ldots\}$, тем самым доказано первое утверждение теоремы. Докажем, что $|M \backslash A| = |M|$. Очевидно, что

$$M = (M \backslash (A \cup B)) \dot{\cup} (A \cup B);$$

$$M \backslash A = (M \backslash (A \cup B)) \dot{\cup} B.$$

Установим биективное соответствие между слагаемыми в этих объединениях: $M \backslash (A \cup B)$ отображается на себя тождественно, а между $A \cup B$ и B имеется биекция, так как B счетно по построению, а $A \cup B$ счетно как объединение двух счетных множеств (т. 5). С учетом того, что объединяемые в M и $M\backslash A$ множества не пересекаются, получаем биекцию M на $M\backslash A$ $\bullet$

Пусть A - произвольное множество. Подмножество $B \subseteq A$ называется *собственным* подмножеством множества A, если $B \neq A$. Это иногда обозначают так: $B \subset A$. Тогда справедливо

Следствие. Множество является бесконечным тогда и только тогда, когда оно равномощно некоторому своему собственному подмножеству $\bullet$

Теорема 7. Пусть M - бесконечное множество, A - счетное или конечное. Тогда $|M| = |M \cup A|$.

Доказательство. Пусть для простоты $M \cap A = \emptyset$. В силу предыдущей теоремы в M имеется счетное подмножество B. Тогда получаем два разложения:

$$M = (M\backslash B)\dot{\cup}B;$$

$$M \cup A = (M\backslash B)\dot{\cup}(A \cup B).$$

Теперь устанавливаем биекцию между M и $M \cup A$ - аналогично предыдущей теореме - по частям: $M\backslash B$ отображается на себя тождественно, $A \cup B$ биективно на B, что возможно, так как оба множества счетные $\bullet$

4 Сравнение мощностей

4.1 Несчетные множества

Последние теоремы предыдущей главы показывают, что счетные множества должны считаться «самыми маленькими» из бесконечных множеств. Значит, нужно указать способ сравнения бесконечных множеств разных мощностей и выяснить, существуют ли такие бесконечные множества.

Определение. Множество называется *несчетным*, если оно бесконечно и не является счетным.

Пока мы ни про одно множество не доказали, что оно несчётное, однако докажем для них некоторое усиление теоремы 6 предыдущей главы.

Теорема 1. Пусть M - несчётное множество, $A \subset M$ - любое конечное или счетное подмножество, тогда $|M \backslash A| = |M|$.

Доказательство. Отметим, что $M \backslash A$ – несчётное. Действительно, если бы $M \backslash A$ было конечным или счётным, то M было бы конечным или счётным, как объединение двух множеств: $M = (M \backslash A) \dot{\cup} A$. Противоречие показывает, что множество $M \backslash A$ несчётно, значит, бесконечно. Тогда в нём можно выделить счётное подмножество $B \subset (M \backslash A)$. Получаем два разложения:

$$M = ((M \backslash A) \backslash B) \dot{\cup} (A \cup B);$$

$$M \backslash A = ((M \backslash A) \backslash B) \dot{\cup} B.$$

Тогда, как и ранее, определяем биекцию между $M \backslash A$ и M по частям: $(M \backslash A) \backslash B$ отображаем на себя тождественно, $A \cup B$ и B оба счётные и потому эквивалентны •

Следующее утверждение очень важно.

Теорема 2. Множество чисел из интервала $(0, 1)$ несчётно.

Доказательство. По определению несчётного множества надо доказать, что множество $(0, 1)$ бесконечно и не является счётным. Бесконечность очевидна. Докажем, что данное множество не является счётным. Для каждого числа из $(0, 1)$ имеется его запись в виде бесконечной десятичной дроби. При этом различным числам соответствуют различные записи в виде дроби, и наоборот, двум различным дробям соответствуют различные числа из интервала $(0,1)$, если не рассматривать дроби, у которых с некоторого места идут одни девятки, например: $0.2999... = 0.3000...$. Предположим теперь, что $(0,1)$ - счётное, тогда все числа из этого интервала могут быть записаны в виде последовательности десятичных дробей:

$$\begin{aligned} x_1 &= 0.x_{11}x_{12}x_{13}...x_{1k}... \\ x_2 &= 0.x_{21}x_{22}x_{23}...x_{2k}... \\ x_3 &= 0.x_{31}x_{32}x_{33}...x_{3k}... \\ &\quad\ \vdots \quad\ \vdots \quad\ \vdots \quad\ \vdots \end{aligned}$$

Построим число $y = 0.y_1y_2y_3...$, которое принадлежит нашему интервалу и не совпадает ни с одним из x_i. В десятичной записи y будем использовать только цифры 1 и 2 следующим образом: $y_k = 1$, если $x_{kk} \neq 1$, $y_k = 2$, если $x_{kk} = 1$. Тогда $y \neq x_1$, так как $y_1 \neq x_{11}$, $y \neq x_2$, так как $y_2 \neq x_{22}$ и так далее. Но $y \in (0,1)$ и, значит, должен совпадать с одним из x_i. Противоречие •

Доказанная теорема основана на знаменитом «канторовском диагональном процессе», идея которого в различных вариантах использовалась впоследствии в других важных теоремах. Эта теорема дает первый важнейший пример несчётного множества, показывая, что имеются, по крайней мере, два типа бесконечных множеств. Как отмечалось ранее, все интервалы равномощны между собой и равномощны множеству всех действительных чисел R, все отрезки также равномощны между собой. Отметим, что из т. 7 гл. 3 следует, что любой отрезок $[a,b]$ равномощен интервалу (a,b), так как отличается от него всего на конечное множество из двух точек - $\{a,b\}$ и, значит, тоже равномощен R. Множество, равномощное R, называется *континуальным*, или имеющим *мощность континуума* (continuum - непрерывный). Слово «мощность» никак не определяется, определяется только словосочетание «равномощность». Отметим, что множество R равномощно также множеству всех точек на прямой - этот факт используется со школы, всегда действительное число и точка отождествляются, однако его точное доказательство требует некоторого углубления в аксиоматику геометрии и действительных чисел и не будет здесь излагаться.

Следствие 1. Множество всех иррациональных чисел континуально.

Доказательство. Пусть $Irr = \mathbb{R} \backslash \mathbb{Q}$ – множество иррациональных чисел. Так как $\mathbb{Q}$ – счетно, а $\mathbb{R}$ – несчётно (т. 2), в силу теоремы 1 получаем: $|Irr| = |\mathbb{R}|$ •

Среди иррациональных чисел, в свою очередь, есть «более простые», например $\sqrt{2}$, и «более сложные», например π. Для первых более понятно, как они получаются из целых чисел, например приведённое число $\sqrt{2}$ является корнем многочлена с целыми коэффициентами - $x^2 - 2 = 0$, а вот π не является корнем никакого многочлена с целыми коэффициентами (что доказывается весьма сложно). Число называется *алгебраическим*, если оно является корнем некоторого многочлена с целыми коэффициентами, и *трансцендентным*, если оно не алгебраическое. Доказать про конкретное число, что оно не алгебраическое, обычно весьма сложно; долгое время вопрос - существуют ли трансцендентные числа - был открытой проблемой в теории чисел. Тем более интересно, что уже сейчас можно установить такие факты.

Теорема 3. Множество всех алгебраических чисел счётно.

Доказательство. Сначала докажем, что множество многочленов с целыми коэффициентами счётно. Для этого сопоставим каждому многочлену $a_0x^n+a_1x^{n-1}+a_2x^{n-2}\ldots+a_n$ последовательность его коэффициентов $(a_0, a_1, \ldots, a_n)$. Для многочленов степени n получим инъективное отображение в счётное множество $\mathbb{Z}^{n+1}$. Многочленам будут соответствовать векторы, у которых первая компонента $a_0 \neq 0$.

Как отмечалось ранее, всякое подмножество счётного множества конечно или счётно (т. 4 гл. 3), подножество таких векторов бесконечно и потому счётно. Значит, множество многочленов степени n счётно, а тогда и множество всех многочленов счётно, как объединение счётного множества счётных множеств. Каждому многочлену соответствует, в свою очередь, конечное множество агебраических чисел - корней этого многочлена. Таким образом, множество всех алгебраических чисел является объединением счётного множества конечных множеств. Согласно т. 5 гл. 3 объединение счётного множества счётных множеств счётно, множество алгебраических чисел часть такого объединения, оно бесконечно и потому счётно (т. 4 гл. 3) $\bullet$

Следствие. Множество всех трансцендентных чисел континуально.

Доказательство. Пусть Al - множество всех алгебраических чисел, Tr - множество всех трансцендентных. Тогда $Tr = \mathbb{R}\backslash Al$ и в силу того, что $\mathbb{R}$ несчётное, а Al счётное, получаем:

$$|Tr| = |\mathbb{R} \backslash Al| = |\mathbb{R}| \bullet$$

Очевидно, имеются включения:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset Al \ .$$

4.2 Неравенство мощностей

Равномощность для конечных множеств совпадает с равенством количества элементов в двух множествах. Но для чисел еще имеется отношение неравенства; как выяснилось, бесконечные множества, как и конечные, могут быть неравномощны (т. 2) - значит, надо определить отношение неравенства мощностей для и бесконечных множеств, притом так, чтобы для конечных множеств это приводило к обычному неравенству для чисел-мощностей.

Определение. Пусть имеются два множества A и B. Говорят, что *мощность множества A не превосходит мощности B*, если A равномощно некоторому подмножеству множества B, то есть $\exists B_1 \subseteq B : \ |A| = |B_1|$. Другими словами, мощность A не превосходит мощности B, если существует инъекция A в B. Это записывается так: $|A| \leq |B|$.

Говорят, что *мощность множества A меньше мощности B*, если $|A| \leq |B|$ и $|A| \neq |B|$. Обозначение: $|A| < |B|$.

Очевидно, что если $A \subseteq B$, то $|A| \leq |B|$, так как имеется инъекция – тождественное вложение A в B.

Следствия.

Для конечных множеств A и B $|A| < |B| \Longleftrightarrow$ количество элементов в A меньше количества элементов в B.

Если A – счётное, а B – бесконечное, то $|A| \leq |B|$ (т. 6 гл. 3).

Если A – счётное, а $|K| < |A|$, то K – конечное (т. 4 гл. 3).

Мощность любого несчётного множества больше мощности счётного множества (т. 6 гл. 3) $\bullet$

Свойства неравенств мощностей.

Теорема 4. Неравенство мощностей множеств имеет свойства:

рефлексивности: $\forall A: \ |A| \leq |A|$;

транзитивности: $|A| \leq |B| \wedge |B| \leq |C| \Longrightarrow |A| \leq |C|$;

антисимметричности: $|A| \leq |B| \wedge |B| \leq |A| \Longrightarrow |A| = |B|$.

Доказательство. Для любого множества A можно определить тождественное отображение I_A - это биекция, и свойство рефлексивности доказано. Пусть $f : A \to B \wedge g : B \to C$ - инъекции; тогда $f \circ g : A \to C$ - тоже инъекция - свойство транзитивности доказано. Доказательству свойства антисимметричности посвящена отдельная теорема, доказываемая далее $\bullet$

Отношение неравенства для натуральных чисел обладает всеми отмеченными в теореме свойствами, и для чисел еще выполнено свойство линейности - любые два числа x и y сравнимы: $x \leq y \vee y \leq x$. Для нестрогого неравенства мощностей вопрос о наличии сравнимости оказывается сложным, ответ на него зависит от выбора аксиоматики теории множеств, которая отсутствует как единая полная система,достаточная для всех потребностей математики. Можно считать, что сравнимость имеется, она действительно есть в наиболее естественных и мощных системах аксиом.

Теорема 5. Пусть для двух множеств имеются соотношения:

$|A| \leq |B|$ и $|B| \leq |A|$. Тогда $|A| = |B|$.

Сначала докажем вспомогательное утверждение.

Лемма. Пусть $A = \dot{\cup}_{i \in I} A_i$ - объединение непересекающихся множеств A_i, аналогично $B = \dot{\cup}_{i \in I} B_i$, при этом $|A_i| = |B_i| \; \forall i \in I$. Тогда $|A| = |B|$.

Доказательство леммы. Определим биекцию A на B следующим образом: $\forall x \in A \; \exists ! i_0 \in I : x \in A_{i_0}$, в силу того что A_i не пересекаются. Так как $|A_{i_0}| = |B_{i_0}|$, имеется единственный $y \in B_{i_0}$, соответствующий x. Аналогичные рассуждения в обратном направлении. Лемма доказана.

Доказательство теоремы. Так как $|A| \leq |B|$, имеется биекция A на некоторую часть B: $f : A \to B_1, \; B_1 \subseteq B$, точно так же, в силу того что $|B| \leq |A|$, получаем еще биекцию: $g : B \to A_1, \; A_1 \subseteq A$. Суперпозиция $f \circ g$ является биекцией A на некоторую часть A_1: $f \circ g : A \to A_2, \; A_2 \subseteq A_1$. Таким образом, получили ситуацию: $A_2 \subseteq A_1 \subseteq A$ и $f \circ g : A \to A_2$ - биекиця. Для доказательства теоремы достаточно показать, что $|A| = |A_1|$, так как $|B| = |A_1|$ - по построению A_1. При отображении $f \circ g : A \to A_2$ A_1, как подмножество множества A, отображается биективно на некоторое подмножество A_2; назовем его A_3; в свою очередь, $A_2 \subseteq A_1$ отображается на некоторое $A_4 \subseteq A_2$ и так далее. Получаем последовательность вложенных множеств:

$$A \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_k \supseteq A_{k+1} \supseteq \ldots$$

со свойствами - $\forall k \; f \circ g : A_k \to A_{k+2}$ - биекции. Биекциями будут и такие отображения: $f \circ g : A \backslash A_1 \to A_2 \backslash A_3$, $f \circ g :$

$A_1 \setminus A_2 \to A_3 \setminus A_4$ и так далее. Положим

$$D = \bigcap_{k=1}^{\infty} A_k.$$

Тогда получаем два разложения на непересекающиеся подмножества:

$$A = (A \setminus A_1) \dot{\cup} (A_1 \setminus A_2) \dot{\cup} (A_2 \setminus A_3) \dot{\cup} \ldots \dot{\cup} D;$$

$$A_1 = (A_1 \setminus A_2) \dot{\cup} (A_2 \setminus A_3) \dot{\cup} (A_3 \setminus A_4) \dot{\cup} \ldots \dot{\cup} D.$$

При этом имеются биекции: $|A \setminus A_1| = |A_2 \setminus A_3|$, $|A_1 \setminus A_2| = |A_1 \setminus A_2|$, $|A_2 \setminus A_3| = |A_4 \setminus A_5|$, $|A_3 \setminus A_4| = |A_3 \setminus A_4|$ и так далее, в силу отмеченных ранее биекций и тождественных отображений. Это означает, что применима лемма и из нее выводится, что $|A| = |A_1|$; тем самым теорема доказана $\bullet$

Теперь завершено доказательство и теоремы 4.

5 Шкала мощностей

5.1 Теорема о шкале мощностей

В предыдущей главе доказана т. 5, с ней завершено доказательство и т. 4, то есть мощности, можно сказать, «линейно упорядочены». Правда, пока у нас доказано существование только двух различных мощностей бесконечных множеств. То есть по возрастанию, согласно определенному ранее отношению порядка, сначала идут мощности конечных множеств - 0 - мощность пустого множества, 1 - мощность любого одноэлементного множества, 2, 3, и так далее по всему натуральному ряду, затем мощность счётного множества, затем континуального. Остаются, по крайней мере, два вопроса – существуют ли множества промежуточной мощности между счётными множествами и континуальными и существуют ли множества, мощность которых больше мощности континуума. На второй вопрос отвечает теорема Кантора о шкале мощностей:

Теорема 1. Для всякого множества A имеется неравенство:

$|A| < |B(A)|$, где $B(A)$ – булеан A.

Доказательство. Прежде всего напомним, что $B(A)$ – это множество всех подмножеств множества A, другими словами:

$$X \in B(A) \Longleftrightarrow X \subseteq A.$$

В доказательстве будет использоваться и то и другое толкование подмножеств множества A.

По определению строгого неравенства надо доказать два утверждения:

$$|A| \leq |B(A)|;$$
$$|A| \neq |B(A)|.$$

Первое неравенство означает, что должна существовать инъекция A в $B(A)$, то есть биекция A на некоторое подмножество $B(A)$. Действительно, каждому элементу $x \in A$ можно, например, сопоставить одноэлементное подмножество $\{ x \} \in B(A)$ – получим биекцию A на множество всех одноэлементных подмножеств A.

Для доказательства второго неравенства надо доказать, что **не существует** биекции между A и **всем** множеством $B(A)$. Предположим противное: пусть существует биекция f множества A на все множество $B(A)$ - $f : A \to B(A)$. Это значит, что каждому элементу x из A соответствует некоторый элемент $f(x) \in B(A)$, другими словами

- некоторое подмножество A: $f(x) \subseteq A$. При этом элемент x может содержаться в подмножестве $f(x)$, которое ему соответствует, или нет. В множестве A образуем подмножество A_1, состоящее из тех x, которые не содержатся в соответствующем подмножестве $f(x)$:

$$A_1 = \{x \in A \mid x \notin f(x)\}.$$

$A_1 \subseteq A$, значит, $A_1 \in B(A)$, тогда по определению биекции для него существует единственный соответствующий x_1:

$$\exists! x_1 \in A \ : \ f(x_1) = A_1.$$

Снова возможны, вообще говоря, два случая: $x_1 \in A_1$ или $x_1 \notin A_1$. Если $x_1 \in A_1$, то по определению A_1 это означает, что $x_1 \notin f(x_1) = A_1$ - противоречие. Если $x_1 \notin A_1$, то, в силу того что $A_1 = f(x_1)$ и определения A_1, получаем, что x_1 должен принадлежать A_1 - снова противоречие. Значит, такого элемента x_1 не существует, то есть нет и биекции f •

В доказанной теореме использована фактически та же идея диагонального процесса для построения исключительного множества A_1, которому нет соответствующего элемента, что и в более частной теореме о несчетности интервала $(0, 1)$ при построении исключительного числа y, не попадающего в пересчет.

Отметим, что если A - конечное множество, содержащее k элементов, то есть $|A| = k$, то $|B(A)| = 2^k$, потому множество $B(A)$ еще обозначают через $2^A = B(A)$. Теорема при этом превращается в тривиальное утверждение: $k < 2^k$, или $|A| < |2^A| = 2^{|A|}$.

Отметим такое более частное, но и более точное утверждение.

Теорема 2. Множество всех подмножеств счетного множества континуально, например если $\mathbb{N}$ - множество натуральных чисел, то $|B(\mathbb{N})| = |\mathbb{R}| = |(0,1)|$.

Доказательство . Докажем, что любому подмножеству натурального ряда можно сопоставить число из интервала $(0,1)$ и что это сопоставление - биекция. Сначала отметим, что всякое число из интервала записывается в виде бесконечной двоичной дроби вида: $0.x_1x_2\dots x_k\dots$, где $\forall i\ x_i = 0 \vee x_i = 1$, аналогично десятичной записи. Некоторые числа при этом могут быть записаны двояко, например $1/2 = 0.1000... = 0.01111...$. Аналогичное положение отмечалось и для десятичных дробей. Не будем рассматривать дроби, у которых с некоторого места в записи только единицы, всегда будем избирать запись, в которой на соответствующих местах нули и предыдущий разряд увеличен на 1, как в примере. Множество таких дробей биективно числам интервала $(0,1)$. Теперь каждому подмножеству $\mathbb{N}$ сопоставим *характеристическую последовательность* из нулей и единиц, как в след. 3 гл. 2. В результате почти каждому подмножеству множества $\mathbb{N}$ будет сопоставлено число из интервала; исключения составят подмножества $\mathbb{N}$, содержащие все натуральные числа, начиная с некоторого; но таких подмножеств счётное множество, поэтому множество **всех** подмножеств равномощно множеству неисключенных подмножеств, и теорема доказана •

5.2 Замечания

Теорема, данная в предыдущем пункте, отвечает положительно на один из вопросов, сформулированных в начале главы, – существуют ли множества, мощность которых больше мощности континуума. Достаточно взять булеан, и получится более мощное множество, чем то, из которого он построен. Значит, шкала бесконечных мощностей не ограничена. Настоящая теория множеств только начинается с этого момента, но в данном пособии она фактически не рассматривается. Отметим лишь некоторые принципиальные трудности в построении теории, сформулированные как некие «парадоксы» теории множеств (и логики), показывающие, что неограниченное применение понятия «множество» может приводить к противоречиям. Например.

Парадокс Кантора. Пусть M - множество **всех** множеств, $B(M)$ - множество всех его подмножеств, и, значит, $B(M) \subseteq M$, тогда, как отмечалось ранее, $|B(M)| \leq |B|$, и это противоречит теореме о шкале мощностей.

Можно сказать, что «множество всех множеств» - это уж слишком... А как провести границу - где слишком, где еще нет? Понятие множества первичное, никак не определено. Через какое еще «более первоначальное» понятие его определять? Это сложные вопросы, на которые не может быть коротких и сразу всем понятных ответов.

Необходима аксиоматизация теории множеств, благодаря которой можно было бы уточнить понятие множества, определив основные свойства, которым множества должны удовлетворять. Аналогичное положение в геометрии - понятие прямой не определяется, но некоторые свойства прямой уточняют это понятие и позволяют строить непротиворечивую теорию, например постулируется, что через две точки можно провести прямую и притом только одну и т. п.

Из «хороших» аксиом можно было бы получить следствие, что, скажем, множество всех множеств нельзя построить, и тем самым парадокс исчезал бы. Например, можно было бы потребовать,что любое множество не должно содержать себя в качестве элемента: $\forall\, A \notin A$. Конечно, аксиоматика должна обеспечить и непротиворечивость, и достаточную выразительную силу теории, чтобы математические постановки проблем можно было формурировать на этом языке. Это трудно совместить. Например, требование $A \notin A$ исключает из рассмотрения такие монстры, как «множество всех множеств» M, так как оно содержит себя в качестве элемента: $M \in M$. Но здесь возникает следующий парадокс.

Парадокс Рассела. Будем называть множество «хорошим», если оно не содержит себя в качестве элемента, и «плохим», если оно содержит себя в качестве элемента. Каково множество всех хороших множеств?

Легко понять, что оно не может быть ни хорошим, ни плохим. Практически все замечания по поводу предыдущего парадокса справедливы и здесь. Отметим еще, что построение «множества всех хороших множеств» несколько напоминает построение в теореме о шкале мощностей «плохого» множества A_1.

Имеется еще несколько подобных примеров, указывающих, что получить вполне строгое изложение теории множеств очень сложно, хотя это базис всей математики. Это обстоятельство является одним из внутренних доводов для изучения логики. Внешними стимулами для изучения математической логики являются, как отмечалось в начале лекций, необходимость разработок по искусственному интеллекту и вообще широкое использование логики в информатике.

Последнее замечание касается первого вопроса, отмеченного в начале главы, - существуют ли множества промежуточной мощности между счётной мощностью и континуумом? Другими словами, ставится вопрос: континуум – это первая несчётная мощность или есть меньшая? Предполагалось долгое время, что это так (гипотеза континуума), однако доказать это не удавалось, вопрос был назван проблемой континуума. Отметим, что для данной мощности большая мощность в теореме о шкале строится с помощью булеана; как показано в теореме 2, континуум тоже строится из счетного множества как булеан, поэтому можно обобщить вопрос о континууме так: существуют ли промежуточные мощности между мощностью множества и мощностью его булеана? Этот вопрос называется обобщённой проблемой континуума.

Примерно через век после первых постановок этих вопросов они были решены, ответ при этом оказался весьма поучительным - ни гипотеза континуума, ни её отрицание не могут быть доказаны в рамках основной, самой мощной системы аксиом теории множеств. Другими словами, гипотеза континуума (или её отрицание) может быть в качестве аксиомы присоединена к системе имеющихся аксиом - это не приведёт к противоречию, если до присоединения система аксиом была непротиворечива (вопрос о непротиворечивости систем аксиом тоже нетривиален). Получим при этом разные теории множеств.

Совершенно аналогичное положение в геометрии с аксиомой о параллельных. Если принять аксиому о том, что через точку вне прямой можно провести не более одной прямой, не пересекающей данную, и все остальные аксиомы по Евклиду - Гильберту, то получим геометрию Евклида. Если же принять отрицание аксиомы и считать, что через точку вне прямой можно провести более одной прямой, не пересекающей данную, а остальные аксиомы оставить неизменными, получим геометрию Лобачевского, описывающую другой «мир». Вот и множества тоже не описываются единым образом, тоже имеется спектр разных теорий множеств, как и разных геометрий.

Конечно, все затронутые замечания далеко выходят за рамки того круга идей и фактов, которые были точно установлены в данном пособии, но они могут быть полезны как стимул для дальнейшего ознакомления с предметом.

Задачи и упражнения

1. Выразить $A \cup B$ через $\cap$ и $\triangle$, то есть составить выражение алгебры множеств, использующее только символы A, B, символы операций $\cap$ и $\triangle$ и задающее $A \cup B$.
2. Выразить $A \cup B$ через $\setminus$ и $\triangle$.
3. Выразить $A \setminus B$ через $\cap$ и $\triangle$.
4. Выразить $A \setminus B$ через $\cup$ и $\triangle$.
5. Выразить $A \cap B$ через $\cup$ и $\triangle$.
6. Выразить $A \cap B$ через $\setminus$ и $\triangle$.
7. Доказать, что $A \setminus B$ не выражается через $\cap$ и $\cup$.
8. Доказать, что $A \cup B$ не выражается через $\cap$ и $\setminus$.
9. Доказать ассоциативность симметрической разности:

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

10. Доказать дистрибутивность пересечения относительно симметрической разности:

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C).$$

11. По диаграмме Эйлера (рис. 2) видно, что три множества A, B и C порождают разбиение универсума (на рисунке - вся плоскость) на восемь частей.

Выразить каждую из отмеченных частей через A, B и C, используя $\cup$, $\cap$, $\setminus$.

На сколько частей могут разбить универсум четыре множества?

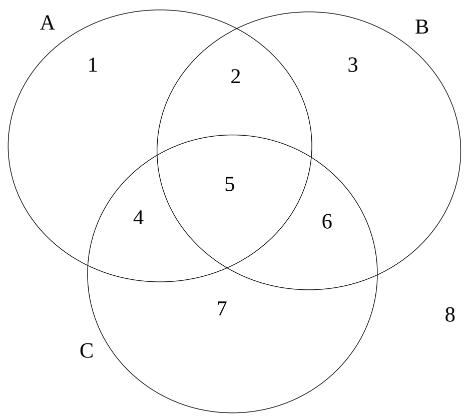

Рис. 2.

12. Доказать, что $(A_1 \cup A_2) \triangle (B_1 \cup B_2) \subseteq (A_1 \triangle B_1) \cup (A_2 \triangle B_2)$.

13. Доказать, что $(A_1 \cap A_2) \triangle (B_1 \cap B_2) \subseteq (A_1 \triangle B_1) \cup (A_2 \triangle B_2)$.

14. Решить уравнение: $A \cup X = B$. Решением уравнения, как обычно, называется множество X, которое при подстановке в левую и правую части уравнения дает верное теоретико-множественное равенство. Требуется выяснить, каким условиям должны удовлетворять множества A и B, чтобы существовало хотя бы одно решение X, и описать семейство всех таких множеств.

15. Решить уравнение: $A \triangle X = X \setminus B$.

16. Решить уравнение: $A \triangle X = B \cap X$.

17. Решить уравнение: $A \triangle X = B \cup X$.

18. Решить уравнение: $A \cap X = B$.

19. Решить уравнение: $A \setminus X = B$.

20. Решить уравнение: $A \triangle X = B \cup X$.

21. Решить уравнение: $A \triangle X = B \setminus X$.

22. Решить систему уравнений

$$\begin{cases} A \cap X = B, \\ A \cup X = C, \end{cases}$$

где A, B, C – данные множества. Определения аналогичны тем, что даны в задаче 14. Другими словами, выяснить, при каких условиях на A, B, C решения существуют и описать семейство всех решений (очевидно, X будет как-то выражаться через исходные множества A, B, C).

Решить следующие системы:

23. $\begin{cases} X \triangle A = B, \\ C \cup X = A. \end{cases}$ 24. $\begin{cases} X \triangle A = B, \\ B \cup X = C. \end{cases}$ 25. $\begin{cases} X \triangle A = B, \\ B \cap X = C. \end{cases}$

26. $\begin{cases} X \triangle A = B, \\ C \cap X = A. \end{cases}$ 27. $\begin{cases} X \triangle A = B, \\ X \setminus C = B. \end{cases}$ 28. $\begin{cases} X \triangle A = B, \\ B \setminus X = C. \end{cases}$

29. $\begin{cases} A \setminus X = B, \\ X \setminus A = C. \end{cases}$ 30. $\begin{cases} A \setminus X = B, \\ A \cup X = C. \end{cases}$ 31. $\begin{cases} A \setminus X = B, \\ A \cap X = C. \end{cases}$

32. $\begin{cases} X \setminus A = B, \\ A \cap X = C. \end{cases}$ 33. $\begin{cases} X \setminus A = B, \\ A \cup X = C. \end{cases}$ 34. $\begin{cases} X \triangle A = B, \\ C \cup X = B. \end{cases}$

35. $\begin{cases} X \triangle A = B, \\ C \cap X = B. \end{cases}$ 36. $\begin{cases} X \triangle A = B, \\ A \cap X = C. \end{cases}$ 37. $\begin{cases} X \triangle A = B, \\ A \cap X = B. \end{cases}$

38. $\begin{cases} X\triangle A = B, \\ C\backslash X = B. \end{cases}$ 39. $\begin{cases} X\triangle A = B, \\ C\backslash X = A. \end{cases}$ 40. $\begin{cases} X\triangle A = B, \\ X\backslash B = C. \end{cases}$

41. $\begin{cases} X\triangle A = B\cap X, \\ A\cap X = C. \end{cases}$ 42. $\begin{cases} X\triangle A = B\cup X, \\ A\cup X = C. \end{cases}$ 43. $\begin{cases} X\triangle A = B\cup X, \\ A\cap X = C. \end{cases}$

Пусть A, B и C - непустые множества. $G_i, i \in I$ - бинарные отношения (соответствия) из A в B, H - соответствие из B в C.

44. Доказать, что

$$(\bigcup_{i\in I} G_i) \circ H = \bigcup_{i\in I}(G_i \circ H).$$

45. Доказать, что

$$(\bigcap_{i\in I} G_i) \circ H \subseteq \bigcap_{i\in I}(G_i \circ H).$$

Пусть A, B и C - непустые множества. G - соответствие из A в B, $H_i \in I$ - соответствия из B в C.

46. Доказать, что

$$G \circ (\bigcup_{i\in I} H_i) = \bigcup_{i\in I}(G \circ H_i).$$

47. Доказать, что

$$G \circ (\bigcap_{i\in I} H_i) \subseteq \bigcap_{i\in I}(G \circ H_i).$$

48. Доказать, что в задачах 2 и 4 не всегда имеется равенство.

49. Пусть $G = \{(x, y) \in R^2 : y = \log_2 x\}$, $H = \{(x, y) \in R^2 : y = 2^x\}$. Построить G^{-1}, $G \circ H$, $H \circ G$.

В задачах 50 - 57 считаем, что G - соответствие из R в R, где R - множество действительных чисел. Напомним, что соответствия из A в A называются еще бинарными отношениями на множестве A.

50. Построить и изобразить на плоскости соответствия G^{-1}, $G \circ G$, $G \circ G^{-1}$, $G^{-1} \circ G$, если G задано следующим образом:

$$G = \{(x, y) \in R^2 : |x| + |y| = 1\}.$$

51. Построить и изобразить соответствия предыдущей задачи, если G задано следующим образом:

$$G = \{(x, y) \in R^2 : |x| + y \leq 1\}.$$

52. Построить и изобразить соответствия, перечисленные в задаче 6, если G задано так:

$$G = \{(x, y) \in R^2 : x^2 + y^2 \leq 1\}.$$

53. Построить и графически изобразить указанные ранее соовестствия для

$$G = \{(x, y) \in R^2 : x - |y| + 1 \geq 0\}.$$

54. Построить и изобразить указанные ранее соовестствия для

$$G = \{(x, y) \in R^2 : x + |y| + 1 \geq 0\}.$$

55. Построить и изобразить указанные ранее соответствия для

$$G = \{(x, y) \in R^2 : x \cdot |y| \geq 2\}.$$

56. Построить и изобразить указанные ранее соответствия для

$$G = \{(x, y) \in R^2 : x \cdot |x| \leq y\}.$$

57. Построить и изобразить указанные ранее соответствия для

$$G = \{(x, y) \in R^2 : (x - 1) \cdot |y| \leq 2\}.$$

В следующих задачах считаем, что все встречающиеся соответствия являются бинарными отношениями на некотором непустом множестве A.

58. Привести пример отношения, которое было бы рефлексивно, транзитивно и не симметрично.

59. Привести пример отношения, которое было бы рефлексивно, антисимметрично и не транзитивно.

60. Привести пример отношения, которое было бы рефлексивно, симметрично и не транзитивно.

61. Привести пример отношения, которое было бы антисимметрично, транзитивно и не рефлексивно.

62. Привести пример отношения, которое было бы симметричным, транзитивным и не рефлексивным.

63. Привести пример отношения, которое было бы рефлексивным, симметричным, антисимметричным и транзитивным.

64. Привести примеры двух транзитивных отношений, произведение которых а) не транзитивно, б) транзитивно.

65. Привести примеры двух симметричных отношений, произведение которых а) не симметрично, б) симметрично.

66. Привести примеры двух антисимметричных отношений, произведение которых а) симметрично, б) антисимметрично.

67. Доказать, что произведение $G_1 \circ G_2$ симметричных отношений симметрично тогда и только тогда, когда они перестановочны:

$G_1 \circ G_2 = G_2 \circ G_1$.

68. Доказать, что произведение $G_1 \circ G_2$ двух отношений эквивалентности является отношением эквивалентности тогда и только тогда, когда они перестановочны: $G_1 \circ G_2 = G_2 \circ G_1$.

69. Доказать, что объединение $G_1 \cup G_2$ двух эквивалентностей является эквивалентностью тогда и только тогда, когда

$G_1 \cup G_2 = G_1 \circ G_2$.

70. Доказать. что произведение $G_1 \circ G_2$ линейных порядков является линейным порядком тогда и только тогда, когда $G_1 = G_2$.

71. Привести пример G и H двух различных отношений частичного порядка, произведение которых $G \circ H$ является частичным порядком, не совпадающим ни с G, ни с H.

72. Доказать, что пересечение любой системы эквивалентностей на данном множестве является отношением эквивалентности.

73. Доказать, что пересечение любой системы частичных порядков на данном множестве является частичным порядком.

74. Построить частично упорядоченное множество без наименьшего элемента, имеющее ровно один минимальный элемент.

75. Привести пример частично упорядоченного множества, в котором существуют любые конечные цепи, но нет бесконечных цепей.

76. Привести пример частично упорядоченного множества, в котором существует любое конечное множество

попарно несравнимых элементов, (антицепь), но не существует бесконечных антицепей.

77. Доказать, что если объединение $A \cup B$ двух множеств счетно, то A или B счетно.

78. Доказать, что если A и B континуальны, то объединение $A \cup B$ континуально.

Пусть M - произвольное множество. Будем через M_∞ обозначать множество всевозможных последовательностей элементов из M : - $M_\infty = \{(x_1, x_2, \ldots, x_n, \ldots)\ x_i \in M\}$.

79. Даны два символа: a и b. Доказать, что множество всевозможных последовательностей из элементов a и b континуально.

80. Доказать, что множество всевозможных последовательностей натуральных чисел N_∞ континуально.

81. Доказать, что множество C_∞ всевозможных последовательностей из элементов счетного множества C континуально.

82. Доказать, что множество R_∞ всевозможных последовательностей действительных чисел континуально.

83. Доказать, что множество всех действительных функций, определенных на отрезке $[a, b]$, имеет мощность больше континуальной.

84. Доказать, что множество всех действительных функций, определенных и непрерывных на отрезке $[a, b]$, является континуальным.

85. Доказать, что объединение

$$C = \bigcup_{\alpha \in R} M_\alpha$$

континуального семейства $M_\alpha, \alpha \in R$ континуальных множеств M_α континуально.

86. Доказать, что множество R^n точек арифметического n-мерного векторного пространства континуально.

6 Элементы математической логики

6.1 Высказывания

В предыдущей главе были приведены замечания, показывающие важность уточнения тех способов рассуждений, которые используются в математике. Это важно для того, чтобы избежать противоречивых математических заключений, то есть для корректного построения математических теорий.

Кроме внутренних стимулов изучения логики имеются сильные внешние причины для ее изучения, одна из основных при этом - проблема автоматизации логического вывода - грубо говоря, проблема построения программной системы автоматического доказательства теорем математики. Автоматизированное получение правильных выводов из имеющихся условий (посылок) важно также для различных диагностических систем в медицине, технике и вообще для систем искусственного интеллекта, когда живого эксперта рядом нет, а действовать надо быстро, например во время какой-либо аварии, несчастного случая и т. п. В подобных ситуациях экспертная система может дать хотя бы какие-то предупреждения или рекомендации.

Другими словами, эти разные доводы подталкивают к одной мысли - необходим формальный однозначный механизм получения правильных выводов из имеющихся посылок (условий). При этом желательно, чтобы способы получения этих выводов можно было легко реализовать программно. Во всяком случае, необходима формальная модель логики. Математика как раз занимается построением всяческих формальных моделей, то есть таких описаний объекта исследований, в котором отсутствует недосказанность, возможность различных толкований получаемых результатов и вообще вопросы истолкования не рассматриваются. Все математические теории строятся в принципе как аксиоматические системы, в которых точно описываются начальные (неопределяемые) понятия и начальные (не доказываемые) утверждения - аксиомы, остальные понятия строятся на основе первоначальных, все утверждения соответственно выводятся из аксиом, хотя явно такая структура может быть иногда описана не до конца.

Математическая логика - логика, изучаемая математическими методами, другими словами, логика здесь излагается в виде аксиоматической теории. Более того, будет дано изложение логики в виде *формальной* аксиоматической теории, то есть для изложения будет использован искусственный ограниченный язык. Это облегчит программную реализацию логики и даст (редкую) возможность показать пример аксиоматической системы в полном объеме, хотя бы для такой простой теории, как исчисление высказываний. При изложении теории множеств мы не могли использовать аксиоматический метод явно ввиду большой сложности предмета изучения - множеств. Мы начнем изучение логики с рассмотрения *высказываний* или *суждений*, то есть предложений, которым можно сопоставить одно из двух возможных *истинностных значений* - истину или ложь. Предполагаем, что истинностных значений всего два, то есть рассматриваем классическую бинарную логику, хотя имеются теории k-значных логик при $k > 2$, а также причинные, временные и другие типы неклассических логик, имеющие большое значение для приложений.

Итак, высказывание - это предложение, которому можно приписать одно из двух возможных истинностных значений - истину или ложь. Примером высказываний могут служить утверждения: «шесть делится на три», «шесть делится на четыре», первое - истинное, второе - ложное. Конечно, далеко не каждое предложение языка является высказыванием, даже если отбросить предложения вида «сегодня хорошая погода» и т. п., истинность или ложность которых оценивается субъективно. Всевозможные вопросы, инструкции или распоряжения типа «следующая лекция начнётся в четырнадцать часов» дают примеры осмысленных предложений, не являющихся высказываниями. Это просто распоряжение, не имеющее истинностного значения. Конечно, для нас в первую очередь интересны высказывания математического содержания, для них истинность или ложность обычно абсолютна в силу формально-аксиоматического характера математических знаний. Еще и потому логика называется математической, что она ориентирована на анализ математических теорий.

6.2 Формальные теории

Мы будем рассматривать некоторый набор начальных (элементарных) высказываний, из которых будем строить более сложные высказывания, используя для этого логические связки, например, которые были определены ранее (или другие подобные):

$\Rightarrow$ - если A, то B, или из A следует B;

$\neg$ - не A, неверно, что A;

$\vee$ - или A или B (или оба);

$\wedge$ - и A и B.

Иногда используется более компактная запись отрицания: $\neg A = \overline{A}$. Ранее эти знаки могли считаться просто стенографическими знаками для сокращения записей, теперь они станут элементами специального формализованного языка изложения логики, поэтому их словесная формулировка не имеет особого значения.

Несколько замечаний о языках. Примерами формальных языков являются языки программирования, сетевые протоколы, языки запросов и т. п., используемые в информатике, язык арифметических выражений в математике и другие. Имеется большая теория формальных языков, которой мы касаться не будем, дадим только два первоначальных определения.

Алфавитом A назовем конечное непустое множество символов. Словом в данном алфавите называется конечная последовательность букв алфавита.

Языком над алфавитом A называется определенное множество слов в данном алфавите.

Например, над латинским алфавитом имеются два языка - французский и английский. В искусственных языках обычно имеются точно определенные правила построения слов - *грамматика* языка. Отметим еще, что здесь говорится о словах, а не о предложениях языка, что кажется необычным, но в действительности это не очень существенно - предложение тоже можно считать словом, если в алфавит добавить знак пробела и другие синтаксические знаки. А в иероглифических языках последовательность нескольких иероглифов без всяких знаков пробела и других разделителей часто является предложением. Дадим определение *формальной аксиоматической теории.*

Определение. Формальной аксиоматической теорией $\mathcal{F}$ называется алфавит A, над которым построено некоторое множество "правильных"слов - формул языка; среди формул выделено некоторое подмножество формул, называемых аксиомами, и на множестве формул задано некоторое конечное множество отношений, называемых *правилами вывода.*

Отметим, что, по определению, формальная аксиоматическая теория есть язык, в котором определены аксиомы и правила вывода.

В рамках нашего курса будут определены две формальные аксиоматические теории, описывающие логику.

Пусть $f_1, f_2, \dots f_n, f_{n+1}$ - формулы теории $\mathcal{F}$, и среди правил вывода есть такое n+1-арное отношение G, что $(f_1, f_2, \dots f_n, f_{n+1}) \in G$. Тогда говорят, что f_{n+1} является *непосредственным следствием* набора формул f_1, $f_2, \dots$ f_n по правилу вывода G. Формулы $f_1, f_2, \dots f_n$ называют *условиями*, или *посылками*, формулу f_{n+1} - *заключением.*

Определение. Последовательность формул $g_1, g_2, \dots g_n$ называется *формальным доказательством*, если каждая формула в этой последовательности является или аксиомой, или непосредственным следствием некоторых предыдущих формул.

Формула g называется *доказуемой*, или *формальной теоремой*, если существует формальное доказательство, заканчивающееся этой формулой.

Обозначается это так: $\vdash g$ и читается «формула g доказуема».

В любой математической теории теоремы обычно не выводятся непосредственно из аксиом, так как это очень громоздко. Теоремы выводятся из некоторых условий, которые, в свою очередь, могут выводиться из предыдущих утверждений, те - аналогично и так далее. Такое последовательное развитие теории наиболее естественно. Аналогично при изучении формальной теории определим понятие *вывода из условий,* обобщающее понятие формального доказательства.

Определение. Пусть имеется произвольный набор формул $G = \{g_1, g_2, \dots g_m\}$, называемый посылками, или условиями, и формула h. Говорят, что формула h выводится из набора условий G, и это обозначается так: $G \vdash h$, если существует конечная последовательность формул $h_1, h_2, \dots h_n$, такая, что каждая h_k является или аксиомой, или одним из условий из набора G, или непосредственным следствием предыдущих формул по одному из правил вывода и $h_n = h$.

Конечно, приведенное определение совпадает с понятием формального доказательства при $G = \emptyset$; понятие непосредственного следствия тоже является простейшим частным случаем вывода из условий.

Цель изучения конкретной формальной аксиоматической теории - описание класса доказуемых формул теории, разработка (по возможности) алгоритмов построения формальных доказательств.

Изучение будет проходить в обычной неформальной манере, как и в других математических теориях, - с помощью обычных неформализованных рассуждений будут устанавливаться какие-то утверждения о формальной теории. Например, вполне может быть доказана (неформальная) теорема о том, что какая-то формула является формальной теоремой. Эта «теорема о теореме» не должна удивлять. По сути эта теорема утверждает, что в нашей формальной теории можно построить последовательность формул определенного вида. Надо только ясно различать объект изучения - формальную теорию, и те обыкновенные доводы, которые используются при этом изучении. Примером простейшей (неформальной) теоремы, справедливой для любой формальной теории, может быть теорема о транзитивности выводимости.

Теорема 1. Пусть $G = \{g_1, g_2, \dots g_m\}$ - набор условий, из которого выводятся формулы $h_1, h_2, \dots h_l$:

$$G \vdash h_1,\ G \vdash h_2, \dots G \vdash h_l,$$

а из набора $H = \{h_1, h_2, \dots h_l\}$ выводится формула s: $H \vdash s$. Тогда из набора G выводится формула s: $G \vdash s$.

Доказательство. Надо доказать, что существует последовательность формул, каждая из которых является или аксиомой, или одним из условий из G, или непосредственным следствием предыдущих формул, заканчивающаяся на формуле s. Для построения такой последовательности выпишем подряд все выводы формул $h_1, h_2, \dots h_l$ из G, существующие по условиям теоремы, и припишем затем к получившейся последовательности вывод s из H. Получим последовательность, заканчивающуюся на формуле s, использующую наряду с аксиомами условия G для выводов h_i и в последней части - условия из H. Однако в этой объединенной последовательности условия из H уже выведены из набора G, и потому теорема доказана $\bullet$

6.3 Исчисление высказываний

В предыдущем пункте было дано общее определение формальной аксиоматической теории. Сейчас будет дано определение конкретной формальной теории - **исчисления высказываний** (ИВ). Определим для этого необходимые элементы определения формальной теории - алфавит, формулы, аксиомы, правила вывода.

Алфавит:

Прописные буквы латинского алфавита - $A, B, \dots Z$, или буквы с индексами $A, A_1, B_k, C \dots,$ (чтобы иметь неограниченный набор символов), называемые *пропозициональными буквами*; логические связки - $\wedge$, $\vee$, $\neg$, $\Rightarrow$, скобки (,).

Формулы:

1. Все пропозициональные буквы есть формулы;

2. Если $\mathcal{A}$ и $\mathcal{B}$ формулы, то следующие слова также являются формулами: $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\neg\mathcal{A})$, $(\mathcal{A} \Rightarrow \mathcal{B})$.

3. Все формулы генерируются в соответствии с правилами 1 и 2.

Аксиомы:

Введение логических связок	Удаление логичеких связок
1. $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$	2. $(\mathcal{A} \Rightarrow \mathcal{B})$ $\Rightarrow ((\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$
3. $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A} \wedge \mathcal{B})$	4. $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{A}$ 5. $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{B}$
6. $\mathcal{A} \Rightarrow \mathcal{A} \vee \mathcal{B}$ 7. $\mathcal{B} \Rightarrow \mathcal{A} \vee \mathcal{B}$	8. $(\mathcal{A} \Rightarrow \mathcal{C})$ $\Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$
9. $(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow ((\mathcal{A} \Rightarrow \overline{\mathcal{B}}) \Rightarrow \overline{\mathcal{A}})$	10. $\overline{\overline{\mathcal{A}}} \Rightarrow \mathcal{A}$

Правило вывода Для любых формул $\mathcal{X}$ и $\mathcal{Y}$ тройка формул вида $\mathcal{X}$, $\mathcal{X} \Rightarrow \mathcal{Y}$, $\mathcal{Y}$ находится в отношении непосредственной выводимости, $\mathcal{Y}$ называется непосредственным следствием двух предыдущих формул согласно данному правилу вывода.

Само правило вывода называется MP (Modus Ponens - «правило удаления»). Теперь все элементы определения ИВ изложены, и необходимо сделать несколько поясняющих замечаний.

Во-первых, данная теория называется исчислением высказываний потому, что при ее применении каждой пропозициональной букве сопоставляется определенное *элементарное* высказывание из какой-то области математики, а логические связки позволяют строить из этих элементарных высказываний другие высказывания. Пусть, например, имеется два элементарных высказывания арифметического характера: «57462916286 делится на 49» и «57462916286 делится на 7»; первое высказывание обозначим через A, второе - через B. Используя связку $\Rightarrow$, можно получить два новых высказывания: $A \Rightarrow B$ и $B \Rightarrow A$, первое из которых, видимо, истинно, а второе не так очевидно, хотя тоже истинно. Вообще вопросы истинности формул тоже требуют своего точного определения, что будет обсуждаться позднее. Читать же приведенные формулы можно, например, так: «из A следует B» или «если A, то B»; условимся только не использовать термин «выводится», для которого есть строгое определение в теории. Для развития формальной теории форма чтения вообще не важна, важны лишь правила действия с формулами.

Логические связки ИВ имеют свои формальные названия:

$\Rightarrow$ - импликация,

$\wedge$ - конъюнкция,

$\vee$ - дизъюнкция,

$\neg$ - отрицание.

Скобки в алфавите ИВ нужны для определения области действия каждой связки в формуле. Условимся не выписывать все скобки, требующиеся по построению формулы, что фактически мы уже и делали, когда давали список аксиом и примеры. Считаем при этом, что отрицание имеет наименьшую область действия, дизъюнкция и конъюнкция - одного ранга и потому всегда требуют поясняющих скобок, импликация имеет наибольший ранг. Например, $A \vee \neg B \Rightarrow C$ в полной записи выглядит так: $((A \vee (\neg B)) \Rightarrow C)$.

Отметим еще, что в определении формул, аксиом и правила вывода использовались буквы в каллиграфичеком (закругленном) шрифте - условимся, что элементы алфавита ИВ - пропозициональные буквы - прямые латинские, а каллиграфическими буквами обозначаются произвольные формулы ИВ. Заметим еще, что индексы при буквах, строго говоря, в алфавит не входят, но у нас используются. Можно было бы включить в алфавит еще и десятичные цифры и использовать индексы "на законных основаниях". Тогда пришлось бы точно определить, что пропозициональный символ - это буква или буква с индексом, индекс - последовательность цифр.

Это означает, что, строго говоря, аксиом - бесконечное множество, а в данном списке приведены лишь *схемы* аксиом - их всего десять. Конкретные аксиомы получаются из схем подстановкой вместо каллигафических букв произвольных формул теории: например, $C \vee D \Rightarrow (A \Rightarrow C \vee D)$ - частный случай первой аксиомы, получающийся если в качестве $\mathcal{A}$ взять $C \vee D$, в качестве $\mathcal{B}$ взять A.

Все аксиомы (схемы) разбиты на два класса - так называемые аксиомы введения и удаления связок. Две первые - введение и удаление импликации, третья, четвертая и пятая - введение и две аксиомы удаления конъюнкции, шестая и седьмая аксиомы - введение дизъюнкции, восьмая - удаление дизъюнкции, девятая и десятая - введение и удаление отрицания. Эти названия аксиом мы будем использовать при ссылках.

В аксиомах связка вводится или удаляется из заключения; напомним, что в импликации тоже есть условие и заключение.

6.4 Примеры формальных выводов

Дадим несколько примеров формальных доказательств и выводов из условий в теории ИВ. По определению, это некоторые последовательности формул. Пример:

1. $A \Rightarrow (A \Rightarrow A)$; введение импликации
2. $(A \Rightarrow (A \Rightarrow A)) \Rightarrow$; удал. импл.
$((A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow (A \Rightarrow A))$
3. $((A \Rightarrow ((A \Rightarrow A) \Rightarrow A)) \Rightarrow (A \Rightarrow A))$; MP 1, 2
4. $A \Rightarrow ((A \Rightarrow A) \Rightarrow A)$; введ. имп.
5. $A \Rightarrow A$; MP 4, 3.

Здесь дан простейший пример формального доказательства или вывода из аксиом. Все формулы последовательности являются или частными случаями аксиом, или следствиями предыдущих формул по правилу MP, о чем говорят *комментарии*, расположенные в строке после точки с запятой. Комментарии являются необходимым элементом обоснования того, что данная последовательность является доказательством.

Отметим, что вместо формул в доказательстве можно было бы иметь в виду аналогичные схемы формул, получилась бы схема доказательства, пригодная для подстановки в нее вместо символов определенных формул и получения конкретного доказательства, например доказательства формулы $C \vee D \Rightarrow C \vee D$.

Доказанная формула $A \Rightarrow A$ весьма примитивна, но это первая формула, доказанная в данной формальной теории; первые теоремы в геометрии тоже кажутся вначале совершенно тривиальными, хотя впоследствии видно, что они используются (явно или неявно) очень часто. Приведенное доказательство также будет использовано в дальнейшем в важной теореме.

Покажем, что $A \wedge B \vdash B \wedge A$, то есть покажем, что из условия $A \wedge B$ *выводится* формула $B \wedge A$.

1. $A \wedge B$	; условие
2. $A \wedge B \Rightarrow A$	; $\wedge$-удаление
3. $A \wedge B \Rightarrow B$	; $\wedge$-удаление
4. A	; MP 1, 2
5. B	; MP 1, 3
6. $B \Rightarrow (A \Rightarrow B \wedge A)$	; $\wedge$-введение
7. $A \Rightarrow B \wedge A$	; MP 5, 6
8. $B \wedge A$	; MP 4, 7

Решение этого примера аналогично предыдущему: вторая, третья и шестая строки - аксиомы, первая - условие, остальные - следствия предыдущих формул по правилу MP. Отметим, что формальный вывод может строиться неоднозначно: например, можно поменять первые три строчки местами или сто раз внести в вывод запись одной и той же аксиомы – снова получим правильный вывод. Другими словами, существует актуальная проблема получения кратчайшего вывода или доказательства. При этом длина вывода - количество строчек в нем.

Здесь ярко проявляется достоинство формальной теории – возможность точно определить понятие сложности доказательства, описать которое без подходящей формализации весьма трудно.

Еще пример вывода.

Лемма о транзитивности импликации: $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$.

Доказательство.

1. $(B \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))$	; $\Rightarrow$-введение
2. $B \Rightarrow C$	; условие 2
3. $A \Rightarrow (B \Rightarrow C)$	; MP 2, 1
4. $A \Rightarrow B$	; условие 1
5. $(A \Rightarrow B) \Rightarrow (A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$	; $\Rightarrow$-удаление
6. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$	; MP 4, 5
7. $A \Rightarrow C$	; MP 3, 6 •

Из этих примеров видно, что непосредственное построение формальных выводов весьма громоздко и вообще бесперспективно, так как ясно, что существуют формулы, кратчайшее доказательство которых может быть как угодно длинно. Это означает, что надо разработать методы доказательства *существования вывода* данной формулы из условий (или только из аксиом), которые не приводили бы к необходимости выписывания всего формального доказательства в явном виде - только так можно получить какой-либо критерий, позволяющий для любой формулы ответить на вопрос – доказуема она или нет.

В следующей главе начнется разработка таких методов.

7 Выводимость

7.1 Теорема о дедукции

Первой теоремой, помогающей установить выводимость какой-либо формулы без явного выписывания полного вывода, является теорема о дедукции. Используя ее, в дальнейшем будут получены другие способы установления выводимости.

Теорема о дедукции. Пусть $\mathcal{G}$ - произвольный набор формул ИВ, A, B - две формулы.

Тогда если $\mathcal{G}, A \vdash B$, то $\mathcal{G} \vdash A \Rightarrow B$.

Доказательство. Требуется доказать, что если существует вывод B из соответствующих условий, то можно построить и другой вывод - формулы $A \Rightarrow B$. В теореме будет дан способ преобразования первого вывода во второй. Сначала ко всем формулам имеющегося вывода припишем слева символы $A \Rightarrow$:

вывод B	преобразованная последовательность
C_1	$A \Rightarrow C_1$
C_2	$A \Rightarrow C_2$
$\vdots$	$\vdots$
C_n	$A \Rightarrow C_n$
B	$A \Rightarrow B$

Преобразованная последовательность формул не является выводом, но заканчивается той формулой, которая требуется в теореме. Перед каждой формулой в полученной последовательности будем вписывать несколько формул так, что после этих вставок получится требуемый вывод. Рассмотрим k-ю формулу в последовательности: $A \Rightarrow C_k$. По определению вывода B могут быть такие случаи: C_k - аксиома , $C_k \in \mathcal{G}$, $C_k = A$, C_k - следствие по правилу МР двух предыдущих формул C_i и C_j. Рассмотрим последовательно все случаи.

Пусть C_k - аксиома.

Тогда перед формулой $A \Rightarrow C_k$ впишем две формулы:

$$\begin{array}{cl} \vdots & \vdots \\ C_k & ;\text{ аксиома} \\ C_k \Rightarrow (A \Rightarrow C_k) & ;\Rightarrow\text{-введение} \end{array}.$$

Тогда следующая за ними формула $A \Rightarrow C_k$ является непосредственным выводом из одного из условий $\mathcal{G}$ и аксиомы:

$$\begin{array}{cl} \vdots & \vdots \\ C_k & ;\text{ аксиома} \\ C_k \Rightarrow (A \Rightarrow C_k) & ;\Rightarrow\text{-введение} \\ A \Rightarrow C_k & ;\text{ МР 1, 2} \end{array}.$$

Пусть C_k - некоторое условие из $\mathcal{G}$. Впишем перед разбираемой формулой те же две формулы, что и в предыдущем случае, только изменим комментарий к формуле C_k. Получим, что текущая формула $A \Rightarrow C_k$ выведена из $\mathcal{G}$.

Если $C_k = A$, впишем перед ней доказательство формулы $A \Rightarrow A$, полученное в предыдущей главе.

Последний случай - C_k – следствие предыдущих формул C_i и C_j по правилу МР. Тогда эти формулы таковы: $C_i = X$, $C_j = X \Rightarrow Y$, $C_k = Y$, и в преобразованной последовательности имеются следующие формулы:

$$\begin{array}{c} \vdots \\ A \Rightarrow X \\ \vdots \\ A \Rightarrow (X \Rightarrow Y) \\ \vdots \\ A \Rightarrow Y \end{array}$$

Впишем соответствующие строки перед рассматриваемой формулой $A \Rightarrow Y$:

$$\begin{array}{ll}
\vdots & \vdots \\
\text{p. } A \Rightarrow X & \vdots \\
\vdots & \vdots \\
\text{q. } A \Rightarrow (X \Rightarrow Y) & \vdots \\
\vdots & \vdots \\
\text{r. } (A \Rightarrow X) \Rightarrow ((A \Rightarrow (X \Rightarrow Y)) \Rightarrow (A \Rightarrow Y)) & ; \Rightarrow\text{-введение} \\
\text{s. } (A \Rightarrow (X \Rightarrow Y)) \Rightarrow (A \Rightarrow Y) & ; \text{MP p, r} \\
A \Rightarrow Y & ; \text{MP q, s.}
\end{array}$$

Таким образом, получаем окончательную последовательность, являющуюся требуемым выводом формулы $A \Rightarrow B$ •

Отметим, что вывод формулы $A \Rightarrow B$, строящийся в теореме, примерно в три раза длиннее исходного вывода формулы B. В этом проявляется смысл теоремы: имея короткий вывод, можно утверждать, что существует более длинный и сложный вывод. При этом теорема дает даже алгоритм построения нового вывода - его построение вполне может быть автоматизировано, хотя, конечно, вывод, построенный при помощи теоремы, не всегда оптимальный. Отметим, что теорема, обратная теореме о дедукции, справедлива и тривиальна:

если $\mathcal{G} \vdash A \Rightarrow B$, то $\mathcal{G}, A \vdash B$.

Для доказательства к имеющемуся выводу импликации $A \Rightarrow B$ надо приписать A и B, A как новое условие и B как следствие этого условия и импликации.

Приведем пример использования теоремы о дедукции. Сначала отметим, что теорема о транзитивности выводимости, доказанная для любой формальной теории, справедлива и для ИВ. Укажем еще два простейших замечания о выводимости: $F \vdash F$, для любой формулы F и если

$\mathcal{H} \vdash F$ и $\mathcal{H} \subseteq \mathcal{G}$, то $\mathcal{G} \vdash F$.

Докажем снова лемму о транзитивности импликации:

$A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$.

1. A, $A \Rightarrow B, B \Rightarrow C \vdash B$; MP усл. 1, 2
2. A, $A \Rightarrow B, B \Rightarrow C \vdash B \Rightarrow C$; тождест.
3. $B, B \Rightarrow C \vdash C$; MP
4. A, $A \Rightarrow B, B \Rightarrow C \vdash C$; т.транз. 1, 2, 3
5. $A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C$; т.дедук. 4.

Отметим, что здесь имеется не последовательность формул, а последовательность утверждений о существовании каких-то выводов, комментарии обосновывают эти утверждения. Например, в четвертой строке используется теорема о транзитивности выводимости, так как в первой и второй строках из одного и того же набора условий выводятся две формулы, а в третьей строке из полученных двух формул выводится еще одна, это соответствует условиям теоремы. В подобном стиле будут оформляться утверждения о существовании выводимостей и в дальнейшем.

7.2 Теорема о десяти выводимых правилах

Предыдущий пример применения теоремы о дедукции совсем простой и не соответствует сложности теоремы. Сейчас будет дано более важное применение этой теоремы.

Теорема о десяти правилах введения и удаления логических связок.

Пусть $\mathcal{G}$ - произвольный список условий, A, B, C - формулы. Тогда справедливы следующие утверждения:

Введения	Удаления
1. Если $\mathcal{G}, A \vdash B$, то $\mathcal{G} \vdash A \Rightarrow B$	2. $A, A \to B \vdash B$
3. $A, B \vdash A \wedge B$	4. $A \wedge B \vdash A$, 5. $A \wedge B \vdash B$
6. $A \vdash A \vee B$, 7. $B \vdash A \vee B$	8. Если $\mathcal{G}, A \vdash C$ и $\mathcal{G}, B \vdash C$, то $\mathcal{G}, A \vee B \vdash C$
9. Если $\mathcal{G}, A \vdash B$ и $\mathcal{G}, A \vdash \neg B$, то $\mathcal{G} \vdash \neg A$	10. $\neg\neg A \vdash A$.

Доказательство. 1 – теорема о дедукции, 2 – MP, 3 – 7 – очевидные следствия соответствующих аксиом. Вот, к примеру, доказательство пункта 3.

1. A ; 1-условие
2. B ; 2-условие
3. $A \Rightarrow (B \Rightarrow A \wedge B)$; $\wedge$-введение
4. $B \Rightarrow A \wedge B$; MP 1, 3
5 $A \wedge B$; MP 2, 4.

Аналогично тривиально доказываются пункты 4 - 7 и 10.

Докажем утверждение 8. Применяя теорему дедукции к условиям, получаем: $\mathcal{G} \vdash A \Rightarrow C$, $\mathcal{G} \vdash B \Rightarrow C$. Тогда тем более:

1. $\mathcal{G},\ A \vee B \vdash A \Rightarrow C$; т.д. усл. 1
2. $\mathcal{G},\ A \vee B \vdash B \Rightarrow C$; т.д. усл. 2
3. $\mathcal{G},\ A \vee B \vdash A \vee B$; тождеств.
4. $A \Rightarrow C, B \Rightarrow C, A \vee B \vdash C$; $\vee$-введение и три раза MP
5. $\mathcal{G},\ A \vee B \vdash C$; т. тр. 1, 2, 3, 4.

Строго говоря, четвертая строка требует своего доказательства, но оно очевидно и потому пропущено. Таким же образом доказывается пункт 9:

1. $\mathcal{G} \vdash A \Rightarrow B$; т.д. 1-условие
2. $\mathcal{G} \vdash A \Rightarrow \neg B$; т.д. 2-условие
3. $A \Rightarrow B$, $A \Rightarrow \neg B \vdash \neg A$; $\neg$ - введение и дважды MP
4. $\mathcal{G} \vdash \neg A$; т.т. 1, 2, 3 $\bullet$

Фактически доказанная теорема переводит аксиомы на более привычный язык выводимости. Девятое правило

- схема рассуждения «от противного», восьмое - способ доказательства разбором случаев, другие правила тоже не противоречат интуитивным представлениям, но теперь это строго доказанные свойства формальной теории.

Дадим примеры применения полученных правил.

Лемма о противоречии. $A,\ \neg A \vdash B$.

Доказательство.

1. $A, \neg A, \neg B \vdash A$; тожд.
2. $A, \neg A, \neg B \vdash \neg A$; тожд.
3. $A, \neg A, \vdash \neg\neg B$; $\neg$ - введение 1, 2
4. $\neg\neg B \vdash B$; $\neg$ - удаление
5. $A, \neg A \vdash B$; т.т. 3, 4 •

Отметим, что третья строка прокомментирована как введение отрицания, это название соответствующей аксиомы, но теперь это и название одного из правил последней теоремы - правила 9, ссылка была на это правило. Аналогичное замечание для следующей строки. Вообще теперь оборот «введение/удаление логических связок» является как названием аксиомы, так и названием соответствующего этой аксиоме правила вывода; это не очень удобно, но не должно приводить к непониманию.

Лемма о противоположной теореме. Пусть $\mathcal{G}$ - произвольный список условий, A, B - формулы.

Тогда если $\mathcal{G}, A \vdash B$, то $\mathcal{G}, \neg B \vdash \neg A$.

Доказательство.

1. $A \Rightarrow B, A, \neg B \vdash B$; MP 2, 1-условия
2. $A \Rightarrow B, A, \neg B \vdash \neg B$; тожд.
3. $A \Rightarrow B, \neg B \vdash \neg A$; $\neg$ - введение 1, 2
4. $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$; т.д. 3.
5. $\mathcal{G} \vdash A \Rightarrow B$; т.д. условие леммы
6. $\mathcal{G} \vdash \neg B \Rightarrow \neg A$; т.т. 5, 4
7. $\mathcal{G}, \neg B \vdash \neg A$; «обратная т.д.» - 6. •

Теперь основные свойства выводимости установлены. Отметим, что получить явный вывод, дающийся, например, в лемме о противоречии, уже довольно трудно.

Напомним, основная задача изучения ИВ, как и любой математической теории, - описание класса формальных теорем. В связи с этим подумаем, что утверждается в лемме о противоречии. Лемма утверждает, что если получено противоречие, то доказуема **любая** формула, и вопрос описания класса выводимых формул решается тривиально – все формулы выводимы Конечно, рассмотрение противоречивых теорий неинтересно. Таким образом, возникает проблема доказательства непротиворечивости нашей теории.

8 Доказуемость, истинность, полнота

8.1 Булевы функции

Как отмечалось ранее, для содержательного изучения теории необходимо убедиться в ее непротиворечивости. В качестве инструмента для доказательства непротиворечивости будут использованы булевы функции, но сначала определим необходимые понятия.

Определение.

Формальная аксиоматическая теория будет называется *внутренне непротиворечивой,* если ни для какой формулы F не может быть одновременно доказуема F и $\neg F$. Это свойство теории называют еще непротиворечивостью в узком смысле.

Другими словами, для любой формулы F хотя бы одно из следующих утверждений неверно: $\vdash F$ или $\vdash \neg F$, может быть - оба.

Если рассматривать формальную аксиоматическую теорию, в которой отсутствует символ отрицания (а такие теории изучаются), то теорию следует назвать непротиворечивой, если в теории существуют недоказуемые формулы; по крайней мере, для ИВ это определение совпадает с предыдущим, как следует из леммы о противоречии.

План доказательства непротиворечивости ИВ таков: зададим некоторый способ, сопоставляющий каждой формуле определенную функцию. При этом доказуемым формулам будут сопоставлены функции-константы; уже отсюда будет ясно, что не все формулы доказуемы, и, значит, в силу леммы о противоречии, теория непротиворечива.

Определение. Пусть $F_2 = \{0, 1\}$ - множество из двух элементов, F_2^n -декартова степень, F_2 - множество соответствующих 0-1-векторов, содержащее, как отмечалось (гл. 2, сл. 2), 2^n элементов.

Логической (булевой) фукцией от n неизвестных называется отображение $f : F_2^n \to F_2$.

Попросту сказать, функция $y = f(x_1, x_2, \ldots x_n)$ называется булевой (логической), если переменные x_i и сама функция y принимают только два значения - 0 и 1. Всякая логическая функция может быть задана конечной таблицей значений (таблицей истинности), содержащей 2^n строк.

Теперь сопоставим каждой логической связке следующие булевы функции:

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1

x	y	$x \Rightarrow y$
0	0	1
0	1	1
1	0	0
1	1	1

x	$\neg x$
0	1
1	0

Пусть теперь $\mathcal{A}$ - произвольная формула ИВ. Всем пропозициональным буквам, входящим в $\mathcal{A}$, сопоставим булевы переменные из F_2. Тогда формуле $\mathcal{A}$ однозначно соответствует булева функция, значение которой на произвольном наборе значений переменных вычисляется согласно определению формулы. Если, например, $\mathcal{A} = \mathcal{B} \wedge \mathcal{C}$, то можно считать (индукция по количеству логических связок), что значения формул $\mathcal{B}$ и $\mathcal{C}$ уже вычислены, и для вычисления значения $\mathcal{A}$ используем таблицу для конъюнкции; для других логических связок вычисления аналогичны.

Ясно, что функции, сопоставленные логическим связкам, соответствуют интуитивным представлениям об истинности и ложности связок, если считать, что 0 - соответствует лжи, 1 - истине.

Определение. Формула A исчисления высказываний называется *тавтологией*, или тождественно истинной, если соответствующая ей булева функция тождественно равна 1. Это обозначается так: $\models A$.

Другими словами, при любом наборе значений входящих в формулу пропозициональных букв значение самой формулы равно 1.

8.2 Непротиворечивость исчисления высказываний

Непротиворечивость ИВ следует из теоремы:

Теорема 1. Если формула $\mathcal{F}$ исчисления высказываний доказуема, то она тождественно истинна. С использованием сокращенных обозначений: если $\vdash \mathcal{F}$, то $\models \mathcal{F}$.

Доказательство. Можно проверить, что все аксиомы тождественно истинны. Отметим при этом, что если схема аксиом задает тождественно истинную функцию от входящих в нее букв, то и частный случай аксиомы, получающийся подстановкой вместо букв произвольных формул, также будет тождественно истинной формулой.

Второй факт - непосредственное следствие по правилу MP двух тождественно истинных формул тождественно истинно, то есть если $\models \mathcal{A}$ и $\models \mathcal{A} \Rightarrow \mathcal{B}$, то и $\models \mathcal{B}$. Действительно, согласно таблице для импликации, если истинны условие и сама импликация, это соответствует четвертой строке, в которой и заключение истинно.

Очевидно, что из этих двух фактов и определения формального доказательства следует, что все формулы любого формального доказательства являются тавтологиями
$\bullet$

Говорят, что теорема 1 устанавливает свойство непротиворечивости относительно тождественной истинности.

Отсюда легко следует непротиворечивость теории.

Теорема 2. Теория ИВ внутренне непротиворечива.

Доказательство. По определению непротиворечивости надо доказать, что для всякой формулы $\mathcal{F}$ хотя бы одно утверждение не выполнено: $\vdash \mathcal{F}$ или $\vdash \neg\mathcal{F}$. Действительно, если $\mathcal{F}$ не является доказуемой - все в порядке; пусть $\mathcal{F}$ доказуема. Тогда $\mathcal{F}$ - тавтология в силу теоремы 1. Тогда $\neg\mathcal{F}$ тождественно ложна и потому не доказуема $\bullet$

Указанное сопоставление формулам булевых функций позволило сформулировать отличительное свойство доказуемых формул – все они являются тавтологиями, на этом основывалось доказательство непротиворечивости. Как отмечалось, непротиворечивость ИВ означет, что не все формулы выводимы из аксиом. В связи с этим имеет смысл рассмотреть следующий вопрос: нельзя ли расширить систему аксиом так, чтобы расширенная система оставалась непротиворечивой? Другими словами, если взять какую-либо невыводимую схему и добавить ее к списку аксиом, будет ли полученная теория противоречивой? В связи с этим

Определение. Непротиворечивая формальная аксиоматическая теория называется *внутренне полной*, если добавление к ее системе аксиом любой недоказуемой схемы нарушает внутреннюю непротиворечивость теории. Это свойство называется еще полнотой в узком смысле.

Можно понять, что в применении к ИВ это определение тесно связано с вопросом, все ли тавтологии доказуемы.

Дальнейшие рассмотрения направлены на установление полноты ИВ; попутно будет получено описание класса формальных теорем ИВ.

Лемма о связи таблиц истинности и выводимости. Для четырех основных логических связок $\wedge$, $\vee$, $\Rightarrow$, $\neg$ с каждой строкой соответствующей таблицы истинности связано отношение выводимости по следующему правилу: из букв или их отрицаний выводима формула или ее отрицание; при этом берется отрицание буквы, если она входит в данную строку со значением 0, берется сама буква, если ее значение в строке - 1, берется отрицание формулы, если ее значение в данной строке - 0, сама формула, если значение - 1. Например, для конъюнкции:

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

$$\neg X, \neg Y \vdash \neg(X \wedge Y)$$
$$\neg X, Y \vdash \neg(X \wedge Y)$$
$$X, \neg Y \vdash \neg(X \wedge Y)$$
$$X, Y \vdash X \wedge Y$$

Подобные соотношения выводимости имеются для каждой строки каждой связки - всего 14 утверждений выводимости.

Доказательство. Рассмотрим выписанные соотношения для конъюнкции. Очевидно, что

1. $X \wedge Y \vdash X$; удаление конъюнкции
2. $\neg X \vdash \neg(X \wedge Y)$; л. противопол. т. 1,

откуда следует первая строка таблицы. Вторая и третья - то же самое, четвертая - введение конъюнкции. Большинство других утверждений тоже доказывается просто, поэтому докажем только соотношение, соответствующее первой строке таблицы дизъюнкции, то есть докажем, что $\neg X, \neg Y \vdash \neg(X \vee Y)$.

1. $\neg X, \neg Y, X \vdash \neg(X \vee Y)$; л. о против.
2. $\neg X, \neg Y, Y \vdash \neg(X \vee Y)$; л. о против.
3. $\neg X, \neg Y, X \vee Y \vdash \neg(X \vee Y)$; удаление дизъюнкции 1, 2
4. $\neg X, \neg Y, X \vee Y \vdash X \vee Y$; тождеств.
5. $\neg X, \neg Y \vdash \neg(X \vee Y)$; введение отрицания 3, 4 •

Теорема 3 – о связи таблиц истинности и выводимости. Пусть $\mathcal{F}$ - произвольная формула ИВ, включающая n пропозициональных символов: $\mathcal{F} = \mathcal{F}(X_1, X_2, \ldots X_n)$. Тогда существует 2^n отношений выводимости, соответствующих каждой строке таблицы значений данной формулы по правилам, описанным в предыдущей лемме.

Доказательство. Проведем индукцию по количеству k логических связок, использованных в формуле. При $k = 1$ все следует из леммы; пусть $k > 1$. Тогда по правилам построения формулы можно считать, что, например, $\mathcal{F} = \mathcal{G} \wedge \mathcal{H}$, где $\wedge$ - последняя логическая связка, использованная в $\mathcal{F}$. Для других связок рассуждения аналогичны. Тогда $\mathcal{G}$ и $\mathcal{H}$ имеют меньше k логических связок. Рассмотрим теперь произвольную строку значений из таблицы $\mathcal{F}$. По этой строке строится набор букв X_i или их отрицаний. Формулы $\mathcal{G}$ и $\mathcal{H}$ можно без ограничения общности считать зависящими от того же набора переменных, что и сама формула $\mathcal{F}$, и по предположению индукции они или их отрицания выводятся из описанного набора букв X_i или отрицаний. Но значение $\mathcal{F}$ на выбранной строке определяется значениями $\mathcal{G}$ и $\mathcal{H}$, и в силу леммы $\mathcal{F}$ или отрицание $\mathcal{F}$ выводится из букв $\mathcal{G}$ и $\mathcal{H}$ или отрицаний. Тогда в силу теоремы транзитивности $\mathcal{F}$ или отрицание $\mathcal{F}$ выводится из описанного набора X_i или их отрицаний $\bullet$

Следствие 1. Тавтология $\mathcal{F} = \mathcal{F}(X_1, X_2, \ldots X_n)$ выводится из набора букв X_i или их отрицаний, построенного по произвольному 0-1 - вектору длины n $\bullet$

Если бы удалось исключить эти наборы условий, получилась бы теорема о доказуемости любой тавтологии. Это действительно можно сделать.

Лемма о законе исключенного третьего: $\vdash A \vee \neg A$.

Доказательство.

1. $X \vdash \neg X \vee X$; $\vee$-введение
2. $\neg(\neg X \vee X) \vdash \neg X$; лемма о против. т. 1.
3. $\neg X \vdash \neg X \vee X$; $\vee$-введение
4. $\neg(\neg X \vee X) \vdash \neg\neg X$; л. п. т. 3.
5. $\vdash \neg\neg(\neg X \vee X)$; $\neg$ - введение 2., 4.
6. $\vdash \neg X \vee X$; $\neg$ - удаление 5 $\bullet$

Теорема 4 – о полноте относительно тавтологий: для любой формулы $\mathcal{F}$ ИВ если $\models \mathcal{F}$, то $\vdash \mathcal{F}$.

Доказательство. Пусть $\mathcal{F}$ содержит только два пропозициональных символа: $\mathcal{F} = \mathcal{F}(X, Y)$. Рассуждения в общем случае аналогичны. Тогда в силу следствия 1 справедливы следующие отношения выводимости:

1. $\neg X, \neg Y \vdash \mathcal{F}$
2. $\neg X, Y \vdash \mathcal{F}$
3. $X, \neg Y \vdash \mathcal{F}$
4. $X, Y \vdash \mathcal{F}$.

Тогда из первых двух строк заключаем по правилу удаления дизъюнкции:

5. $\neg X,\ Y \vee \neg Y \vdash \mathcal{F}$.

Из третьей и четвертой строки - аналогично:

6. $X,\ Y \vee \neg Y \vdash \mathcal{F}$.

Теперь из строк 5 и 6 снова по правилу удаления дизъюнкции:

7. $X \vee \neg X,\ Y \vee \neg Y \vdash \mathcal{F}$.

По лемме о законе исключенного третьего $\vdash \mathcal{A} \vee \neg \mathcal{A}$. Тогда по теореме транзитивности выводимости получаем окончательно: $\vdash \mathcal{F}$ $\bullet$

Суть этой теоремы совершенно очевидна: если какая-то формула доказывается и при выполнении условия X и при его невыполнении, а остальные условия при этом неизменны, то условие X не играет никакой роли и его можно исключить. В общем случае n переменных происходит такое же попарное взаимное уничтожение условий.

Отметим, что теорема о дедукции, о десяти правилах и все последующие доказаны *конструктивно*, то есть в этих теоремах не просто доказывалось существование выводов, но и давались алгоритмы их построения. Например, можно написать программу (и это сделано), которая по любой тавтологии построит ее вывод из аксиом.

Отметим одно следствие теоремы 4. Можно дать критерий выводимости формулы из набора условий:

Следствие. Формула F выводится из набора условий $G_1, \dots G_n$ тогда и только тогда, когда формула $(G_1 \Rightarrow (G_2 \Rightarrow (G_3 \dots (G_n \Rightarrow F))...)$ тождественно истинна.

Доказательство. n раз применить теорему о дедукции и затем теорему 4 •

8.4 Полнота исчисления высказываний

Теперь получено полное описание класса формальных теорем ИВ.

Теорема 5. Произвольная формула $\mathcal{F}$ исчисления высказываний доказуема тогда и только тогда, когда она тождественно истинна.

Доказательство. Следствие теорем 1 и 4 •

Таким образом, в исчислении высказываний имеется алгоритм распознавания выводимости данной формулы - очень простой: надо построить таблицу значений формулы и посмотреть, все значения равны 1 или нет. Такие теории называются *разрешимыми.* Но в исчислении высказываний имеется, как отмечалось ранее, даже алгоритм построения самого доказательства, хотя и весьма сложный. Отметим, что не для всякой разрешимой теории имеется алгоритм построения вывода, другими словами, про формулу можно знать, что она выводима, но как построить вывод - неизвестно. Но для ИВ такое невозможно, для нее выполнены все «хорошие» свойства. Одно из важных свойств еще не доказано.

Теорема 6. Исчисление высказываний внутренне полно.

Доказательство.

Требуется доказать, что добавление любой недоказуемой формулы в качестве схемы к системе аксиом нарушает непротиворечивость. Пусть $\mathcal{F}(X_1, X_2, \ldots X_n)$ некоторая недоказуемая формула, добавленная к списку аксиом. В силу недоказуемости $\mathcal{F}$ - не тавтология. Согласно т. 4. на некотором наборе значений X_i значение $\mathcal{F}$ равно 0. Зададим следующие формулы: $Z_i = Y \Rightarrow Y$, если значение X_i на выбранной строке равно 1, и $Z_i = \neg(Y \Rightarrow Y)$, если значение X_i равно 0, и рассмотрим формулу: $\mathcal{F}(Z_1, Z_2, \ldots Z_n)$. Эта формула содержит один пропозициональный символ Y и тожественно ложна. Действительно, напомним, что формула $Y \Rightarrow Y$ тождественно истинна, и потому значения Z_i независимо от значений Y всегда будут совпадать со значениями сооветствующих X_i на выбранной строке. Формула $\mathcal{F}(Z_1, Z_2, \ldots Z_n)$ является частным случаем аксиомы и по определению доказуема. Но ее отрицание тождественно истинно и потому выводится даже из первоначального списка аксиом согласно т. 4, а значит, и из расширенного. Таким образом получаем, что из нового списка аксиом выводится как частный случай новой аксиомы, так и ее отрицание, то есть нарушена непротиворечивость теории •

8.5 Замечания

Рассмотренная формальная теория оказалась непротиворечивой, полной и даже разрешимой - есть алгоритм распознавания выводимости формулы из аксиом; есть даже алгоритм построения этого вывода. Надо отметить, что это практически единственный случай в математике из всех изучавшихся формальных систем, когда выполнено такое количество свойств. Связано это, видимо, с исключительной простотой предмета изучения - высказываний.

Отметим еще одно свойство системы аксиом - независимость.

Аксиоматика формальной теории называется независимой, если ни одна из аксиом не выводится из остальных.

Естественно, эта проблема не столь принципиальна, как непротиворечивость или полнота, но все же, если какая-то аксиома выводится из остальных, то это не аксиома, а теорема, и можно обойтись меньшим количеством аксиом, ничего не потеряв в классе выводимых формул.

Аксиоматика, предолженная здесь для ИВ, является независимой. Для доказательства того, что одна аксиома не выводится из остальных, надо найти свойство, которым обладают все остальные аксиомы и следствия из них, а изучаемая аксиома данного свойства не имеет. Провести такое исследование для каждой из десяти аксиом на достигнутом уровне изучения ИВ не слишком сложно, но здесь оно не приводится, частично и из-за следующего замечания.

Можно было бы выбрать другую систему аксиом, равносильную исходной в том смысле, что класс доказуемых формул был бы тот же самый. Действительно, возможны другие аксиоматизации с меньшим количеством первичных связок и аксиом. Возможна даже аксиоматизация с единственной схемой аксиом и с первичными связками $\neg$ и $\Rightarrow$. При этом дизъюнкция является просто сокращенной записью следующей формулы: $X \vee Y = \neg X \Rightarrow Y$, конъюнкция - $X \wedge Y = \neg(X \Rightarrow \neg Y)$. Единственная схема аксиом оказывается при этом весьма громоздкой.

Некоторые из отмеченных утверждений изложены в конце данного раздела в виде ряда задач.

Приведенная же система наиболее близка шаблонам рассуждений человека. Кроме того, из этой системы аксиом минимальным перестроением можно получить *интуиционистское* исчисление высказываний, весьма важное для анализа алгоритмов. Система аксиом ИИВ получается, если формулу $\mathcal{A} \Rightarrow (\neg\mathcal{A} \Rightarrow \mathcal{B})$ взять в качестве схемы вместо десятой аксиомы - удаления отрицания, остальные аксиомы оставить такими же, и вообще все остальные элементы определения формальный теории оставить неизменными. Получится *неклассическая* логика - в ней неверен закон исключенного третьего, неверен закон удаления отрицания, который был исключен из списка аксиом, и вообще многое непривычно.

Геометрия Лобачевского тоже отличается от классической евклидовой только одной аксиомой и тоже вначале кажется непривычной: как это - через точку вне прямой проходит более одной прямой, не пересекающей данную?.. Просто эта геометрия описывает другой мир и логика ИИВ - тоже.

Начала ИИВ также даны в виде нескольких задач в конце раздела.

Для других аксиоматических теорий доказать такие свойства, какие имеются для ИВ, удается редко. Для множеств трудности аксиоматизации немного обсуждались ранее; для арифметики, даже наоборот, доказано (К. Гедель), что **если** аксиоматика арифметики непротиворечива, то она не полна и даже не пополняема, то есть, добавляя в систему аксиом любые формулы, полную систему не получить. Все это, видимо, указывает на содержательность математических теорий и принципиальную невозможность их полного формального описания.

9 Логика предикатов

9.1 Предикаты

Мы познакомимся с еще одной формальной аксиоматической теорией, посвященной логике, - исчислением предикатов. Исчисление предикатов гораздо сложнее, чем ИВ, поэтому изложение не будет полным. Как и исчисление высказываний, исчисление предикатов (ИП) разрабатывалось как средство формализации математических рассуждений. Можно сказать, что ИП является детализацией исчисления высказываний и его возможности, в отличие от средств ИВ, в принципе достаточны для адекватного описания любых математических рассуждений.

В основе ИВ лежало понятие высказывания, то есть предложения, которому можно приписать одно из двух возможных истинностных значений. Предполагалось, что все высказывания относятся к одной и той же математической теории, и поэтому их можно соединять логическими связками и получать при этом новые осмысленные высказывания. Совершенно такой же подход будет проводиться и сейчас, только теперь в основе дальнейших построений лежат *предикатные* предложения.

Предикатное предложение - предложение, зависящее от нескольких *предметных* переменых. Переменные могут принимать значения из некоторой *предметной области*, и при каждом конкретном наборе значений предикатное предложение становится высказыванием, истинным или ложным.

Предложение $x < y$ - предикатное предложение. Считаем, что переменные x и y принадлежат множеству натуральных чисел $\mathbb{N}$. Этот пример чисто математический, даже написан на языке математических обозначений, но это не принципиально. Действительно, для любой конкретной пары значений x и y, например 7, 4, получается высказывание, в данном случае ложное: $7 < 4$. Если бы были выбраны числа 1 и 2, получилось бы высказывание $1 < 2$, истинное. Таким образом, говоря математическим языком, предикат это функция, в данном примере от двух переменных x и y. Поэтому ИП ещё называют функциональным исчислением.

Должно быть понятно, что практически любая математическая формулировка содержит предикаты от разного количества переменных.

Предикатные предложения от одного переменного еще называют свойствами. Пусть снова x принадлежит множеству натуральных чисел $\mathbb{N}$, тогда примерами свойств будут предложения типа: x делится на 3, x больше 1. Допустимым вырожденным случаем предикатного предложения будет предложение, не зависящее вообще от предметных переменных – это высказывание.

Таким образом, предикатное предложение задает функцию от n предметных переменных, значениями которой являются высказывания.

В связи с этим

Определение. Пусть G - произвольное непустое множество, называемое *предметной областью.* Предикатом P от n переменных на области G называется функция $P: G^n \to F_2$ со значениями 0 или 1.

Каждому предикату соответствует некоторая *область истинности* - подмножество множества G^n, для элементов которого

$$P(x_1, x_2, \dots x_n) = 1$$

Область истинности определяет на G n-арное отношение (см. гл. 2), которым предикат однозначно определяется.

Понятно, что каждому предикатному предложению соответствует предикат. Как высказывания в ИВ обозначались пропозициональными символами, так и в исчислении предикатов предикаты будут обозначаться предикатными символами, затем из них при помощи связок и кванторов будут строиться новые предикаты.

Дадим соответствующие точные определения.

9.2 Алфавит и формулы исчисления предикатов

Напомним, что для определения формальной аксиоматической теории требуется четыре элемента: алфавит, формулы, аксиомы, правила вывода. Определим эти элементы для ИП, сначала - алфавит и формулы.

Алфавит состоит из следующих символов: прямые прописные буквы латинского алфавита $A, B, \dots Z$, или буквы с индексами, например, $A_1, B_k, \dots$ (чтобы иметь неограниченный набор символов), называемые *предикатными* *буквами*; символы предметных переменных - строчные латинские буквы $a, b, \ldots x, y, z$ или буквы с индексами $x_i, a_1, \ldots$, логические связки - $\wedge$, $\vee$, $\neg$, $\Rightarrow$, кванторы - $\forall$, $\exists$, скобки (,).

Отличие алфавита ИП от алфавита исчисления высказываний - в наличии предметных переменных и кванторов.

Замечание об индексах - такое же, как для ИВ.

Формулы. Элементарная предикатная формула - это предикатная буква с приданными переменными: например, $A(x, y)$, $A(t, t)$, $B(x_1, x_2, x_3)$, $A(z)$ и т. п.

1. Элементарная предикатная формула есть формула.

2. Если $\mathcal{A}$ и $\mathcal{B}$ - формулы, x - произвольная предметная переменная, то следующие слова также являются формулами: $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\neg\mathcal{A})$, $(\mathcal{A} \Rightarrow \mathcal{B})$, $(\forall x\mathcal{A})$, $(\exists x\mathcal{A})$.

Часть формулы, заключенная в скобки при использовании квантора, называется *областью действия квантора.*

В дальнейшем при написании формулы будем изображать лишь необходимое количество скобок, позволяющее однозначно восстановить формулу. При этом сохраняем те соглашения об областях действия логических связок, которые имелись в ИВ.

Области действия кванторов считаем наименьшими возможными, например формула $\forall x A(x, y) \Rightarrow B(x)$ есть сокращенная запись для формулы $((\forall x A(x, y)) \Rightarrow B(x))$. Если же требуется, чтобы область действия квантора по x охватывала всю импликацию, в сокращенной записи надо написать соответствующие скобки: $\forall x(A(x, y) \Rightarrow B(x))$, в полной - соответственно $(\forall x(A(x, y) \Rightarrow B(x)))$.

9.3 Свободные и связанные вхождения и подстановки

Прежде чем давать список аксиом, необходимы предварительные определения.

Напомним, что любая формула есть просто слово в данном алфавите, построеннное по определенным правилам. То есть формула есть некоторая последовательность символов алфавита.

Вхождение предметной переменной x в формулу есть элемент последовательности, равный x. Например, в слове $\forall x A(x, y) \Rightarrow B(x)$ имеются три вхождения x.

Определение. Некоторое вхожение переменной x в формулу называется *связанным*, если оно находится в области действия квантора по x. Вхождение, не являющееся связанным, называется *свободным*.

В последней приведенной формуле первое и второе вхождения x являются связанными, третье - свободным. Вхождение y в данную формулу является свободным, так как это вхождение не находится в области действия квантора по y - в формуле вообще нет кванторов по y, хотя y и лежит в области действия квантора по x. Если формула не содержит свободных вхождений данной переменной x, то говорят короче: формула не зависит от x. Например, $\forall x(A(x, y) \Rightarrow B(x))$ не зависит от x.

Если формула F содержит свободные вхождения переменной x, то можно произвести *подстановку* новой неизвестной t вместо x. Подстановка есть замена всех **свободных** вхождений x на t.

Чтобы указать замену t вместо x в формуле F, будем использовать следующие обозначения - вместо F обозначим исходную формулу через $F(x)$, формулу, получившуюся в результате замены, – через $F(t)$. Отметим, что если F не содержит свободных вхождений x, то $F = F(x) = F(t)$, так как t никуда не будет подставлено.

Но вообще может быть два случая: либо все вхождения переменной t, **возникшие в результате подстановки,** являются свободными, либо не все. В первом случае подстановка t вместо x называется свободной, во втором - нет. Другими словами, подстановка t вместо x называется свободной, если все свободные вхождения x не находятся в области действия квантора по t. Например, подстановка в формулу $\forall x(A(x,y) \Rightarrow B(x))$ t вместо y свободна, подстановка же x вместо y не свободна. Результат подстановки в первом случае: $\forall x(A(x,t) \Rightarrow B(x))$, во втором - $\forall x(A(x,x) \Rightarrow B(x))$. Разница между формулами в том, что в формуле, возникшей после первой подстановки, вхождение t свободно, а третье вхождение x во второй формуле, возникшее в результате подстановки, связанное. Ещё пример. Подстановка t вместо x в формулу $A(t) \Rightarrow \exists y(B(x) \vee \forall tC(t,y))$ приводит к результату $A(t) \Rightarrow \exists y(B(t) \vee \forall tC(t,y))$. Эта подстановка свободна, так как второе вхожение t, получающееся в результате подстановки, свободно.

9.4 Аксиомы и правила вывода

Теперь получены необходимые технические понятия, требующиеся в дальнейших определениях, и можно определить два оставшихся элемента новой формальной теории - аксиомы и правила вывода.

Аксиомы. Список содержит 12 схем аксиом, первые 10 текстуально те же, что и для исчисления высказываний:

Введение логических связок	Удаление логичеких связок
1. $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A})$	2. $(\mathcal{A} \Rightarrow \mathcal{B})$ $\Rightarrow ((\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \Rightarrow (\mathcal{A} \Rightarrow \mathcal{C}))$
3. $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{A} \wedge \mathcal{B})$	4. $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{A}$ 5. $\mathcal{A} \wedge \mathcal{B} \Rightarrow \mathcal{B}$
6. $\mathcal{A} \Rightarrow \mathcal{A} \vee \mathcal{B}$ 7. $\mathcal{B} \Rightarrow \mathcal{A} \vee \mathcal{B}$	8. $(\mathcal{A} \Rightarrow \mathcal{C})$ $\Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$
9. $(\mathcal{A} \Rightarrow \mathcal{B}) \Rightarrow ((\mathcal{A} \Rightarrow \overline{\mathcal{B}}) \Rightarrow \overline{\mathcal{A}})$	10. $\overline{\overline{\mathcal{A}}} \Rightarrow \mathcal{A}$

Отличие от ИВ в том, что теперь вместо букв в схемы можно вписывать любые формулы исчисления предикатов. Кроме того, имеются две аксиомы, использующие кванторы:

11. $\forall x A(x) \Rightarrow A(t)$,

где $A(x)$ - любая такая формула, что подстановка t вместо x свободна; называется $\forall$-схема или аксиома всеобщности.

12. $A(t) \Rightarrow \exists x A(x)$,

где $A(x)$ - любая такая формула, что подстановка t вместо x свободна; называется $\exists$-схема или аксиома существования.

Правила вывода:

1. Правило МР текстуально такое же, как в ИВ: из $\mathcal{X}, \mathcal{X} \Rightarrow \mathcal{Y}$ непосредственно выводится $\mathcal{Y}$, теперь применяется для формул ИП.

2. $\forall$-правило: из формулы $C \Rightarrow A(x)$ непосредственно выводится формула $C \Rightarrow \forall x A(x)$; если C не содержит свободных вхождений x (не зависит от x).

3. $\exists$-правило: из формулы $A(x) \Rightarrow C$ непосредственно выводится формула $\exists x A(x) \Rightarrow C$, если C не содержит свободных вхождений x (не зависит от x).

Теперь определение исчисления предикатов завершено.

9.5 Примеры простейших доказательств

Мы не будем рассматривать теорию доказательств для ИП, которая содержит аналог теоремы о дедукции, теоремы о различных выводимых правилах и т. п., - все это выходит за рамки данного пособия. Мы дадим лишь простейшие примеры формальных доказательств и выводов из условий в исчислении предикатов. Напомним, что определения этих понятий были даны в общем виде - в применении к любой аксиоматической теории. В частности, будет использоваться обозначение $\mathcal{G} \vdash F$, если формула F выводится из набора условий $\mathcal{G}$, может быть пустого.

Правило переименования свободных переменных.

Пусть подстановка y вместо x в формуле $F(x)$ свободна, тогда если $F(x)$ доказуема, то и $F(y)$ доказуема.

Доказательство. Докажем, что $F(x) \vdash F(y)$.

1. $F(x)$; условие

2. $F(x) \Rightarrow (G \Rightarrow F(x))$; схема аксиом 1. - $\Rightarrow$-введение, в качестве G выберем любую доказуемую формулу, не зависящую от x.

3. $G \Rightarrow F(x)$; MP 1., 2.

4. $G \Rightarrow \forall x F(x)$; $\forall$-правило, примененное к 3.

5. G ; доказуемо по выбору.

6. $\forall x F(x)$; MP 5., 4.

7. $\forall x F(x) \Rightarrow F(y)$; $\forall$-аксиома.

8. $F(y)$; MP 6., 7.

Построенная последовательность является выводом формулы $F(y)$ из формулы $F(x)$: $F(x) \vdash F(y)$. По условию $\vdash F(x)$, а тогда по теореме транзитивности выводимости $\vdash F(y)$ $\bullet$

Первое правило переименования связанных переменных.

Пусть 1) - подстановка y вместо x в формуле $F(x)$ свободна и 2) - $F(x)$ не зависит от y. Тогда если $\forall x F(x)$ доказуема, то $\forall y F(y)$ доказуема.

Доказательство. Докажем, что $\forall x F(x) \vdash \forall y F(y)$.

1. $\forall x F(x)$; условие.

2. $\forall x F(x) \Rightarrow F(y)$; $\forall$-схема акс. 11, усл. 1).

3. $\forall x F(x) \Rightarrow \forall y F(y)$; $\forall$-правило, примененное к 2. Отметим, что в силу условия 2) $\forall x F(x)$ не зависит от y.

4. $\forall y F(y)$; MP 1, 3 $\bullet$

Второе правило переименования связанных переменных.

Пусть 1) подстановка y вместо x в формуле $F(x)$ свободна и 2) $F(x)$ не зависит от y. Тогда если $\exists x F(x)$ доказуема, то $\exists y F(y)$ доказуема.

Доказательство. Докажем, что $\exists x F(x) \vdash \exists y F(y)$.

Сначала докажем, что при условиях 1) и 2) подстановка x вместо y в формулу $F(y)$ свободна. Действительно, все свободные вхождения y в $F(y)$ появились в результате подстановки y вместо x в силу 2). В силу 1) все свободные вхождения x были заменены на свободные вхождения y. Поэтому подстановка x в $F(y)$ произойдет на места всех исходных свободных вхождений x в $F(x)$. Это значит, что подстановка x в $F(y)$ свободна и результат ее - исходная формула $F(x)$.

1. $\exists x F(x)$; условие.

2. $F(x) \Rightarrow \exists y F(y)$; $\exists$-схема акс. 12; замечание о свободе подстановки x вместо y.

3. $\exists x F(x) \Rightarrow \exists y F(y)$; $\exists$-правило вывода, примененное

к 2. Правило применимо, так как $\exists y F(y)$ не зависит от x.

4. $\exists y F(y)$; MP 1, 3 $\bullet$

10 Интерпретация формул логики предикатов

10.1 Определения

Полное длинное определение исчисления предикатов было приведено для того, чтобы можно было доказать хотя бы одну содержательную теорему для исчисления. Это будет теорема о непротиворечивости ИП и один пример, показывающий принципиальную разницу между исчислением высказываний и исчислением предикатов.

Вспомним, что для доказательства непротиворечивости ИВ каждой формуле была сопоставлена определенная булева функция. При этом оказалось, что всем доказуемым формулам соответствуют тождественно истинные функции, и потому ИВ оказалась непротиворечивой.

Конечно, смысл рассмотрения булевых функций не только в том, что с их помощью можно доказать непротиворечивость. Булевы функции дают точное определение понятия **истинности**, с их помощью возможно истолковать, *интерпретировать* аксиомы, как основные истины, из которых остальные истины выводятся.

Можно всю теорию высказываний изложить на основе понятия истинности и соответствующих таблиц значений, только это уже была бы не формальная аксиоматическая теория, это было бы действительно «исчисление».

Для доказательства непротиворечивости ИП тоже можно идти путём *интерпретации*, то есть определить некую процедуру сопоставления каждой формуле ИП **предиката** - аналогично подходу, проведенному в ИВ. Снова можно отметить, что это сопоставление даст строгое формальное определение истинности предикатных формул, снова аксиомы будут выступать как основные истины, только, в отличие от ИВ, исчисление предикатов не сводится к вычислениям по конечным таблицам.

Опишем процедуру, называющуюся *интерпретацией*, сопоставляющую каждой формуле ИП предикат от всех свободных переменных, входящих в формулу.

Для задания интерпретации требуются следующее:

1. Предметная область – непустое множество D. Предполагается, что **в данной интерпретации** все предметные переменные будут принимать значения из этого множества.

2. Каждой элементарной предикатной формуле F (предикатной букве с приданными переменными) ставится в соответствие какой-то предикат $I(F)$ от соответствующего количества переменных на предметной области (множестве D). В вырожденном случае, когда элементарная предикатная формула имеет 0 приданных переменных, ей сопоставляется один из символов - 0 или 1.

Тем самым каждой элементарной предикатной формуле уже поставлен в соответствие предикат от свободных переменных этой формулы (а других переменных в таких формулах нет).

Для остальных формул ИП соответствующий предикат уже однозначно определяется по следующим правилам.

Каждая формула C ИП имеет один из следующих видов:

$A \wedge B$, $A \vee B$, $(\neg A)$, $(A \Rightarrow B)$, $(\forall x A)$, $(\exists x A)$, где формулы A и B имеют меньшее количество логических связок и кванторов.

Проводим индукцию по общему количеству k связок и кванторов в формуле. При $k = 0$ формула – элементарная и ее интерпретация имеется. Пусть формула имеет вид $C = (A \wedge B)$. Тогда формулы A и B имеют меньшее количество связок и у каждой из них свой набор свободных переменных - $\{x_1, x_2, \dots x_n\}$ в формуле A и $\{y_1, y_2, \dots y_m\}$ в формуле B. По построению формулы C её набор свободных переменных есть объединение наборов x_i и y_j, и пусть задан произвольный фиксированный набор значений всех этих переменных. Заданием этих значений определяются наборы значений переменных x_i и y_j. По предположению индукции, тем самым однозначно определяются булевские значения формул A и B, точнее, значения тех предикатов $I(A)$ и $I(B)$, которые соответствуют этим формулам. Тогда, по определению, значение предиката $I(C)$ вычисляется как соответствующее табличное значение конъюнкции: $I(C) = I(A) \wedge I(B)$.

В действительности, все это описание сводится просто к естественному вычислению по структуре формулы. Точное различение формулы C и соответствующего ей предиката $I(C)$ будет отмечаться явно, когда, например, рассматриваются две интерпретации: $I_1(C)$ и $I_2(C)$, и в других необходимых случаях. Когда же это не приведёт к непониманию, будем ради краткости допускать вольность речи и говорить про значения формулы C на заданном наборе значений переменных, имея в виду, что формуле C соответствует предикат с тем же обозначением.

Для оставшихся логических связок вычисление значений определяется аналогично.

Рассмотрим кванторы.

Пусть формула C имеет вид: $C = (\forall x A)$ или $C = (\exists x A)$. Пусть формула A зависит от n свободных пермен-ных: $\{x_1, x_2, \dots x_n\}$. Если среди них нет переменной x, то $C = (\forall x A) = A$. Это описание вырожденного случая, когда квантор взят по переменной, свободных вхождений которой в формуле нет.

Пусть $x = x_n$; номер переменной, конечно, не имеет значения в последующих построениях. Тогда формула $C = (\forall x A)$, по определению свободного вхождения переменной, имеет свободные вхождения только $n - 1$ переменного: $\{x_1, x_2, \dots x_{n-1}\}$, и ей будет соответствовать предикат от этих переменных. Пусть взят некоторый набор значений указанных переменных из предметной области: $\{d_1, d_2, \dots d_{n-1}\}$, $\forall i\ d_i \in D$. Значение $C = (\forall x A)$ на данном наборе равно 1 тогда и только тогда, когда значение A равно 1 на любом наборе значений вида:

$$\{d_1, d_2, \dots d_{n-1}, d\}\ \forall\ d \in D.$$

Другими словами, C равно 1 на выбранном наборе значений тогда и только тогда, когда **на любом** расширении этого набора значений произвольным значением последней переменной исходная формула A равна 1.

Действительно, определение вполне естественно: формула $(\forall x A)$ равна 1 тогда и только тогда, когда формула A равна 1 при всех значениях x, остальные переменные при этом фиксированы.

Для формулы $C = (\exists x A)$ все совершенно аналогично: она равна 1 на некотором наборе значений $\{d_1, d_2, \dots d_{n-1}\}$, $\forall i\ d_i \in D$ тогда и только тогда, когда формула A равна 1 на **некотором** расширении этого набора, полученном присоединением значения последней переменной x_n.

Как условились ранее, в приведенных определениях допущены выражения вида «значение формулы A» вместо более точного $I(A)$ и т. п., кроме того, в дальнейшем внешние скобки в формулах будем для краткости опускать.

Теперь процедура интерпретации определена полностью.

10.2 Примеры задания интерпретации

Для построения интерпретации требуется задать предметную область D и каждой предикатной букве сопоставить предикат на D от соответствующего количества переменных. Пусть предметная область $D = \{a, b, c\}$ состоит из трех произвольных символов. Для краткости будем рассматривать только предикатные буквы, имеющиеся в формуле $F = \exists y(A(x) \Rightarrow \forall x B(x, y))$, и построим предикат $I(F)$.

Сначала, по определению интерпретации, надо элементарным формулам $B(x, y)$ и $A(x)$ сопоставить некоторые предикаты на области D от двух или одного переменного соответственно:

x	y	$B(x,y)$
a	a	1
a	b	1
a	c	1
b	a	0
b	b	1
b	c	1
c	a	1
c	b	0
c	c	1

x	$A(x)$
a	1
b	1
c	0

Теперь можно вычислять подформулы формулы F:

y	$\forall x B(x,y)$
a	0
b	0
c	1

Как получено, например, значение 0 в первой строке? По определению интерпретации квантора всеобщности были рассмотрены первая, четвертая и седьмая строки в таблице для $B(x,y)$, в которых значение y равно a. Оказалось, что не во всех из них значение $B(x,y)$ равно 1. Поэтому значение формулы с квантором считаем равным 0. Аналогично получены остальные две строки значений.

Теперь построим таблицу значений для формулы
$A(x) \Rightarrow \forall x B(x,y)$.

Эта формула задает предикат от двух переменных - x и y (объединение свободных переменных составляющих подформул):

x	y	$A(x) \Rightarrow \forall x B(x,y)$
a	a	0
a	b	0
a	c	1
b	a	0
b	b	0
b	c	1
c	a	1
c	b	1
c	c	1

Эта таблица получена как таблица импликации из A в B, что и было еще раз указано перед её построением. Построим таблицу значений всей формулы F:

$$F = \exists y (A(x) \Rightarrow \forall x B(x,y))$$

:

x	$\exists y(A(x) \Rightarrow \forall x B(x,y))$
a	1
b	1
c	1

Формула оказалась тождественно истинной в данной интерпретации. Если изменить таблицы для $A(x)$ и $B(x,y)$, получили бы на той же предметной области D вообще говоря, другую интерпретацию формулы F, она получила бы другую таблицу значений.

Ясно, что количество различных интерпретаций данной формулы на данном конечном множестве конечно. Действительно, например, для задания интерпретации формулы F необходимо определить два предиката на D – одноместный для буквы A и двухместный для буквы B. Очевидно, количество различных одноместных предикатов на D равно 2^3, двухместных – 2^9, количество пар - 2^{12}.

Кроме того, ясно, что количество различных интерпретаций данной формулы на конечном множестве определяется только количеством элементов $|D|$ в данном множестве и не зависит от того, из каких элементов состоит D.

Иногда формула может оказаться тождественно истинной при любой интерпретации на данном множестве D. Простейший пример: формула $\exists x A(x) \Rightarrow \forall x A(x)$ тождественно истинна на любой области из одного элемента. Грубо «по смыслу» формулы: если существует значение x, для которого $A(x)$ истинно, то $A(x)$ будет истинно и для всех x, потому что возможных значений x в нашей интерпретации всего одно.

Можно придумать формулу, которая будет тождественно истинной при любой интерпретации на двухэлементном множестве, например достаточно в формулу $\mathcal{X} \Rightarrow \mathcal{X}$ вместо $\mathcal{X}$ вписать **любую** формулу ИП. В силу того что схема, в которую подставляются формулы, тождественно истинна, полученная формула тоже будет тождественно истинной. Ясно, что такая формула будет тождественно истинной при любой интерпретации на любом множестве вообще.

Определение. Формула $\mathcal{F}$ исчисления предикатов называется *общезначимой*, если она тождественно истинна при любой интерпретации на любой предметной области. Обозначение: $\models \mathcal{F}$.

В связи с данным определением интересен такой вопрос: можно ли придумать не общезначимую формулу, которая была бы все же тождественно истинна при любой интерпретации на любом двухэлементном множестве?

Назовем формулу k-общезначимой, если она тождественно истинна при любой интерпретации на любом множестве, имеющем не более k элементов. Тогда возникают следующие вопросы: существуют ли k-общезначимые, но не $k+1$-общезначимые формулы? Существуют ли формулы, k-общезначимые для любого k, но не общезначимые?

Второй вопрос - фактически о том, нужно ли для проверки истинности формул ИП «уходить в бесконечность», то есть рассматривать бесконечные предметные области, - весьма важен; в дальнейшем он будет решен.

Рассмотрим пример с бесконечной предметной областью D. Первое затруднение при этом - определение предикатов для элементарных формул. Так как прямое построение бесконечных таблиц невозможно, необходимо указать какие-то **правила** построения истинностных значений предиката для произвольных наборов значений переменных (См. [4], задачи 35,36 в конце главы).

Построение предикатов для составных формул в этом случае также не сводится к просмотру таблиц, которые теперь бесконечны, а должно быть как-то обосновано рассуждениями.

Пусть $D = \mathbb{N}$, где $\mathbb{N} = \{0, 1, 2, \dots n, \dots\}$ множество натуральных чисел. Рассмотрим две элементарные предикатные формулы $S(x, y, z)$ и $P(x, y, z)$ от трех переменных. С помощью их построим ряд формул, которые при интерпретации будут означать вполне осмысленные арифметические утверждения. Определим предикаты, соответствующие выбранным буквам: $S(x, y, z) = 1$ тогда и только тогда, когда $x + y = z$, $P(x, y, z) = 1$ тогда и только тогда, когда $x * y = z$. Таким образом, **бесконечные** таблицы заменены арифметическими формулами. Можно считать неважным, как именно задан предикат, главное, что можно вычислить его значение на произвольном наборе значений пременных (хотя это и не совсем так).

Рассмотрим простые примеры формул ИП, построенных на этих двух буквах, интерпретированных как сумма и произведение.

$\exists x \forall y S(x, y, y)$. Это так называемая *замкнутая формула* - она не имеет свободных переменных и должна представлять «предикат от 0 переменных», то есть высказывание. При данной интерпретации это высказывание истинно - оно означает, что в $\mathbb{N}$ существует элемент, нейтральный относительно сложения: $x + y = y$ для всех y

из $\mathbb{N}$. Действительно, такой элемент существует – это 0. Если бы интерпретация проводилась только на множестве положительных чисел, высказывание было бы ложным. Аналогично $\exists x \forall y P(x, y, y)$ – истинное высказывание, означающее существование 1 в $\mathbb{N}$.

Конечно, вторую (и первую) формулу можно разбирать «в строгом табличном стиле», как в примере с конечной областью D.

Формула $P(x, y, z)$ определена, теперь рассмотрим фрагмент $\forall y P(x, y, y)$. Эта подформула зависит от одного свободного неизвестного x. Построим таблицу (бесконечную) значений этой формулы. При данной интерпретации она означает: $\forall y\ (x * y = y)$. Это предикат от x. Вычисляем его для каждого значения $x \in \mathbb{N}$. Пусть сначала $x = 0$. Верно ли, что $\forall y\ (0 * y = y)$? Нет, неверно. Значит, при $x = 0$ подформула равна 0. Затем $x = 1$. Верно ли, что $\forall y\ (1 * y = y)$? Да. Значит, при $x = 1$ подформула равна 1. И так далее до бесконечности. Но уже из двух вычисленных значений одно равно 1, и потому вся формула истинна.

Это нарочитый пример, но понимание интерпретации формулы должно быть именно таковым. В книге [2] об этом говорится так: «Конечно, при больших конечных $|D|$ или очень сложных формулах вычисление может оказаться невероятно длинным. Если же область D бесконечна, истинностная таблица перестает быть конечным объектом, который теоретически можно вычислить, хотя сама идея этой таблицы остается совершенно ясной, и о ней можно рассуждать».

Еще примеры. $\exists y S(y, y, x)$ задает, очевидно, предикат от одного неизвестного x, истинный тогда и только тогда, когда x четно, $\exists z S(x, z, y)$ – $x \leq y$, $\neg(\exists y S(y, y, x))$ – x нечетно. Таким образом, имея две основные предикатные буквы, можно строить множество новых осмысленных арифметических предикатов, определяющих простоту числа, делимость одного числа на другое и т. п., формулировать теоремы арифметики – другими словами, ИП может служить основой формального языка описания математических теорий.

Для упрощения таких описаний, то есть для усиления выразительных возможностей исчисления, можно рассматривать варианты ИП, в которых, кроме предметных переменных, имеются еще предметные константы, которые тоже можно подставлять в предикатные буквы, но константы нельзя использовать с кванторами. При интерпретации каждой константе надо сопоставить фиксированный элемент предметной области. Рассматривая последний пример для такого исчисления, можно было бы каким-то символам констант присвоить значение 0, 2, 2002 ..., если именно эти константы позволят упростить формулировки. Можно, кроме того, в определение ИП вводить символы операций или функциональные буквы. Функциональные буквы зависят от нескольких предметных переменных и могут подставляться вместо предметных переменных в предикатные буквы. Функциональные буквы можно подсталять вместо переменых в другие функциональные буквы. При интерпретации каждой функциональной букве сопоставляется операция на D от соответствующего количества переменных. В нашем примере при таком подходе можно, скажем, рассмотреть на области $\mathbb{N}$ выражение $x * y + x + y$, считая его сопоставленным некоторому функциональному символу $f(x, y)$, вообще возникает возможность непосредственно строить арифметические выражения.

В нашем же *чистом* исчислении предикатов даже основные константы вроде нуля или единицы определялись косвенно при помощи формул. Однако все варианты определения ИП идейно одинаковы, зато чистое исчисление имеет самое простое описание.

Ещё некоторые другие аналогичные задачи имеются в упражнениях 34, 35.

10.3 Логическое следование и равносильность

Как отмечалось ранее, теория доказуемости для исчисления предикатов в данном пособии не будет развита в силу ее сложности, однако процедура интерпретации формул предоставляет некоторую возможность изучения выводимости и доказуемости на основе следующего определения.

Определение. Пусть имеются две формулы ИП - A и B. Говорим, что формула B является *логическим следствием* формулы A, если при любой интерпретации на любой предметной области D область истинности формулы A является подмножеством области истинности формулы B.

Обозначается это так: $A \models B$, что согласуется с предыдущим использованием этого знака, в частности если A общезначима, то и B общезначима.

Раскроем это определение.

Пусть $\{x_1, x_2, \dots x_n\}$ - объединение всех свободных переменных формул A и B. Теперь можно считать, что A и B зависят от одного и того же набора свободных переменных. Пусть задана предметная область D и некоторый набор значений $\{d_1, d_2, \dots d_n\}, \forall d_k \in D$. В определении требуется, чтобы B на данном наборе значений было истинным, если на нем истинна формула A; и нужно, чтобы это выполнялось при любой интерпретации на любой предметной области.

Легко видеть, что $A \models B$ тогда и только тогда, когда $\models A \Rightarrow B$, этим частично объясняется название «логическое следствие», хотя по смыслу это следствие, полученное в результате «проверки на модели».

Можно обобщить приведенное определение на любое количество условий и говорить, что формула B логически следует из набора формул: $A_1, A_2, \dots A_m \models B$, если при любой интерпретации пересечение областей истинности A_k содержится в области истинности формулы B.

Справедлива теорема о транзитивности отношения логической выводимости, аналогичная т. 1 гл. 6 о транзитивности выводимости.

Теорема 1. Отношение логического следования обладает свойствами рефлексивности и транзитивности:

1) $A \models A$, 2)если $A \models B$ и $B \models C$, то $A \models C$. Более того: если $A_1, A_2, \dots A_m \models B_k, k = 1, 2, \dots l$ и $B_1, B_2, \dots B_l \models C$, то $A_1, A_2, \dots A_m \models C$.

Доказательство. Свойства 1) и 2) очевидны. Докажем обобщение свойства 2) для нескольких формул. Если B_k логически следует из набора формул $A_1, A_2, \dots A_m$, это по определению означает, что для любой интерпретации пересечение областей истинности A_i является подмножеством области истинности $B_k, k = 1, 2, \dots l$. Тогда пересечение областей истинности A_i содержится в пересечениии областей истинности B_k и, значит, в области истинности C •

Напомним, что бинарные отношения со свойствами рефлексивности и транзитивности называются отношениями квазипорядка, они рассматривались в гл. 2. Отношение логического следования также, в силу теоремы 1, является квазипорядком на множестве всех формул ИП.

Понятие логического следования позволяет определить следующее отношение между формулами:

Определение. Две формулы A и B исчисления предикатов называются равносильными, если $A \models B$ и $B \models A$. Обозначается равносильность следующим знаком: $A \sim B$.

Таким образом, две формулы ИП являются равносильными тогда и только тогда, когда при любой интерпретации они определяют один и тот же предикат.

Теорема 2. Отношение равносильности есть отношение эквивалентности на множестве всех формул ИП.

Доказательство. Отношение равносильности $\sim$ является отношением ассоциированности, определенным для квазипорядка $\models$. В силу т. 6 гл. 2 такое отношение является отношением эквивалентности •

В действительности, то, что отношение равносильности является отношением эквивалентности, легко проверяется непосредственно по определению.

Отношение равносильности разбивает множество всех формул ИП на непересекающиеся классы равносильных формул (т. 5 гл. 2). В силу т. 6 гл. 2 на эти классы можно перенести отношение логического следования: класс $\overline{A} \models \overline{B} \Longleftrightarrow A \models B$.

Словесная формулировка этого определения: один класс равносильных формул является логическим следствием другого, если хотя бы одна формула первого класса является логическим следствием некоторой формулы второго класса. Тогда, конечно, и любая формула первого класса является логическим следствием любой формулы второго класса.

Понятие логического следствия, как отмечалось, позволяет выявить некоторые соотношения между формулами.

Теорема 3 – о переносе квантора через отрицание.

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

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

Доказательство. Пусть, как обычно, D - предметная область, на которой задана интерпретация формулы A, $\{x, y_1, y_2, \dots y_n\}$ - набор всех свободных переменных A. Докажем первое утверждение. Заметим, что обе формулы в нем зависят от переменных $\{y_1, y_2, \dots y_n\}$. Пусть $\{d_1, d_2, \dots d_n\}, d_k \in D$ - произвольный набор значений y_i. Требуется доказать, что формула $\neg(\forall x A)$ истинна тогда и только тогда, когда $\exists x(\neg A)$ истинна.

Может быть два случая: либо формула A истинна на всех наборах значений вида $\{d, d_1, d_2, \dots d_n\}$, $d, d_k \in D$, полученных расширениями набора значений для y_i, либо не на всех.

В первом случае формула $\forall x A$ по определению интерпретации квантора истинна на наборе $\{d_1, d_2, \dots d_n\}$, ее отрицание ложно. Формула $\neg A$ в этом случае на всех наборах $\{d, d_1, d_2, \dots d_n\}$ ложна и по определению интерпретации квантора существования формула $\exists x(\neg A)$ ложна на наборе значений $\{d_1, d_2, \dots d_n\}$, то есть левая и правая формулы принимают одинаковые значения.

Пусть теперь формула A истинна не на всех наборах значений вида $\{d, d_1, d_2, \dots d_n\}$. Другими словами, существует такое значение $d = d_0$, что A ложна на наборе значений $\{d_0, d_1, d_2, \dots d_n\}$,а $\neg A$ истинна. Тогда $\forall x A$ ложна на наборе $\{d_1, d_2, \dots d_n\}$, значит, ее отрицание истинно, и формула $\exists x(\neg A)$ истинна.

Доказательство второго утверждения теоремы совершенно аналогично •

Теорема 4 – о равносильном переносе кванторов через дизъюнкцию и конъюнкцию.

$$\forall x(A \wedge B) \sim \forall x A \wedge \forall x B.$$

$$\exists x(A \vee B) \sim \exists x A \vee \exists x B.$$

Доказательство. Пусть D - предметная область, задана интерпретация формул A и B, $\{x, y_1, y_2, \dots y_n\}$ - объединение свободных переменных A и B.

Докажем первое утверждение. Формулы $\forall x(A \wedge B)$ и $\forall x A \wedge \forall x B$ зависят от переменных $\{y_1, y_2, \dots y_n\}$. Требуется доказать, что при любом наборе значений этих переменных формулы принимают одинаковые значения.

Пусть $\{d_1, d_2, \dots d_n\}$ - произвольный набор значений y_i.

Снова два случая: либо формула $A \wedge B$ истинна на всех наборах значений вида $\{d, d_1, d_2, \dots d_n\}$, $d, d_k \in D$, полученных расширениями набора значений для y_i, либо не на всех.

В первом случае и A, и B истинны на всех таких расширениях. Тогда формулы $\forall x(A \wedge B)$, $\forall x A$ и $\forall x B$ истинны на $\{d_1, d_2, \dots d_n\}$ и, значит, формулы $\forall x(A \wedge B)$ и $\forall x A \wedge \forall x B$ истинны на этом наборе.

Второй случай: формула $A \wedge B$, зависящая от d, истинна не на всех наборах $\{d, d_1, d_2, \dots d_n\}$. Значит, существует значение $d = d_0$ такое, что $A \wedge B$ ложна на наборе значений $\{d_0, d_1, d_2, \dots d_n\}$. Тогда $\forall x(A \wedge B)$ ложна на $\{d_1, d_2, \dots d_n\}$, кроме того, или формула A, или B ложна на наборе $\{d_0, d_1, d_2, \dots d_n\}$. Последнее означает, что или $\forall xA$, или $\forall xB$ соответственно ложна на наборе значений $\{d_1, d_2, \dots d_n\}$ и конъюнкция этих формул ложна. Значит, формулы $\forall x(A \wedge B)$ и $\forall xA \wedge \forall xB$ ложны и первое утверждение теоремы доказано.

Второе утверждения доказывается аналогично •

В доказанной теореме не указано, как «взаимодействует» квантор всеобщности с дизъюнкцией и квантор существования с конъюнкцией. На эту тему – следующие утверждения:

Теорема 5 – о неравносильном переносе кванторов через дизъюнкцию и конъюнкцию.

$$\forall xA \vee \forall xB \models \forall x(A \vee B).$$

$$\exists x(A \wedge B) \models \exists xA \wedge \exists xB.$$

Доказательство. Пусть D - предметная область, задана интерпретация формул A и B, $\{x, y_1, y_2, \dots y_n\}$ - объединение свободных переменных A и B.

Тогда формулы $\forall xA \vee \forall xB$ и $\forall x(A \vee B)$ зависят от переменных $\{y_1, y_2, \dots y_n\}$. Требуется доказать, что если на некотором наборе значений этих переменных первая формула истинна, то и вторая тоже истинна. Пусть $\{d_1, d_2, \dots d_n\}$ - набор значений y_i, на котором формула $\forall xA \vee \forall xB$ истинна. Тогда на этом наборе истинна формула $\forall xA$ или $\forall xB$. Это означает, что формула A или формула B истинна на всех наборах вида $\{d, d_1, d_2, \dots d_n\}$, где $d, d_k \in D$, полученных расширениями набора значений для y_i. Тогда формула $A \vee B$ истинна на всех таких расширениях. По определению интерпретации квантора всеобщности это означает, что формула $\forall x(A \vee B)$ истинна на наборе значений $\{d_1, d_2, \dots d_n\}$.

Второе утверждение доказывается аналогично •

Можно дополнить полученные результаты очевидными соотношениями о перестановке одноименных кванторов:

$$\forall x(\forall y A) \sim \forall y(\forall x A);$$

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

Все эти свойства, в сочетании с правилами переименования свободных и связанных переменных, сформулированными раньше для отношения выводимости, но верными и для отношения логического следования, являются основой для приведения любой формулы ИП к некоторому равносильному *нормальному* виду, в котором все кванторы вынесены перед формулой.

Приведение формул к нормальному виду проводится как предварительное преобразование при доказательстве полноты ИП, что оправдывает рассмотрение отмеченных свойств.

Однако у любого подхода, опирающегося на общезначимость, имеется принципиальное ограничение - отсутствие для формул ИП алгоритма проверки общезначимости. Этот факт не доказан, но в следующей лекции он будет обсуждаться.

11 Непротиворечивость, неразрешимость, полнота

11.1 Непротиворечивость исчисления предикатов

После того как было введено понятие интерпретации, можно проводить доказательство непротиворечивости ИП по той же схеме, которая использовалась для исчисления высказываний.

Теорема 1. Аксиомы исчисления предикатов общезначимы.

Доказательство. Сначала разберем первые десять схем аксиом. Рассмотрим произвольную интерпретацию аксиом на некоторой области D. Каждая аксиома построена при помощи подстановки в схему формул ИП. Формулам при интерпретации сопоставлены по известным правилам предикаты от имеющихся свободных переменных. Набор свободных переменных аксиомы является объединением наборов свободных переменных подформул, из которых аксиома построена. Любому набору значений переменных соответствуют определенные значения подформул. Значение самой аксиомы получается из значений подформул при помощи булевых таблиц истинности. Как отмечалось ранее (т. 1, гл. 8), все схемы аксиом ИВ тождественно истинны. Десять схем ИП перенесены из ИВ без изменений. Поэтому значение аксиомы на любом наборе значений переменных будет равно 1.

Расссмотрим $\forall$-схему $\forall x A(x) \Rightarrow A(t)$ - аксиому 11. По определению, подстановка t вместо x свободна. Здесь $A(x)$ произвольная формула ИП, у которой ни одно свободное вхождение x не находится в области действия квантора по t. Надо доказать, что такая формула тождественно истинна при любой интерпретации в любой области D.

Сначала тривиальный случай: $A(x)$ вообще не зависит от x, то есть не имеет свободных вхождений x. Тогда подстановка t вместо x никуда не будет произведена и $A(t)$ просто совпадает с $A(x)$; соответственно совпадут и их значения при интерпретации. Кроме того, по правилам интерпретации значения $\forall x A(x)$ и $A(x)$ в таком случае также совпадают. Значит, условие и заключение в $\forall$-схеме при интерпретации будут принимать одинаковые значения и схема будет тождественно истинна.

Пусть $A(x) = A(x, y_1, y_2, \dots y_n)$ - формула A с явно выписанным списком всех имеющихся свободных переменных. Может быть два случая: либо среди y_k есть переменная t, либо нет. Рассуждения почти одинаковы в обоих случаях, проведем их поэтому, когда свободной переменной t в формуле $A(x)$ нет. Отметим, что тогда подформула $\forall x A(x)$ зависит только от $\{y_1, y_2, \dots y_n\}$, а подформула $A(t)$ - от $\{t, y_1, y_2, \dots y_n\}$. Вхождения t, появившиеся в $A(t)$ в результате подстановки, являются свободными в силу свободы подстановки, и притом это все свободные вхождения t вообще - других свободных вхождений не было. Вся аксиома тоже зависит от этого набора: $\{t, y_1, y_2, \dots y_n\}$. Пусть теперь задана область D и дано какое-то распределение значений всех этих переменных: $\{d_0, d_1, d_2, \dots d_n\}$, при этом $\forall k \;\; d_k \in D$.

Может быть два случая: либо $A(t)$ на этом наборе истинна, либо ложна. В первом случае вся импликация тоже истинна, так как заключение истинно. Во втором случае докажем, что значение формулы $\forall x A(x)$ на наборе $\{d_1, d_2, \dots d_n\}$ ложно. Действительно, значение формулы

$A(x) = A(x, y_1, y_2, \dots y_n)$ на наборе значений переменных $\{d_0, d_1, d_2, \dots d_n\}$ получается при подстановке d_k вместо y_k при $k > 0$ и d_0 вместо свободных вхождений x. По условию, свободные вхождения x в формуле $A(x)$ заменены на вхожения t, которые тоже остались свободными в силу свободы подстановки. Значит, d_0 в формуле $A(x)$ будет подставлено на те же места, что и в формуле $A(t)$. Так как $A(t)$ на этом наборе ложно, $A(x)$ тоже. Это означает, что $\forall x A(x)$ на наборе $\{d_1, d_2, \dots d_n\}$ ложно. Если условие ложно, импликация истинна.

Рассуждения для $\exists$-схемы совершенно аналогичны. При тех же обозначениях и предположениях имеются два содержательных случая: либо $A(t)$ на определённом наборе $\{d_0, d_1, d_2, \dots d_n\}$ истинна, либо ложна. Если посылка импликации ложна, импликация истинна. Если $A(t)$ при данных значениях истинна, то, в силу свободы подстановки, $A(x)$ тоже будет истинна при $x = d_0$. Рассуждения при этом аналогичны предыдущему случаю. Если $A(x)$ при некотором $d_0 \in D$ истинно, то $\exists x A(x)$ истинно на наборе значений $\{d_1, d_2, \dots d_n\}$, а тогда импликация тоже истинна $\bullet$

Простейший пример показывает, что, если в аксиомах 11 и 12 не выполнены условия свободы подстановки t вместо x, общезначимая формула может не получиться.

Пусть $A(x) = \exists t B(x, t)$. Для этой формулы подстановка t вместо x не свободна. Проверим, что формула $\forall x \exists t B(x, t) \Rightarrow \exists t B(t, t)$ не общезначима.

В качестве предметной области D рассмотрим двухэлементное множество: $D = \{a, b\}$. Таблицу значений для $B(x, t)$ определим так:

x	t	$B(x,t)$
a	a	0
a	b	1
b	a	1
b	b	0

Тогда, очевидно, $A(x) = \exists t B(x,t)$ в этой интерпретации истинна и при $x = a$ и при $x = b$, значит, $\forall x \exists t B(x,t)$ – истинное высказывание. Но $A(t) = \exists t B(t,t)$ – ложно, и вся импликация ложна.

Теорема 2. Формулы ИП, полученные как непосредственные следствия общезначимых формул, тоже являются общезначимыми.

Доказательство. В исчислении предикатов имеется три правила вывода, которые и надо проверить. Насчет правила МР (т. 1, гл. 8) известно, что из тавтологий выводятся тавтологии. Из этого следует, что из общезначимых формул по правилу МР снова получаются общезначимые.

Рассмотрим $\forall$-правило: из формулы $C \Rightarrow A(x)$ непосредственно выводится формула $C \Rightarrow \forall x A(x)$; если C не содержит свободных вхождений x (не зависит от x).

Пусть D - произвольная предметная область, на ней задана некоторая интерпретация, и $\{x, y_1, y_2, \dots y_n\}$ - список всех свободных переменных формулы $C \Rightarrow A(x)$. Тогда формула $C \Rightarrow \forall x A(x)$ зависит от $\{y_1, y_2, \dots y_n\}$. Подформула C тоже зависит только от $\{y_1, y_2, \dots y_n\}$. Пусть $\{d_1, d_2, \dots d_n\}$ - некоторый набор значений из предметной области.

Может быть два случая: либо формула $\forall x A(x)$ на этом наборе истинна, либо ложна. Если формула истинна, вся импликация тоже истинна на наборе $\{d_1, \dots d_n\}$.

Пусть формула $\forall x A(x)$ на указанном наборе ложна. По определению интерпретации квантора это значит, что существует такое $d_0 \in D$, что формула $A(x)$ на наборе значений $\{d_0, d_1, d_2, \dots d_n\}$ ложна. Значение формулы $C \Rightarrow A(x)$ на этом наборе истинно в силу общезначимости формулы. Но если заключение импликации ложно, а вся импликация истинна, то условие тоже ложно, другими словами, C на наборе $\{d_0, d_1, d_2, \dots d_n\}$ ложна. В силу того что C не зависит от x, фактический набор значений для C - $\{d_1, d_2, \dots d_n\}$. Так как C на этом наборе ложна, вся импликация $C \Rightarrow \forall x A(x)$ истинна.

Рассуждения для $\exists$-правила совершенно аналогичны •

Замечание. Пусть имеется набор формул $T_1, T_2, \dots T_n$, тождественно истинных на одной фиксированной предметной области D. Тогда всякая формула F ИП, выводимая из этого набора, также будет тождественно истинна на D.

Действительно, все аксиомы и формулы T_i, участвующие в выводе F, тождественно истинны на D. Тогда и следствия из них будут тождественно истинны на D. Этот факт устанавливается такими же рассуждениями, как и в теореме 2.

Теорема 3. Если формула F предикатов доказуема, то она общезначима. В стандартных обозначениях: если $\vdash F$, то $\models F$.

Доказательство. По теореме 1 все аксиомы общезначимы. По теореме 2 следствия общезначимых формул общезначимы. Если формула F доказуема, существует ее формальное доказательство, то есть последовательность формул из аксиом и непосредственных следствий предыдущих формул, заканчивающаяся формулой F. В силу предыдущих замечаний заключаем, что все формулы в формальном доказательстве общезначимы $\bullet$

Свойство теории ИП, выраженное в теореме 3, называется непротиворечивостью относительно общезначимости.

Отсюда следует внутренняя непротиворечивость теории:

Теорема 4. Исчисление предикатов внутренне непротиворечиво.

Доказательство. По определению непротиворечивости, надо доказать, что для всякой формулы F хотя бы одно утверждение не выполнено: $\vdash F$ или $\vdash \neg F$. Действительно, если F не является доказуемой – все доказано; пусть F доказуема. Тогда F общезначима в силу теоремы 3. Тогда $\neg F$ тождественно ложна и потому не доказуема $\bullet$

11.2 Неразрешимость и полнота ИП

Все заключения, полученные в предыдущем разделе, совершенно аналогичны результатам о непротиворечивости для исчисления высказываний. Содержательная основа – интерпретация формул ИП, до некоторой степени аналогична таблицам значений для формул ИВ.

Полной аналогии, однако, между исчислением высказываний и исчислением предикатов нет, как, в частности, показывает следующая теорема, фактически сформулированная в предыдущей главе.

Теорема 5. (А. Черч) Не существует алгоритма распознавания общезначимости формул исчисления предикатов $\bullet$

Доказательство теоремы на элементарном уровне изложить невозможно. Действительно, доказать существование алгоритма можно просто, предъявив какой-либо алгоритм. Для доказательства отсутствия алгоритма надо хотя бы иметь какое-то определение алгоритма, чтобы знать, отсутствие чего требуется доказать. А вопрос определения порождает целую теорию - теорию алгоритмов, так как алгоритм – первичное понятие.

Во всяком случае, теорема Черча показывает, что не существует простого описания класса общезначимых формул, вроде того критерия тождественной истинности, что был получен для ИВ.

Напомним, теорию называют разрешимой, если существует алгоритм распознавания выводимости формулы из аксиом. Конечно, это близко к теореме Черча, только там говорится о распознавании общезначимости. Для исчисления высказываний общезначимость (тавтологичность) и выводимость - одно и то же, в силу теоремы о полноте. Оказывается, что исчисление предикатов тоже полно относительно общезначимости.

Теорема 6. (К. Гедель) Если формула исчисления предикатов общезначима, то она доказуема. В принятых обозначениях: если $\models F$, то $\vdash F$ •

Доказательство этой теоремы весьма сложно. В качестве первого шага используется приведение формулы к равносильной нормальной форме.

Следствие. Для исчисления предикатов класс доказуемых формул и класс общезначимых формул совпадают.

Доказательство – применение теорем 3 и 6 •

Замечание. Как отмечалось, теорема Геделя о полноте устанавливает полноту ИП относительно класса общезначимых формул. Этот результат аналогичен факту полноты исчисления высказываний относительно тавтологий – т. 5 гл. 8. Но для исчисления высказываний имеется и свойство внутренней полноты – т. 6 гл. 8, согласно которому добавление к системе аксиом любой недоказуемой схемы нарушает внутреннюю непротиворечивость теории.

Для исчисления предикатов свойства внутренней полноты нет.

Действительно, дополним систему аксиом схемой $\exists xA \Rightarrow \forall xA$. Эта схема недоказуема. Ранее отмечалось, что она тождественно истинна на предметной области из одного элемента, но, очевидно, не общезначима. В то же время присоединение этой схемы к списку аксиом не приводит к внутренней проитворечивости: все аксиомы и эта формула тождественно истинны на предметной области D из одного элемента, и потому все следствия из них тоже тождествеено истинны на D в силу замечания к теореме 2.

Исчисление предикатов - неразрешимая теория, теперь это следует из теоремы Черча и совпадения классов доказуемых и общезначимых формул. Поэтому теорему Черча называют теоремой о неразрешимости ИП.

11.3 Пример необщезначимой k-общезначимой формулы

Как отмечалось, доказательство теоремы о неразрешимости далеко выходит за рамки данного пособия. Однако можно привести пример, показывающий, что для распознавания общезначимости недостаточно конечных предметных областей. Этот пример до некоторой степени поясняет несуществование алгоритма распознавания.

Теорема 7. Существует формула исчисления предикатов, являющаяся k-общезначимой для любого k, но не общезначимой.

Доказательство. Рассмотрим формулу:

$$G = (\forall x \neg P(x,x)) \wedge \forall x \forall y \forall z (P(x,y) \wedge P(y,z) \Rightarrow P(x,z)) \wedge \forall x \exists y P(x,y).$$

Формула G не содержит свободных переменных и при любой интерпретации является высказыванием, истинным или ложным. Докажем, что при **любой** интерпретации на конечной области формуле G соответствует ложное высказывание.

Предположим противное: нашлась конечная предметная область D и такая интерпретация, при которой G истинна. Без ограничения общности будем считать, что D состоит из трех элементов: $D = \{a, b, c\}$. Формула G использует только одну предикатную букву - $P(x, y)$. Будем строить таблицу значений $P(x, y)$ (см. ниже), учитывая, что G истинно. G состоит из трех конъюнктивных сомножителей: $\forall x \neg P(x,x)$, $\forall x \forall y \forall z (P(x,y) \wedge P(y,z) \Rightarrow P(x,z)$ и $\forall x \exists y P(x,y)$. В силу истинности всей формулы каждый сомножитель тоже истинный. Так как истинна формула $\forall x \neg P(x,x)$, в первой, пятой и девятой строках таблицы значений $P(x, y)$ должно быть равно 0. Впишем эти значения в таблицу. В силу истинности формулы $\forall x \exists y P(x,y)$ и при $x = a$, и при $x = b$, и при $x = c$ должно быть хотя бы одно значение y, при котором $P(x, y)$ равно 1. Другими словами, в первых трех строках должна быть хотя бы одна единица, в четвертой, пятой и шестой строках тоже, и в седьмой, восьмой, девятой строках - аналогично.

Так как в первой строке должен быть 0, имеются две возможности: или во второй, или в третьей строке значение $P(x, y)$ должно быть равно 1. Эти случаи совершенно одинаковы, считаем потому, что во второй строке значение $P(x, y)$ равно 1. Впишем и его в таблицу. Теперь рассмотрим вторую формулу: $\forall x \forall y \forall z(P(x, y) \wedge P(y, z) \Rightarrow P(x, z)$. В силу ее истинности можно заключить, что, например, в четвертой строке значение $P(x, y)$ должно быть равно 0. Действительно, предположим, что $P(b, a) = 1$. Тогда, в силу $P(a, b) = 1$, $P(b, a) = 1$ и истинности импликации для любой тройки значений, должно быть истинно заключение: $P(a, a) = 1$ - противоречие. Значит, $P(b, a) = 0$. Впишем и этот результат в таблицу. Теперь можно утверждать, что $P(b, c) = 1$, так как хотя бы одна единица при $x = b$ должна быть. Тогда аналогично предыдущим рассуждениям $P(c, b) = 0$. Записав его в таблицу, видим, что должно быть: $P(c, a) = 1$. Теперь заметим, что в силу $P(a, b) = 1$ и $P(b, c) = 1$ из-за истинности импликации можно заключить, что $P(a, c) = 1$. Но тогда $P(a, c) = 1$ и $P(c, a) = 1$, откуда $P(a, a) = 1$ - противоречие. Таким образом, предположение истинности G противоречиво.

x	y	$P(x, y)$
a	a	0
a	b	1
a	c	?
b	a	0
b	b	0
b	c	1
c	a	1
c	b	0
c	c	0

Теоретически можно было бы проверить все возможные интерпретации $P(x, y)$ на данном множестве D. Различных интерпретаций, то есть различных таблиц значений, для $P(x, y)$ имеется 2^9 – многовато для вычислений «вручную». Кроме того, оставался бы вопрос - что делать с областями из четырех и более элементов?

Сейчас этот вопрос тоже актуален – но проведенные рассуждения можно строго оформить в виде индукции по количеству элементов предметной области D.

Итак, при любой интерпретации в любой конечной предметной области формула G ложна.

Рассмотрим теперь интерпретацию G на множестве натуральных чисел $\mathbb{N} = \{0, 1, 2, \dots n, \dots\}$. Значения $P(x, y)$ определим таким образом: $P(x, y) = 1$ тогда и только тогда, когда $x < y$. Тогда получаем, что $\forall x \neg P(x, x) = 1$ есть свойство иррефлексивности строгого неравенства. Попросту сказать, для всякого x верно, что x не меньше x. $\forall x \forall y \forall z (P(x, y) \wedge P(y, z) \Rightarrow P(x, z) = 1$ на $\mathbb{N}$ - это в точности свойство транзитивности, которое справедливо для строгого неравенства натуральных чисел. Снова словесная формулировка: для любых x, y, z если $x < y$ и $y < z$, то $x < z$. Последняя формула: $\forall x \exists y P(x, y)$ - в данной интерпретации утверждает, что для всякого x существует y, больший, чем x. Это, если угодно, утверждение о бесконечности предметной области. Во всяком случае, очевидно, что $\forall x \exists y P(x, y) = 1$. Тогда и вся формула G истинна на $\mathbb{N}$.

Рассмотрим теперь формулу $F = \neg G$. В силу полученных результатов F будет истинна при любой интерпретации на любой конечной предметной области, но она будет ложна при указанной интерпретации на $\mathbb{N}$ •

Таким образом, для проверки формулы ИП на общезначимость недостаточно рассматривать лишь конечные предметные области, нужно еще рассматривать интерпретации формулы на бесконечных множетвах D. В качестве маленького «утешения» можно отметить, что среди бесконечных областей D достаточно рассмотреть только счётное множество.

Задачи и упражнения

Используя теорему о десяти выводимых правилах, леммы о противоположной теореме и о противоречии, доказать, что имеются следующие отношения выводимости:

1. $A \to B \ \vdash \ (B \to C) \to (A \to C)$
2. $A \to B \ \vdash \ (C \to A) \to (C \to B)$
3. $A \to B \ \vdash \ (A \vee C) \to (B \vee C)$
4. $A \to B \ \vdash \ (A \wedge C) \to (B \wedge C)$
5. $A \to \neg B \ \vdash \ B \to \neg A$
6. $A \to B \ \vdash \ \neg B \to \neg A$
7. $\vdash \ A \to \neg\neg A$
8. $\vdash \ (A \to B) \to ((A \to C) \to (A \to B \wedge C))$
9. $\vdash \ \neg A \vee A$
10. $\vdash \ (A \to B) \vee (B \to A)$

Будем говорить, что формула F не слабее G, если $F \ \vdash \ G$. Две формулы F и G исчисления высказываний называются равносильными, если каждая не слабее другой, то есть существует вывод F из G: $G \ \vdash \ F$ и вывод G из F: $F \ \vdash \ G$. Равносильность двух формул F и G будем обозначать так: $F \equiv G$.

11. Доказать, что отношение «не слабее» на множестве M всех формул ИВ является отношением квазипорядка, а отношение равносильности - ассоциированным отношением эквивалентности, согласно т. 6 гл. 2. При этом

фактор-множество $M/\equiv$ становится частично упорядоченным относительно индуцированного отношения выводимости, указанного в отмеченной теореме. Указать классы формул, являющихся в этом частично упорядоченном множестве наименьшим и наибольшим элементом.

Доказать следующие равносильности:

12. $A \to B \equiv \neg A \vee B$ 13. $\neg(A \vee B) \equiv \neg A \wedge \neg B$
14. $\neg(A \wedge B) \equiv \neg A \vee \neg B$ 15. $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

$$16. A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

$$17. A \to (B \to C) \equiv (A \wedge B) \to C$$

Пусть имеется формула $\mathcal{F}$, содержащая пропозициональную букву X. Это будем обозначать так: $\mathcal{F}(X)$. Пусть $\mathcal{G}$ - произвольная формула ИВ. Через $\mathcal{F}(\mathcal{G})$ будем обозначать формулу, полученную из $\mathcal{F}$ заменой всех вхождений X на $\mathcal{G}$.

Будем говорить, что формула $\mathcal{F}(X)$ монотонно возрастает по переменной X, если из того, что $\mathcal{G}_1$ не слабее $\mathcal{G}_2$, следует, что $\mathcal{F}(\mathcal{G}_1)$ не слабее $\mathcal{F}(\mathcal{G}_2)$. Другими словами, $\mathcal{F}(X)$ монотонно возрастает по X тогда и только тогда, когда справедливо следующее отношение выводимости:

$$\mathcal{G}_1 \to \mathcal{G}_2 \vdash \mathcal{F}(\mathcal{G}_1) \to \mathcal{F}(\mathcal{G}_2).$$

Аналогично, формула $\mathcal{F}(X)$ монотонно убывает по переменной X, если справедливо обратное отношение:

$$\mathcal{G}_1 \to \mathcal{G}_2 \vdash \mathcal{F}(\mathcal{G}_2) \to \mathcal{F}(\mathcal{G}_1).$$

18. Доказать, что $X \vee Y$ и $X \wedge Y$ монотонно возрастают по X и по Y, $\neg X$ - монотонно убывает по X, $X \to Y$ монотонно возрастает по Y и монотонно убывает по X.

19. Доказать, что если формулы $\mathcal{G}$ и $\mathcal{H}$ равносильны, а формула $\mathcal{F}(X)$ содержит вхождения X, то формулы $\mathcal{F}(\mathcal{G})$ и $\mathcal{F}(\mathcal{H})$ равносильны. При этом утверждение остаётся справедливым, если в формуле $\mathcal{F}$ только одно вхождение X заменяется на $\mathcal{G}$ или $\mathcal{H}$ соответственно.

Дадим определение *подформулы* данной формулы $\mathcal{F}$ ИВ. Оно состоит из трёх пунктов.

Если $\mathcal{F}$ является пропозициональной буквой, то подформула - сама буква.

Если формула $\mathcal{F}$ имеет вид $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \wedge \mathcal{B})$ или $(\mathcal{A} \to \mathcal{B})$, то $\mathcal{A}$ и $\mathcal{B}$ - подформулы $\mathcal{F}$. Если $\mathcal{F}$ имеет вид $(\neg \mathcal{A})$, то $\mathcal{A}$ - подформула $\mathcal{F}$.

Если $\mathcal{G}$ - подформула $\mathcal{F}$, $\mathcal{H}$ - подформула $\mathcal{G}$, то $\mathcal{H}$ - подформула $\mathcal{F}$.

20. Пусть $\mathcal{G}$ - подформула $\mathcal{F}$ и $\mathcal{H}$ равносильна $\mathcal{G}$. Тогда формула $\mathcal{F}_1$, полученная из формулы $\mathcal{F}$ заменой подформулы $\mathcal{G}$ на $\mathcal{H}$, равносильна $\mathcal{F}$. Доказать.

Как отмечалось в пункте 8.5, приведенная аксиоматика исчисления высказываний не является единственной, то есть можно привести другие аксиоматические системы, в некотором смысле эквивалентные ИВ. Имеет смысл исследовать и некоторые формальные аксиоматические системы, не эквивалентные исходной системе ИВ. Все они отличаются от изученной системы ИВ только составом аксиом, остальные элементы определения: алфавит, определение формул и правила вывода – остаются неизменными. Определим формальную аксиоматическую систему ИВ2, определяющуюся так же, как исходная система ИВ, за исключением одного фрагмента: из списка аксиом ИВ исключается схема 3 - введение конъюнкции, вместо которой вводится схема

$$(\mathcal{A} \to \mathcal{B}) \to ((\mathcal{A} \to \mathcal{C}) \to (\mathcal{A} \to \mathcal{B} \wedge \mathcal{C})).$$

Систему ИВ3 определим так: из исходного списка аксиом ИВ исключим аксиому 9 - введение отрицания и добавим две аксиомы:

$$(\mathcal{A} \to \mathcal{B}) \to (\neg\mathcal{B} \to \neg\mathcal{A})$$

$$\mathcal{A} \to \neg\neg\mathcal{A}.$$

Система ИВ4 получается из ИВ изменениями списка аксиом, указанными для получения ИВ2 и ИВ3 одновременно. Другими словами, из списка аксиом ИВ удаляются две аксиомы - 3 и 9 и добавляются три указанные схемы.

Приведем пример еще одной системы, упоминавшейся в п. 8.5, - интуиционистского исчисления высказываний (ИИВ). Система ИИВ получается из ИВ, если в списке аксиом аксиому 10 - удаление отрицания - заменить на следующую аксиому:

$$\mathcal{A} \to (\neg\mathcal{A} \to \mathcal{B}).$$

21. Доказать, что множество формул, доказуемых в ИВ2, совпадает с множеством формул, доказуемых в ИВ.

22. Доказать, что множество формул, доказуемых в ИВ3, совпадает с множеством формул, доказуемых в ИВ.

23. Доказать, что множество формул, доказуемых в ИВ4, совпадает с множеством формул, доказуемых в ИВ.

Задачи 21-23 показывают, что в определённых пределах можно варьировать список аксиом, сохраняя множество доказуемых формул. При этом в данных примерах всегда вместо одной исключаемой аксиомы добавлялась одна или две другие. Естественный вопрос, упоминавшийся в п. 8.5, таков: если исключить одну из аксиом ИВ, ничего не добавив в список аксиом взамен, уменьшится ли множество доказуемых формул?

Точное определение следующее. Рассмотрим формальную аксиоматическую систему ИВ-10 (ИВ минус десять), получающуюся из ИВ, если из списка аксиом исключить аксиому 10: $\neg\neg\mathcal{A} \to \mathcal{A}$. Будем говорить, что в ИВ аксиома 10 *независима*, если $\neg\neg\mathcal{A} \to \mathcal{A}$ не доказуема в ИВ-10. Это условие означает, что аксиома 10 не выводится из остальных девяти аксиом, то есть множество формул, выводимых в системе ИВ-10, есть собственное подмножество формул, выводимых в ИВ. Аналогичное определение независимости дается и для любой другой аксиомы.

24. Доказать, что аксиома 10 ИВ независима.

25. Доказать, что аксиомы 3 – 9 ИВ независимы.

26. Доказать, что в ИИВ справедлива теорема о дедукции: пусть $\Gamma = \{A_1, A_2, \dots, A_k\}$ - произвольный набор формул, $k \geq 0$, A, B - еще две формулы ИИВ. Тогда если $\Gamma, A \vdash_{\text{иив}} B$, то $\Gamma \vdash_{\text{иив}} A \to B$.

27. $A \to B, B \to C \vdash_{\text{иив}} A \to C$

28. $\vdash_{\text{иив}} A \to \neg\neg A$

29. $A \to B \vdash_{\text{иив}} \neg B \to \neg A$

30. Доказать, что формула $\neg\neg A \to A$ не доказуема в ИИВ.

31. Доказать, что формула $A \vee \neg A$ не доказуема в ИИВ.

32. Пусть задана предметная область $D = \{a, b, c\}$ из трёх предметов и формула $\exists y(\forall x A(x, y, z) \to \exists t B(y, t))$.

Перечислить интерпретации данной формулы на данной области, не являющиеся тождественно ложными.

33. Доказать, что формула

$$\exists x \forall y (A(x, y) \to (\overline{A(x, x)} \equiv A(y, y)))$$

истинна в любой предметной области, имеющей не более трёх элементов.

34. Построить 2-общезначимую, но не общезначимую формулу ИП.

35. Пусть задана предметная область $D = \mathbb{N}$, где $\mathbb{N} = \{0, 1, \ldots\}$ – множество натуральных чисел, и на ней определены два предиката $S(x, y, z)$ и $P(x, y, z)$. $S(x, y, z) = 1$ тогда и только тогда, когда $x + y = z$, $P(x, y, z) = 1$ тогда и только тогда, когда $xy = z$.

Используя связки ИП, записать формулы с одной свободной переменной x, истинные в D тогда и только тогда, когда $x = 0$; когда x чётно; когда x простое число.

Записать формулы с двумя свободными переменными x и y, истинные тогда только тогда, когда $x \leq y$; когда $x < y$; когда x является делителем y.

Записать формулы с тремя свободными переменными x, y, z, истинные в D тогда и только тогда, когда z – наибольший общий делитель x и y; когда z – наименьшее общее кратное x и y.

Записать замкнутые (т. е. не содержащие свободных переменных) формулы, утверждающие коммутативность сложения в области D; ассоциативность умножения в области D; бесконечность множества простых чисел в D.

Построить замкнутую формулу, утверждающую дистрибутивность умножения относительно сложения.

Построить замкнутую формулу, утверждающую,что каждое число из D является суммой четырёх квадратов.

Построить замкнутую формулу, утверждающую, что каждое число из D является суммой двух квадратов.

Построить замкнутую формулу, утверждающую, что в D множество простых чисел конечно.

Построить замкнутую формулу, утверждающую, что в D существует наибольшее число.

Построить замкнутую формулу, утверждающую, что в D не существует наименьшего числа.

Построить замкнутую формулу, утверждающую, что в D всякое чётное число, большее двух, является суммой двух простых.

Построить замкнутую формулу, утверждающую, что в области D существует бесконечное множество простых чисел-близнецов.

Что можно сказать об истинности данных утверждений в D?

36. Пусть задана предметная область $D = B(M)$, где M – некоторое непустое множество, $B(M)$ – его булеан. Пусть на D задан предикат $Q(x, y)$, равный 1 тогда и только тогда, когда $x \supseteq y$. Записать формулы ИП с использованием Q и трёх свободных переменных x, y, z которые будут истинны тогда и только тогда, когда $x = y \cap z$; когда $x = y \cup z$.

Записать формулу от двух свободных переменнных x и y, истинную тогда и только тогда, когда $x = \bar{y}$.

Построить формулу от одного свободного переменного x, истинную тогда и только тогда, когда $x = \emptyset$.

37. Построить выводы следующих формул:

$$\forall x \forall y A(x,y) \to \forall y \forall x A(x,y)$$
$$\exists x \exists y A(x,y) \to \exists y \exists x A(x,y)$$
$$\exists x \forall y A(x,y) \to \forall y \exists x A(x,y)$$

12 Булевы функции

12.1 Элементарные булевы функции, равенство функций

Определение булевых или логических функций было дано в гл. 8 в связи с определением истинности или ложности формул исчисления высказываний. Теперь мы начинаем изучение этих функций как самостоятельного объекта. Напомним определение:

Определение. Пусть $F_2 = \{0, 1\}$ - множество из двух элементов, F_2^n -декартова степень F_2, то есть множество соответствующих 0-1-векторов.

Логической (булевой) функцией от n неизвестных называется отображение $f : F_2^n \to F_2$. Множество всех булевых функций будем обозначать B_2. Для задания булевой функции достаточно выписать следующую таблицу значений:

x_1	$\dots$	x_{n-1}	x_n	$f(x_1, \dots x_{n-1}, x_n)$
0	$\dots$	0	0	$f(0, \dots 0, 0)$
0	$\dots$	0	1	$f(0, \dots 0, 1)$
0	$\dots$	1	0	$f(0, \dots 0, 1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	$\dots$	1	1	$f(1, \dots 1, 1)$

Общее количество строк в таблице для функции от n переменных равно 2^n.

Условимся наборы значений переменных в таблице всегда располагать одинаково - как записи чисел $0, 1, 2, \ldots 2^n - 1$ в двоичной системе исчисления. После такого соглашения функцию от n переменных можно задавать просто строкой 0-1 значений длиной 2^n.

Отметим два свойства таблицы значений переменных, необходимые для дальнейшего:

1. Для каждой переменной количество нулей и единиц в строках таблицы одинаково, другими словами, количество нулей и единиц в каждом столбце таблицы равно 2^{n-1};

2. Строки, равноотстоящие от концов таблицы, получаются друг из друга инвертированием, то есть заменой всех нулей на единицы и единиц - на нули. Такие наборы значений называются противоположными.

Теорема 1. Количество всех булевых функций от n переменных равно 2^{2^n}.

Доказательство. Как отмечалось, каждой функции от n переменных можно сопоставить 0-1-вектор значений длины 2^n. Это сопосталение - биекция между множеством функций и множеством векторов. Количество векторов длины k равно 2^k (сл. 2 гл. 2), и утверждение тем самым доказано •

Задание функций в табличном виде громоздко. Например, в математическом анализе основной способ задания функций - арифметические выражения, составленные из некоторого набора исходных «элементарных» функций с помощью определенных операций.

Аналогичный подход развивается и для булевых функций.

Сначала определим список исходных элементарных функций. Функций от одного переменного всего четыре: константы 0 и 1, тождественная функция $f_1(x) = x$ и отрицание, которое теперь будем изображать так: $f_2(x) = \overline{x}$.

Остальные элементарные функции – от двух переменных. Зададим их таблицами значений:

x	y	$f_3 = x \vee y$	$f_4 = x \wedge y$	$f_5 = x \to y$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	1

x	y	$f_6 = x \oplus y$	$f_7 = x \mid y$	$f_8 = x \downarrow y$
0	0	0	1	1
0	1	1	1	0
1	0	1	1	0
1	1	0	0	0

Новыми являются здесь лишь фукции $x \oplus y$ - *сложение по модулю два*, булево сложение, $x \mid y$ - *штрих Шеффера* и $x \downarrow y$ - *стрелка Пирса*, да и здесь новизна не слишком велика - ясно, что $x \mid y = \overline{x \wedge y}$, $x \downarrow y = \overline{x \vee y}$. Всего функций от двух переменных 16 штук, еще остались две константы - 0 и 1, четыре функции, зависящие фактически от одного переменного, и четыре, легко получающиеся из рассмотренных. Но, конечно, полный смысл выбора предложенных функций за основные будет проясняться постепенно.

Заметим, что функции 0 и 1 упоминались дважды: как функции одного аргумента и двух. Пунктуально по определению, это действительно различные отображения - зависят от различного количества аргументов. Но здесь хотелось бы такие функции отождествлять.

Определение. Пусть $f(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) \in B_2$ - произвольная булева функция. Говорят, что f *существенно* зависит от аргумента x_i, если существует такой набор $a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ значений остальных переменных $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, что

$$f(a_1, a_2, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, a_2, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Значит, если x_i - существенная, имеется ситуация, задаваемая значениями остальных переменных, где все определяется значением x_i.

Если переменная x_i не является существенной, она называется фиктивной. Ясно, что в постоянной функции все переменные фиктивны. В приведенных элементарных функциях двух аргументов все переменные существенны.

Можно дать независимое определение фиктивной переменной.

Определение. Пусть $f(x_1, \ldots, x_i, \ldots, x_n) \in B_2$ – произвольная булева функция. Говорят, что переменная x_i фиктивна, если для любого набора $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ значений остальных переменных

$$f(a_1, a_2, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) = f(a_1, a_2, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Это просто переформулировка определения.

Пусть у функции $f(x_1, x_2, \ldots, x_n)$ переменная x_i является фиктивной. По таблице значений функции f построим новую таблицу вычеркиванием всех строчек, в которых $x_i = 1$, и вычеркиванием столбца x_i. Полученная таблица будет содержать 2^{n-1} строк и задавать некоторую функцию $g(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Говорят, что функция g получена из функции f удалением фиктивной переменной x_i, а f получена из g введением фиктивной переменной x_i.

Отметим, что, по определению фиктивной переменной, значения на тех наборах, где $x_i = 1$ соответственно совпадают со значениями функции на наборах, в которых $x_i = 0$, поэтому с тем же результатом можно было бы вычеркнуть все строки, где $x_i = 0$.

Можно проверить, что получившаяся таблица значений переменных $x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_n$ будет заполнена в условленном порядке.

Определение. Функции f_1 и f_2 называются равными, если одна из другой получается удалением и/или добавлением фиктивных переменных.

Конечно, это определение шире, чем просто равенство отображений. Легко проверить, что, удаляя все фиктивные переменные данной функции в произвольном порядке, в результате будем получать единственную таблицу значений, включающую только существенные переменные. Поэтому две функции равны тогда и только тогда, когда их таблицы совпадут после удаления всех фиктивных переменных в обеих функциях.

Согласно этому определению, константы 0 и 1 не имеют существенных переменных - их можно формально рассматривать как функции от нуля переменных.

Замечание. Если дана произвольная конечная система булевых функций $f_1, f_2, \dots, f_k$, $\forall i \ f_i \in B_2$, то без ограничения общности можно считать, что все функции зависят от одних и тех же переменных $x_1, x_2, \dots, x_n$, то есть имеют вид:

$$f_1(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n).$$

Действительно, всегда можно перейти от исходных функций к равным, введя соответствующие фиктивные переменные. Точнее сказать, это можно сделать, если рассматриваемое для функций свойство переносится на равные функции.

12.2 Свойства основных операций для булевых функций

В предыдущем пункте были определены элементарные булевы функции. Каждая функция от двух переменных задает алгебраическую операцию на множестве F_2 и имеет, наряду с функциональным, алгебраическое обозначение: например, $f_3(x, y) = x \vee y$. Аналогично можно сказать, что для действительных чисел $f(x, y) = x * y$ является функцией от двух переменных, или операцией умножения.

В арифметике чисел основные свойства этих операций, такие как ассоциативность, дистрибутивность и другие, лежат в основе всех вычислений. Рассмотрим и для булевых операций подобные основные свойства, которые в дальнейшем будут использоваться без особых ссылок.

Теорема 2. Для элементарных функций справедливы следующие свойства:

1. Ассоциативность дизъюнкции, конъюнкции, булева сложения:

$(x \vee y) \vee z = x \vee (y \vee z); \quad (x \wedge y) \wedge z = x \wedge (y \wedge z);$
$(x \oplus y) \oplus z = x \oplus (y \oplus z).$

2. Коммутативность дизъюнкции, конъюнкции, булева сложения, штриха Шеффера, стрелки Пирса:

$x \vee y = y \vee x; \quad x \wedge y = y \wedge x; \quad x \oplus y = y \oplus x; \quad x \mid y = y \mid x; x \downarrow y = y \downarrow x.$

3. Дистрибутивность дизъюнкции относительно конъюнкции, конъюнкции относительно дизъюнкции, конъюнкции относительно сложения:

$(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$; $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$; $(x \oplus y) \wedge z = (x \wedge z) \oplus (y \wedge z)$.

4. Законы де Моргана:

$\overline{x \wedge y} = \overline{x} \vee \overline{y}$; $\overline{x \vee y} = \overline{x} \wedge \overline{y}$; $\overline{\overline{x}} = x$.

5. Свойства поглощения:

$(x \wedge y) \vee x = x$; $(x \vee y) \wedge x = x$; $x \vee x = x$; $x \wedge x = x$; $x \vee 0 = x$;

$x \vee 1 = 1$; $x \wedge 0 = 0$; $x \wedge 1 = x$; $x \wedge \overline{x} = 0$; $x \vee \overline{x} = 1$.

6. Связи между операциями:

$x \mid y = \overline{x \wedge y}$; $x \downarrow y = \overline{x \vee y}$; $x \to y = \overline{x} \vee y$.

Доказательство - проверка равенства функций по таблицам значений $\bullet$

Аналогичные свойства формулировались для операций над множествами – т. 1 гл. 1, и это не случайно, так как операция пересечения множеств определяется при помощи связки «и» – конъюнкции, объединение – при помощи дизъюнкци, а булево сложение используется для определения операции симметрической разности множеств.

Другие утверждения теоремы фактически встречались при изучении исчисления высказываний, например $x \vee \overline{x} = 1$ – просто закон исключенного третьего. Это тоже не удивительно – закон является доказуемой формулой, поэтому ему соответствует тождественно истинная булева функция, что здесь еще раз и отмечено.

Конечно, количество соотношений можно было увеличить или уменьшить, некоторые соотношения выводятся друг из друга. Приведенные свойства просто наиболее употребительны.

12.3 Формулы. Принцип двойственности

Имея набор элементарных функций, можно получать новые функции, строя *формулы* при помощи *суперпозиции.*

Определение. Пусть C - некоторое множество булевых функций: $C \subseteq B_2$. Тогда:

1. Всякая функция $f(x_1, x_2, \ldots, x_n) \in C$ является *формулой над* C.

2. Если $f(x_1, x_2, \ldots, x_n)$ - функция из C и $G_1, G_2, \ldots, G_n$ - выражения, являющиеся либо формулами над C, либо переменными, то выражение $f(G_1, G_2, \ldots, G_n)$ является *формулой над* C.

Говорят, что функция f выражается через систему C, если f равна некоторой формуле над C.

Это рекурсивное определение совершенно аналогично определению формулы исчисления высказываний. Основное отличие данного определения от определения в ИВ в том, что там формулы строились на основе фиксированного начального набора *логических связок.*

В отличие от этого, теперь будут рассматриваться различные исходные наборы функций C. Одна из основных задач теории булевых функций состоит в поиске наилучших (в каком-либо смысле) исходных наборов C, через которые остальные функции выражаются.

Примеры. Пусть C – перечисленное выше множество элементарных функций. Тогда следующие выражения являются формулами над C:

$x \oplus (y \vee z) \oplus \overline{x \mid z}; \quad x \to (x \to (y \wedge z); \quad x \downarrow (y \to x).$

Вообще, любая формула исчисления высказываний является формулой над множеством элементарных функций.

Написание формул над множеством элементарных функций будем проводить с теми же соглашениями о сокращении количества скобок, что были установлены в исчислении высказываний. Добавим, кроме того, что в силу имеющейся ассоциативности и коммутативности ряда операций будем без дальнейших пояснений употреблять, например, такие записи: $x \oplus (y \oplus t) = x \oplus t \oplus y$.

Условимся, что конъюнкция по умолчанию выполняется раньше сложения: $x \oplus y \wedge z = x \oplus (y \wedge z)$, а если нужен другой порядок операций, то расставляются скобки.

Конъюнкция в булевых функциях часто обозначается как произведение - $x \wedge y = x \cdot y = xy$; при этом последнее соглашение становится по виду таким же, как в арифметике чисел: $x \oplus yz = x \oplus (yz)$. В силу дистрибутивности конъюнкции относительно сложения можно записать: $(x \oplus y)z = xz \oplus yz$.

Каждой формуле над произвольным множеством C соответствует функция из B_2, вычисление значений которой на любом наборе переменных проводится согласно построению формулы. Считаем, что любая функция, равная данной, тоже реализуется этой формулой.

Работу с формулами упрощают соображения, использующие понятие двойственности.

Определение. Пусть $f(x_1, x_2, \ldots, x_n) \in B_2$ – булева функция. Функция $f^*(x_1, x_2, \ldots, x_n)$ называется *двойственной* к функции f, если:

$$f^*(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_1})}.$$

Таким образом, двойственная функция на противоположных наборах значений переменных принимает противоположные значения по сравнению с исходной функцией. Столбец значений двойственной функции получается из столбца значений исходной функции переворачиванием сверху вниз и инвертированием, то есть заменой 0 на 1, и наоборот.

Замечание. Легко проверить, что $(f^*)^* = f$.

Примеры. Очевидно, что $0^* = 1$, $x^* = x$, $(\overline{x})^* = \overline{x}$, $(x \wedge y)^* = x \vee y$.

Определение. Функция $f \in B_2$ называется *самодвойственной*, если $f^* = f$.

Например, $\overline{x}$ - самодвойственная функция, $x \oplus y \oplus z$ - тоже.

Класс всех самодвойственных функций обозначается через S.

Замечание. Функция, равная самодвойственной, также является самодвойственной.

Другими словами, если в самодвойственной функции удалить или добавить фиктивную переменную, снова получим самодвойственную функцию.

Теорема 3 – о суперпозиции.

Пусть

$$f(t_1, t_2, \ldots, t_m), g_1(x_{11}, x_{12}, \ldots, x_{1k_1}), \ldots, g_m(x_{m1}, x_{m2}, \ldots, x_{mk_m}) \in B_2$$

- набор булевых функций, пусть $x_1, x_2, \ldots, x_n$ - объединение всех переменных x_{ij}. Тогда если $F(x_1, x_2, \ldots, x_n) = f(g_1, g_2, \ldots, g_m)$, то

$F^*(x_1, x_2, \ldots, x_n) = f^*((g_1)^*, (g_2)^*, \ldots, (g_m)^*)$.

Доказательство.

$F^*(x_1, x_2, \ldots, x_n) = \overline{F}(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}) =$
$\overline{f}(g_1(\overline{x}_{11}, \overline{x}_{12}, \ldots, \overline{x}_{1k_1}), \ldots, g_m(\overline{x}_{m1}, \ldots, \overline{x}_{1k_1})) =$
$= \overline{f}(\overline{\overline{g_1}}(\overline{x}_{11}, \overline{x}_{12}, \ldots, \overline{x}_{1k_1}), \ldots, \overline{\overline{g}_m}(\overline{x}_{m1}, \ldots, \overline{x}_{1k_1})) =$
$= \overline{f}(\overline{g_1^*}(x_{11}, x_{12}, \ldots, x_{1k_1}), \ldots, \overline{g_m^*}(x_{m1}, \ldots, x_{1k_1})) =$

$f^*(g_1^*(x_{11}, x_{12}, \ldots, x_{1k_1}), \ldots, g_m^*(x_{m1}, \ldots, x_{1k_1}))$ •

Следствие 1 - принцип двойственности.

Пусть формула F построена с помощью набора функций $f_1, f_2, \ldots, f_k$ и задает функцию f. Тогда формула, полученная из F заменой набора исходных функций соответственно на $f_1^* f_2^*, \ldots, f_k^*$, реализует функцию f^*. Соответствующую формулу обозначают через F^*.

Доказательство. Индукция по количеству функций k, использованных для построения формулы F. При $k = 1$ $f = f_1$, и все доказано. При $k > 1$ формула F получена с помощью суперпозиции из формул, для которых утверждение доказано. Тогда и для формулы F утверждение следствия справедливо в силу предыдущей теоремы •

Следствие 2. Пусть $C = \{0, 1, \overline{x}, x \wedge y, x \vee y\}$, F - формула над C. Тогда для получения формулы F^* нужно в формуле F заменить всюду 0 на 1, 1 на 0, $\wedge$ на $\vee$, $\vee$ на $\wedge$.

Доказательство. В соответствии с принципом двойственности для получения двойственной формулы необходимо все входящие в формулу функции заменить на двойственные, что и утверждается в следствии •

Примеры. $(x \vee y)^* = x \wedge y$, $(xy \vee z\overline{t})^* = (x \vee y)(z \vee \overline{t})$. В последнем примере использовано написание конъюнкции в виде произведения.

Принцип двойственности можно использовать для получения различных соотношений между функциями, так как если $f = g$, то и $f^* = g^*$. Поэтому если, например, известно, что $\overline{x \wedge y} = \overline{x} \vee \overline{y}$, тогда по принципу двойственности получаем без вычислений: $\overline{x \vee y} = \overline{x} \wedge \overline{y}$.

13 Полные системы функций

13.1 Теорема об СДНФ

Всякую булеву функцию можно задать таблицей значений, хотя это и весьма громоздко. Можно ли подобрать такой набор функций C, что всякая функция выражается как формула над C? В такой постановке задача неинтересна - можно взять $C = B_2$, и тогда всякая функция сама через себя выражается. Значит, желательно выбирать конечный набор и вообще минимальный - как некоторое далекое обобщение базиса в линейном пространстве - через него тоже все векторы выражаются.

Рассмотрение этих вопросов для булевых функций - одна из основных задач теории. Пусть x - произвольная переменная, a - параметр, равный либо 0, либо 1. Будем обозначать через x^a булеву функцию, равную $\overline{x}$ при $a = 0$, или x – при $a = 1$. Очевидно, что $x^a = 1$ тогда и только тогда, когда $x = a$.

Определение. Элементарной конъюнкцией от n переменных называется булева функция вида $x_1^{a_1} \wedge x_2^{a_2} \wedge \ldots x_n^{a_n}$, где $(a_1, a_2, \ldots a_n)$ - произвольный набор длины n из нулей и единиц. Говорим, что элементарная конъюнкция *соответствует* данному набору.

Тогда очевидны такие утверждения.

Замечание 1. Количество различных элементарных конъюнкций от n переменных равно 2^n. Элементарная конъюнкция от n переменных равна 1 только на наборе значений, соответствующем этой конъюнкции •

Определение. Совершенной дизъюнктивной нормальной формой F (СДНФ) от n переменных называется одна элементарная конъюнкция или дизъюнкция нескольких различных элементарных конъюнкций.

Теорема 1. Всякая булева функция f от n неизвестных, не равная тождественно нулю, представляется некоторой СДНФ от n неизвестных, и это представление единственно.

Доказательство.

Рассмотрим таблицу значений функции $f(x_1, x_2, \ldots, x_n)$. Так как $f \neq 0$, в таблице имеются значения, равные 1. Возьмем наборы значений переменных в этих строках и по каждому набору построим соответствующую элементарную конъюнкцию. Тогда дизъюнкция этих элементарных конъюнкций будет предствлять функцию f:

$$f(x_1, x_2, \ldots, x_n) = F(x_1, x_2, \ldots, x_n) = \bigvee_{f(a_1, a_2, \ldots, a_n)=1} x_1^{a_1} \wedge x_2^{a_2} \wedge \ldots \wedge x_n^{a_n}.$$

Действительно, докажем, что функция f и форма F совпадают на любом наборе $b = (b_1, b_2, \ldots, b_n)$ значений переменных. Если $f(b_1, b_2, \ldots, b_n) = 0$, то этот набор не соответствует ни одной построенной элементарной конъюнкции, поэтому, в силу замечания 1, каждая конъюнкция на наборе b равна 0, дизъюнкция нескольких нулей - тоже ноль, значит, $F(b) = 0$.

Если же $f(b_1, b_2, \ldots, b_n) = 1$, то этот набор соответствует одной построенной элементарной конъюнкции, эта конъюнкция на наборе b равна 1 и дизъюнкция единицы с остальными конъюнкциями (которые на этом наборе равны 0) дает 1, значит, $F(b) = 1$. Таким образом, $f \equiv F$.

Единственность формы следует из того, что различных элементарных конъюнкций всего 2^n штук, значит, различных СДНФ столько, сколько непустых подмножеств в множестве элементарных конъюнкций, а их $2^{2^n}-1$. Столько же имеется и не равных тождественно нулю функций от n переменных в силу т. 1 гл. 12 $\bullet$

Примеры СДНФ. $x \to y = (\overline{x} \wedge \overline{y}) \vee (\overline{x} \wedge y) \vee (x \wedge y)$; $x \oplus y = (\overline{x} \wedge y) \vee (x \wedge \overline{y})$.

Теорема 2. Всякая функция $f \in B_2$ выражается как формула над множеством $C = \{\neg, \wedge, \vee\}$. Другими словами, всякая булева функция выражается через отрицание, конъюнкцию и дизъюнкцию.

Доказательство. Если функция $f \neq 0$, то она представляется с помощью соответствующей СДНФ, если же $f(x_1, x_2, \ldots, x_n) \equiv 0$, то можно взять, например, такое выражение: $f(x_1, x_2, \ldots, x_n) = x_1 \wedge \overline{x}_1$, или приписать еще несколько таких же сомножителей с другими, тоже фиктивными, переменными:

$$f(x_1, x_2, \ldots, x_n) = x_1 \wedge \overline{x}_1 \wedge x_2 \wedge \overline{x}_2 \ldots x_k \wedge \overline{x}_k \bullet$$

Таким образом, практически любую булеву функцию можно задавать не таблично, а с помощью СДНФ. При этом чем больше единиц среди значений функции, тем длиннее такое задание. Можно, используя двойственную форму, несколько упростить задание функций в этих случаях.

Двойственным для понятия элементарной конъюнкции является понятие элементарной дизъюнкции от n неизвестных.

Определение. Элементарной дизъюнкцией от n переменных называется булева функция вида $x_1^{a_1} \vee x_2^{a_2} \vee \ldots x_n^{a_n}$, где $(a_1, \ldots a_n)$ - произвольный набор длины n из нулей и единиц. Набором, *соответствующим данной элементарной дизъюнкции*, называется набор вида $(\overline{a}_1, \overline{a}_2, \ldots \overline{a}_n)$.

Снова справедливо

Замечание 2. Количество различных элементарных дизъюнкций от n переменных равно 2^n. Элементарная дизъюнкция от n переменных равна 0 только на соответствующем ей наборе значений $\bullet$

Определение. Совершенной конъюнктивной нормальной формой F (СКНФ) от n переменных называется одна элементарная дизъюнкция или конъюнкция нескольких различных элементарных дизъюнкций.

Теорема 3. Всякая булева функция f от n неизвестных, не равная тождественно 1, представляется некоторой СКНФ от n неизвестных, и это представление единственно.

Доказательство. Отображение $* : f \rightarrow f^*$ является биективным отображением множества всех функций от n переменных на себя. При этом функции, не равные тождественно единице, отображаются на множество функций, не равных тождественно нулю. Поэтому для построения СКНФ для функции f достаточно построить функцию f^*, для нее построить СДНФ, $f^* = F$, и еще раз взять двойственную функцию: $f = (f^*)^* = F^*$, или, подробнее:

$$f(x_1, x_2, \ldots, x_n) = F^*(x_1, x_2, \ldots, x_n) = \bigwedge_{f^*(a_1, a_2, \ldots, a_n)=1} x_1^{a_1} \vee x_2^{a_2} \vee \ldots \vee x_n^{a_n}.$$

Согласно сл. 2 гл. 12 для построения двойственной функции к форме F надо все дизъюнкции заменить на конъюнкции и конъюнкции на дизъюнкции. По построению формы F ясно, что получится некоторая СКНФ и она единственна в силу биективности отображения двойственности $\bullet$

Непосредственное построение СКНФ по таблице значений для данной функции f проводится следующим образом: отбираются все строки, в которых значение функции равно **нулю**, по каждому набору значений переменных $b = (b_1, b_2, \ldots, b_n)$ строится соответствующая элементарная дизъюнкция: $x_1^{\bar{b}_1} \vee x_2^{\bar{b}_2} \vee \ldots x_n^{\bar{b}_n}$. После этого строится конъюнкция всех построенных элементарных дизъюнкций.

Примеры СКНФ. $x \to y = \overline{x} \vee y$; $x \oplus y = (x \vee y) \wedge (\overline{x} \vee \overline{y})$.

13.2 Теоремы о полноте

Теорема 2 объясняет значение дизъюнкции, конъюнкции и отрицания в списке элементарных функций. В частности, теперь понятно, почему в языках программирования в качестве булевых операций часто выбираются именно эти три операции. В действительности и другие наборы функций тоже могут обладать таким же свойством.

Определение. Система $C = \{f_1, f_2, \ldots, f_k, \ldots\}$ функций из B_2 называется *(функционально) полной*, если любая булева функция может быть представлена формулой над C.

Примеры полных систем:

1. $C = B_2$ - множество всех булевых функций - полная система.

2. $C = \{\overline{x}, x \vee y, x \wedge y\}$ - полна в силу теоремы 2.

3. Ясно, что если система C полна, то любая система $C_1 \supseteq C$ полна.

В то же время понятно, что не любая система полна. Вопрос получения критериев полноты будет рассмотрен позднее, а следующая теорема позволит увеличить количество примеров полных систем.

Теорема 4. Пусть даны две системы функций: $C = \{f_1, f_2, \ldots\}$ и $D = \{g_1, g_2, \ldots\}$, некоторая функция $h \in B_2$ является формулой над C и каждая функция из C является формулой над D. Тогда h - формула над D.

Доказательство. Данная теорема о транзитивности выразимости совершенно очевидна: пусть $h = F(f_1, f_2, \ldots)$ - запись функции h как формулы, использующей для своего построения функции $f_1, f_2, \ldots$ первой системы. Так как функции системы C выражаются через D, то $f_1 = F_1(g_1, g_2, \ldots)$, $f_2 = F_2(g_1, g_2, \ldots) \ldots$ являются формулами над D. Тогда $h = F(F_1(g_1, g_2, \ldots), F_2(g_1, \ldots) \ldots)$ - выражение функции h как формулы над D •

Следствие. Если каждая функция некоторой полной системы C выражается как формула через систему D, то D - функционально полная система.

Доказательство. Пусть $f \in B_2$ - произвольная булева функция. В силу полноты C f является формулой над C. Тогда по теореме 4 f - формула над D •

Теперь можно определить еще несколько полных систем.

Теорема 5. Следующие системы являются полными:

1. $\{\overline{x}, x \vee y\}$.
2. $\{\overline{x}, x \wedge y\}$.
3. $\{x \mid y\}$.
4. $\{x \downarrow y\}$.
5. $\{\overline{x}, x \to y\}$.
6. $\{1, x \wedge y, x \oplus y\}$.

Доказательство.

1. Из теоремы 2, как отмечалось, следует полнота системы $C = \{\overline{x}, x \vee y, x \wedge y\}$. Согласно следствию, доста-

точно доказать, что система C выражается через систему 1. Достаточно доказать тогда, что $x \wedge y$ выражается через систему1:

$x \wedge y = \overline{\overline{x \wedge y}} = \overline{\overline{x} \vee \overline{y}}$, согласно т. 2 гл. 12 (законы де Моргана).

2. Например, из системы 1 по принципу двойственности: так как система 2 двойственна 1, значит, если какая-то функция f выражается через систему 1, то f^* - выражается через систему 2. А так как 1 - полная, через неё выражается любая функция, значит, двойственная любой функции выражается через систему 2. Значит, система 2 полна.

3. Докажем, что система 2 (она полна) выражается через 3: $x \mid x = \overline{x \wedge x} = \overline{x}$, снова т. 2 гл. 12.

Тогда:

$(x \mid y) \mid (x \mid y) = \overline{x \mid y} = \overline{\overline{x \wedge y}} = x \wedge y$, согласно имеющимся связям между операциями - т. 2 гл. 12.

Так же просто доказываются пункты 4, 5 и 6.

Докажем полноту 6. Легко видеть, что $\overline{x} = 1 \oplus x$ •

Определение. Булевым одночленом от n переменных $x_1, x_2, \ldots, x_n$ называется функция вида $x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_k}$, где $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ или единица.

Замечание 3.

Количество различных булевых одночленов от n переменных равно числу различных подмножеств множества $x_1, x_2, \ldots, x_n$ из n элементов, а имеено - 2^n.

Например, все булевы одночлены от двух переменных x и y таковы: $1, x, y, x \wedge y$. Грубо говоря, булев одночлен от n переменных есть конъюнкция («произведение») некоторого подмножества переменных, может быть пустого.

«Степеней» не существует, так как $x \wedge x = x$. Условимся для простоты обозначений писать вместо $x \wedge y = xy$.

Определение. Булевым многочленом от n переменных называется булева сумма нескольких различных одночленов от n переменных или ноль.

Примеры: $x \to y = 1 \oplus x \oplus xy$, $x \vee y = x \oplus y \oplus xy$. Имеется общий факт:

Теорема 6. Всякая булева функция от n переменных единственным образом представляется в виде булева многочлена от n переменных.

Доказательство. В силу полноты системы 6 всякая булева функция выражается через единицу, конъюнкцию и булеву сумму. Раскрывая скобки с учетом дистрибутивности конъюнкции (умножения) относительно сложения, ассоциативности и коммутативности сложения и умножения (т. 2 гл. 12), получим многочлен. Единственность представления следует, как и в других теоремах, из того, что число различных булевых многочленов от n переменных, как видно из замечания 3, равно числу всех функций от n переменных - 2^{2^n} ●

Отметим, что если для двух булевых функций f и g имеется соотношение $f \cdot g = 0$, то $f \vee g = f \oplus g$, как отмечено в последнем примере. Очевидно, что конъюнкция двух различных элементарных коъюнкций равна нулю, потому в СДНФ можно дизъюнкции заменить на знаки булевой суммы. Отсюда получаем один из способов построения булева многочлена для произвольной функции: сначала строится СДНФ, затем в ней дизъюнкции заменяются на сложение, затем в элементарных конъюнкциях отрицания заменяются на суммы: $\overline{x} = 1 \oplus x$, раскрываются скобки с учетом дистрибутивности и «приводятся подобные члены» с учетом свойства $x \oplus x = 0$.

Другой способ построения булева многочлена для данной функции использует метод неопределенных коэффициентов.

Считаем, что для построения многочлена используются две константы 0 и 1, а также булево сложение и умножение (конъюнкция). Тогда многочлен в общем виде может быть записан так:

$$f(x_1, x_2, \ldots, x_n) =$$

$$a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n \oplus a_{n+1} x_1 x_2 \oplus \ldots \oplus a_{2^{n-1}} x_1 x_2 \ldots x_n.$$

Коэффициенты a_i равны нулю или единице, $a_i x_i$ означает произведение (конъюнкцию), и каждый многочлен определяется набором коэффициентов: $a_0, a_1, \ldots, a_{2^n-1}$ длины 2^n. Таблица значений функции $f(x_1, x_2, \ldots, x_n)$ также содержит 2^n строк, поэтому, подставляя в выражение для многочлена всевозможные наборы значений переменных, получим систему 2^n уравнений с 2^n неизвестными a_i. Решив систему, получим значения всех коэффициентов и, значит, определим многочлен.

Пример:

x	y	$x \mid y$	
0	0	1	$1 = a \oplus b \cdot 0 \oplus c \cdot 0 \oplus d \cdot 0 \cdot 0 = a$
0	1	1	$1 = a \oplus c$
1	0	1	$1 = a \oplus b$
1	1	0	$0 = a \oplus b \oplus c \oplus d,$

$x \mid y = a \oplus b \cdot x \oplus c \cdot y \oplus d \cdot x \cdot y$

откуда видно, что $a = 1,\ c = 0,\ b = 0,\ d = 1$, и получаем выражение: $x \mid y = 1 \oplus xy$.

Конечно, для небольших примеров все эти вычисления тривиальны, но для реальных прикладных задач вопросы построения экономных алгоритмов нахождения формул и выражений весьма актуальны: например, разрядность стандартного компьютера обычно равна 32 - это количество переменных; тогда система уравнений будет содержать 2^{32} уравнений и неизвестных, это не меньше миллиарда.

14 Критерий функциональной полноты

14.1 Замкнутость

С понятием полноты связаны понятия замыкания и замкнутого класса функций.

Определение. Пусть $K \subseteq B_2$ - некоторое множество булевых функций. Замыканием множества K называется множество всех функций, представимых формулами над K. Замыкание множества K обозначается через $[K]$.

Так как при подстановке равных функций $f = g$ в функцию $h(x_1, x_2, \ldots, x_n)$ вместо одного и того же x_i получаются равные функции:

$$h(x_1, x_2, \ldots, x_{i-1}, f, x_{i+1}, \ldots, x_n) =$$

$$h(x_1, x_2, \ldots, x_{i-1}, g, x_{i+1}, \ldots, x_n)$$

и при подстановке одной функции в равные снова получаются равные, считаем, что замыкание наряду, с каждой функцией, содержит и все равные ей функции.

Примеры.

1. $K = B_2$. Очевидно - $K = [K] = B_2$.

2. $K = \{\overline{x}, x \vee y, x \wedge y\}$. Согласно т. 2 гл.13 $[K] = B_2$.

3. $K = \{x \mid y\}$. Согласно т. 5 гл.13 $[K] = B_2$. Вообще, K является полной системой тогда и только тогда, когда

$[K] = B_2$.

4. $K = \{1, x \oplus y\}$. Замыкание $[K]$ этого множества функций называется классом *линейных* функций и обозначается через $L = [K]$. Легко проверить, что $f \in L$ имеют вид:

$$f(x_1, x_2, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n.$$

Коэффициенты a_i равны нулю или единице. Коэффициентам, равным нулю, соответствуют фиктивные переменные.

Всякая линейная функция является частным случаем булева многочлена.

Теорема 1. Справедливы следующие свойства замыкания:

1. $K \subseteq [K]$
2. $[[K]] = [K]$
3. Если $K \subseteq M$. то $[K] \subseteq [M]$ - монотонность замыкания •

Определение. Пусть $K \subseteq B_2$. Множество K называется *(функционально) замкнутым* классом, если $K = [K]$.

Примеры замкнутых классов.

L - замкнутый класс в силу пункта 2 теоремы, так как он является замыканием некоторого множества функций.

Обозначим через T_0 класс всех булевых функций, *сохраняющих ноль*, то есть

$f(x_1, x_2, \ldots, x_n) \in T_0 \Longleftrightarrow f(0, 0, \ldots, 0) = 0$.

Примеры:

$0, x, x \wedge y, x \vee y, x \oplus y \in T_0, \quad 1, \overline{x} \notin T_0$.

T_1 - класс всех булевых функций, *сохраняющих единицу*, то есть

$f(x_1, x_2, \ldots, x_n) \in T_0 \Longleftrightarrow f(1, 1, \ldots, 1) = 1$.

Примеры:

$1, x, x \wedge y, x \vee y, x \to y \in T_1, \quad 0, \overline{x}, x \oplus y \notin T_1.$

S - класс всех самодвойственных функций, то есть

$f \in S \Longleftrightarrow f^* = f.$

Примеры:

$x,\ \overline{x},\ xy \vee xz \vee yz \in S, \quad x \oplus y,\ x \to y,\ \ldots \notin S.$

Теорема 2. Классы T_0, T_1 и S функционально замкнуты.

Доказательство.

Пусть $f(x_1, x_2, \ldots, x_m), f_1, f_2, \ldots f_m \in T_0$. Рассмотрим суперпозицию $F = f(f_1, f_2, \ldots, f_m)$ и докажем, что $F \in T_0$. Действительно,

$$F(0, \ldots, 0) = f(f_1(0, \ldots, 0), \ldots, f_m(0, \ldots, 0)) = f(0, \ldots, 0) = 0.$$

Отметим, что в приведенных выкладках в суперпозиции участвовали только функции и не было подстановок переменных, но это не уменьшает общности, так как подстановка переменных есть подстановка тождественной функции, а она принадлежит T_0. Таким образом, строго рассуждая, приведенные выкладки дают полноценную базу индукции, и, значит, все утверждение справедливо при подстановке произвольных формул из T_0.

Легко проверить также, что если функция сохраняет ноль, то и равная ей функция также сохраняет ноль.

Легко видеть, что $T_1 = T_0^*$, откуда следует замкнутость T_1. Это можно проверить и непосредственно, совершенно аналогично выкладкам для T_0. T_1, как и T_0, содержит с каждой функцией все равные ей.

Проверим замкнутость S. Снова, как и предыдущих случаях, S, наряду с каждой функцией, содержит все равные ей функции и содержит тождественную функцию $f(x) = x$. Поэтому достаточно проверить, что $f(f_1, \ldots, f_m)$ является самодвойственной, если f, $f_1, f_2, \ldots, f_m$ самодвойственны. То, что $F = f(f_1, f_2, \ldots, f_m)$ является самодвойственной, следует из т. 3 гл. 12:

$F^* = f^*(f_1^*, f_2^*, \ldots, f_m^*) = F = f(f_1, f_2, \ldots, f_m)$ •

Для описания еще одного полного класса функций необходимо предварительное определение.

Определение. Пусть имеются два 0-1-вектора

$$a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in F_2^n$$

. Определим для них отношение $\preceq$ по правилу:

$$a \preceq b \Longleftrightarrow a_1 \leq b_1, a_2 \leq b_2, \ldots, a_n \leq b_n.$$

То есть это покоординатное неравенство n-мерных 0-1-векторов.

Легко проверить, что отношение $\preceq$ является отношением частичного порядка, то есть удовлетворяет свойствам рефлексивности, транзитивности и антисимметричности (гл. 2).

Определение. Булева функция $f(x_1, x_2, \ldots, x_n)$ называется монотонной, если для любых двух наборов a и b, удовлетворяющих условию $a \preceq b$, имеется неравенство $f(a) \leq f(b)$.

Обозначим через M класс монотонных функций.

Примеры: $0,\ 1,\ x,\ x \wedge y,\ x \vee y \in M$; $\quad \overline{x},\ x \to y,\ x \oplus y \notin M$.

Два набора a и b назовем смежными, если они различаются только одной координатой:

$a = (a_1, a_2, \ldots, a_i, \ldots, a_n)$, $b = (a_1, a_2, \ldots, \overline{a_i}, \ldots, a_n)$.

Очевидно, если $a \prec b$ – строгое неравенство двух наборов, то существует возрастающая цепочка смежных наборов, ведущая от a к b. Например, $(0,1,0,0) \prec (1,1,0,1)$. Тогда:

$(0,1,0,0) \prec (1,1,0,0) \prec (1,1,0,1)$

– цепочка смежных 0-1-векторов. Отсюда очевидно: если функция монотонна на смежных парах наборов, то она монотонна.

Замечание. M - функционально замкнутый класс, содержащий наряду с любой функцией все равные ей. Доказательство аналогично рассмотрению предыдущих классов.

14.2 Основные леммы

Рассмотрим несколько вспомогательных утверждений, которые будут далее использованы для получения критерия функциональной полноты.

Лемма 1 – о несамодвойственной функции.

Если $f(x_1, x_2, \ldots, x_n) \notin S$, то из нее при помощи подстановок функций x и $\overline{x}$ можно получить константу.

Доказательство. В силу того что $f \notin S$, существует такой набор значений $(a_1, a_2, \ldots, a_n)$, что

$f(a_1, a_2, \ldots, a_n) = f(\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n)$.

Рассмотрим функции одного переменного $g_i(x) = x^{a_i}$, $i = 1, 2, \ldots, n$. Напомним обозначения (гл. 13): каждая $g_i(x)$ есть либо x при $a_i = 1$, либо отрицание x при $a_i = 0$. Пусть

$h(x) = f(g_1(x), g_2(x), \ldots, g_n(x))$.

Это константа. Действительно,

$h(0) = f(g_1(0), g_2(0), \ldots, g_n(0)) = f(\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n) =$

$f(a_1, a_2, \ldots, a_n) = f(g_1(1), g_2(1), \ldots, g_n(1)) = h(1)$ •

Отметим, что в лемме не уточняется, какая именно константа получена - это может быть и ноль, и единица.

Лемма 2 – о немонотонной функции.

Если функция $f(x_1, \ldots, x_n) \notin M$, то из нее при помощи подстановок констант 0, 1 и функции x можно получить $\overline{x}$.

Доказательство. Так как f немонотонна, существуют два набора $a \prec b$ такие, что $f(a) > f(b)$. Рассмотрев возрастающую цепочку смежных наборов, ведущую от a к b, видим, что имеется пара смежных наборов $c \prec d$, для которых $f(c) > f(d)$, то есть $f(c) = 1$, а $f(d) = 0$. Пусть

$c = (c_1, c_2, \ldots c_{i-1}, 0, c_{i+1} \ldots c_n)$

$d = (c_1, c_2, \ldots c_{i-1}, 1, c_{i+1} \ldots c_n)$

различаются только i-й координатой. Рассмотрим функцию:

$h(x) = f(c_1, c_2, \ldots, a_{i-1}, x, a_{i+1}, \ldots, c_n)$.

Тогда $h(x) = \overline{x}$; действительно:

$h(0) = f(c_1, c_2, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, c_n) = f(c) = 1$,

$h(1) = f(c_1, c_2, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, c_n) = f(d) = 0$ •

Лемма 3 – о нелинейной функции.

Если $f(x_1, x_2, \ldots, x_n) \notin L$, то из нее при помощи подстановок констант 0, 1, функций x, $\overline{x}$ и применения отрицания к f можно получить функцию $x \wedge y$.

Доказательство. В силу т. 6 гл. 13 функция f единственным образом представляется булевым многочленом:

$$f(x_1, x_2, \ldots, x_n) =$$

$$a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_{n+1}x_1x_2 \oplus \ldots \oplus a_{2^n-1}x_1x_2 \ldots x_n.$$

В силу нелинейности функции f в ее представлении многочленом имеется слагаемое, содержащее не менее двух сомножителей. Не ограничивая общности рассуждений, можно считать, что это x_1x_2. Тогда можно собрать все слагаемые, в которых имеется этот множитель, вынести его за скобку и записать многочлен в следующем виде:

$f(x_1, x_2, \ldots, x_n) =$
$x_1x_2f_1(x_3, x_4, \ldots, x_n) \oplus x_1f_2(x_3, \ldots, x_n) \oplus x_2f_3(x_3, \ldots, x_n) \oplus f_4(x_3, \ldots, x_n)$.

В силу единственности многочлена функция $f_1(x_3, \ldots, x_n)$ не может быть тождественно равна нулю. Поэтому существуют такие значения $a_3, a_4, \ldots, a_n$, что $f_1(a_3, \ldots, a_n) = 1$.

Теперь рассмотрим функцию:

$g(x_1, x_2) = f(x_1, x_2, a_3, \ldots, a_n) = x_1x_2 \oplus px_1 \oplus qx_2 \oplus r.$

Здесь $p = f_2(a_3, \ldots, a_n)$, $q = f_3(a_3, \ldots, a_n)$, $r = f_4(a_3, \ldots, a_n)$ – константы, равные нулю или единице.

Теперь построим еще одну функцию:

$h(x_1, x_2) = g(x_1 \oplus q, x_2 \oplus p) \oplus pq \oplus r.$

Отметим, что $x_1 \oplus q$ есть либо x_1, если $q = 0$, либо $\overline{x}_1$, если $q = 1$. Аналогично для второй переменной, то есть эти подстановки оговаривались в условии. Сумма $pq \oplus r$ тоже равна либо нулю, либо единице; поэтому справа написана либо функция g, либо $\overline{g}$. Однако

$g(x_1 \oplus q, x_2 \oplus p) \oplus pq \oplus r =$
$(x_1 \oplus q)(x_2 \oplus p) \oplus p(x_1 \oplus q) \oplus q(x_2 \oplus p) \oplus r \oplus pq \oplus r = x_1x_2$ •

14.3 Теорема о функциональной полноте

Теперь подготовлено все необходимое для доказательства критерия полноты, вынесенного в заголовок главы.

Теорема 3 (Е. Пост) Для того чтобы система P булевых функций была полной, необходимо и достаточно, чтобы она не содержалась ни в одном из пяти замкнутых классов:

$T_0,\ T_1,\ S,\ M,\ L.$

Критерий полноты можно формально описать так:

$$[P] = B_2$$

$$\longleftrightarrow \neg(P \subseteq T_0) \wedge \neg(P \subseteq T_1) \wedge \neg(P \subseteq S) \wedge \neg(P \subseteq M) \wedge \neg(P \subseteq L).$$

Доказательство. Если система функций P полна, тогда все условия «невключения» выполнены. Действительно, если бы $P \subseteq T_0$, то в силу монотонности зымыкания имелись бы включения $B_2 = [P] \subseteq [T_0] = T_0 \neq B_2$ - противоречие. Аналогично, полная система не может содержаться ни в каком замкнутом неполном классе. Необходимость китерия доказана.

Докажем достаточность. Если система P не содержится в указанных классах, то сущетсвует набор функций f_0, f_1, f_s, f_m, f_l из P, не принадлежащих соответствующим классам. Вообще говоря, некоторые функции из выбранных пяти могут совпадать, но это несущественно. Можно также считать, что все функции f_i зависят от одних и тех же переменных $x_1, x_2, \dots, x_n$, часть которых фиктивна. Так как полученные функции равны исходным, они, как отмечалось в леммах 1, 2, 3 тоже не принадлежат соответствующим классам. Сначала при помощи функций f_0, f_1, f_s построим константы 0 и 1. Рассмотрим значение $f_0(1, 1, \dots, 1)$. Оно равно либо 1, либо 0. Если $f_0(1, 1, \dots, 1) = 1$, тогда функция $g(x) = f_0(x, x, \dots, x)$ - константа 1, так как $g(0) = f_0(0, 0, \dots, 0) = 1$, в силу того что $f_0 \notin T_0$, и $g(1) = f_0(1, 1, \dots, 1) = 1$ в данном случае. Если же $f_0(1, 1, \dots, 1) = 0$, тогда $g(x) = f_0(x, x, \dots, x) = \overline{x}$. Действительно, $g(0) = f_0(0, 0, \dots, 0) = 1$, как отмечалось, $g(1) = f_0(1, 1, \dots, 1) = 0$ в данном случае. Тогда из f_s при помощи леммы 1 получаем какую-то константу. Теперь, используя $\overline{x}$, строим вторую константу. Таким образом, 0 и 1 всегда получаются как суперпозиции трех указанных функций.

Теперь при помощи леммы 2 из функций 0, 1 и f_m строится отрицание: $\overline{x}$.

При помощи леммы 3 из функций 0, 1, $\overline{x}$ и f_l строится конъюнкция - $x \wedge y$. Таким образом, через функции из P выражена полная система $\{\overline{x}, x \wedge y\}$. Тогда из следствия т. 4 гл. 13 система P полна $\bullet$

Следствие 1. Всякий неполный класс K булевых функций содержится в одном из построенных классов:

$$T_0,\ T_1,\ S,\ M,\ L\ \bullet$$

Определение. Класс K булевых функций называется максимальным или *предполным*, если K неполный, но любое его расширение полно: то есть для любой функции $f \in B_2 \backslash K$ класс $K \cup \{f\}$ полон: $[K \cup \{f\}] = B_2$.

Замечание. Максимальный класс является замкнутым.

Действительно, пусть K - максимальный класс. Всегда $K \subseteq [K]$. Если $K \neq [K]$, тогда существует функция $f \in [K] \backslash K$ и для нее $[K \cup \{f\}] \subseteq [[K]]$ в силу монотонности замыкания. Но так как K максимальный, $[K \cup \{f\}] = B_2$ откуда: $B_2 = [[K]] = [K]$, значит, класс K полный, что противоречит условию максимальности $\bullet$

Следствие 2. В B_2 имеется ровно пять максимальных классов:

$$T_0,\ T_1,\ S,\ M,\ L.$$

Доказательство. Сначала рассмотрит таблицу, показывающую, что все пять рассматриваемых классов не содержатся друг в друге:

$*$	T_0	T_1	S	M	L
T_0	$*$	0	0	$x \oplus y$	xy
T_1	1	$*$	1	$\overline{x \oplus y}$	xy
S	$\overline{x}$	$\overline{x}$	$*$	$\overline{x}$	$xy \vee xz \vee yz$
M	1	0	0	$*$	xy
L	1	0	0	$\overline{x}$	$*$

В таблице на пересечении i-й строки и j-го столбца указана функция, которая содержится в i-м классе и не содержится в j-м. Самый левый столбец и верхняя строка - не в счет, это обозначения классов. Например, в пятой строке и третьем столбце указана функция 0, это значит, что $0 \in L \wedge 0 \notin S$. Наоборот, в третьей строке и пятом столбце указана функция трех переменных, упоминавшаяся ранее в примерах самодвойственных функций, то есть она лежит в S, но не содержится в L. Таблицу можно проверить или придумать другие функции, которые подтвердили бы наше высказывание, во всяком случае верно, что любые два указанных класса друг друга не содержат.

Отсюда легко следует, что все пять классов являются максимальными. Действительно, для доказательства максимальности T_0 надо доказать, что если $f \notin T_0$, то класс $P = T_0 \cup \{f\}$ полный. Класс P не содержится в T_0 по построению, а в остальных четырех классах не содержится даже T_0, тем более P. Тогда, согласно теореме Поста, класс P полный. Совершенно такие же рассуждения для доказательства максимальности остальных классов, так как условия для всех классов одинаковы.

Других максимальных классов нет. Действительно, всякий максимальный класс является замкнутым, согласно замечанию. Всякий замкнутый класс, согласно следствию 1, содержится в одном из построенных классов, а тогда в силу максимальности совпадает с ним •

Последнее следствие показывает роль пяти избранных классов.

Задачи и упражнения

1. Каково число булевых функций от n переменных, принимающих на противоположных наборах одинаковые значения?

2. Каково число булевых функций от n переменных, принимающих на смежных наборах противоположные значения?

3. Каково число булевых функций от n переменных, принимающих значение 1 не менее чем на k наборах?

Пусть

$C = \{f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_m), \ldots, f_l\}$

множество булевых функций. Определим понятие dep g *глубины формулы над* C по индукции:

1 - если g - символ переменной или константы из C, то dep $g = 0$;

2 - если $g = f_i(g_1, g_2, \ldots, g_k)$, где $f_i(x_1, x_2, \ldots, x_k) \in C$ и $g_1, g_2, \ldots, g_k$ - формулы над C, то dep $g = \max\limits_{1 \le r \le k} \mathrm{dep}(g_r) + 1$.

4. Найти формулы над $C = \{x \downarrow y\}$ и над $C = \{|\}$ минимальной глубины, реализующие функции:

$f = x \vee y,\ f = x \oplus y,\ f = x \cdot y$. 5. Можно ли реализовать функцию f формулой над C глубиной k, если:

1)$f = x \to y,\ k = 3,\ C = \{\wedge,\ \neg\}$;

2)$f = x \oplus y \oplus z,\ k = 2,\ C = \{\to, \wedge\}$.

6. Можно ли реализовать функцию f формулой над C

глубиной $k+1$, если она реализуется формулой глубины k над C?

7. Доказать, что если функция f реализуема формулой над C глубины k, то она реализуема над C некоторой формулой, глубина которой больше k.

Длиной СДНФ называется количество элементарных конъюнкций, используемых для построения данной СДНФ. Длиной булева многочлена называется количество различных одночленов, используемых для построения данного многочлена.

8. Найти число различных булевых многочленов длины k от n переменных, равных нулю на нулевом и единичном наборах значений переменных.

9. Найти булеву функцию от n переменных, у которой длина многочлена в 2^n раз превосходит длину её СДНФ.

10. Доказать, что количество функций, существенно зависящих от n переменных, равно

$$\sum_{k=0}^{n}(-1)^k C_n^k 2^{2^{n-k}}.$$

11. Доказать, что x_i является существенной переменной функции f тогда и только тогда, когда x_i явно входит в булев многочлен функции f.

12. Доказать, что если функция f существенно зависит от переменной x_i, то функция f^* также существенно зависит от x_i.

13. Перечислить все самодвойственные функции, существенно зависящие от переменных x, y, z.

14. Перечислить все функции, существенно зависящие от трех переменных, такие, что отождествление любых двух переменных приводит к функции, существенно за-

висящей ровно от одной переменной.

15. Определить количество неравных самодвойственных функций, существенно зависящих от n переменных.

16. Доказать, что если с помощью отождествления переменных из функции f от n переменных, $n \geq 3$, нельзя получить функцию, существенно зависящую ровно от двух переменных, то функция f самодвойственная.

17. Пусть L_n - множество линейных функций от переменных

$x_1, x_2, \ldots, x_n$.

Найти число самодвойственных функций, принадлежащих множеству L_n.

18. Доказать, что функция, существенннo зависящая от всех своих переменных, является линейной тогда и только тогда, когда при замещении любого подмножества переменных любым набором констант получается функция, существенно зависящая от всех оставшихся переменных.

19. Доказать, что из многочлена степени $k \geq 3$ можно с помощью отождествления переменных получить многочлен степени $k-1$.

Пусть D - замкнутый класс в B_2. Подмножество $K \subseteq D$ называется полной системой в D, если $[K] = D$. Множество K называется неприводимой системой, если замыкание любого собственного подмножества K_1 из K меньше замыкания всего множества K: $[K_1] \subset [K]$ и $[K_1] \neq [K]$. Неприводимая полная в замкнутом классе D система K называется базисом класса D.

20. Доказать, что любой базис в T_0 содержит не более трех функций. Дать примеры базисов класса T_0, состоящих из одной, двух и трёх функций.

21. Доказать, что любой базис в $T_0 \cap T_1$ содержит не

более двух функций. Привести пример базиса, состоящего из одной функции.

22. Каково число монотонных самодвойственных функций, существенно зависящих ровно от четырёх переменных?

23. Доказать, что всякая монотонная функция содержится не менее чем в двух классах из трех: T_0, T_1, L.

Обобщим понятие элементарной конъюнкции. Формулу

$x_{k_1}^{c_1} \cdot x_{k_2}^{c_2} \cdot \ldots \cdot x_{k_r}^{c_r}$,

где x_i – попарно различные переменные из набора

$x_1, x_2, \ldots, x_n$, а $c_i \in \{0, 1\}$, будем называть элементарной конъюнкцией (э.к.) на множестве $\{x_1, x_2, \ldots, x_n\}$. Как обычно, полагаем, что $x^1 = x$, $x^0 = \bar{x}$. Элементарная конъюнкция называется монотонной, если она не содержит отрицаний переменных. Дизъюнкция нескольких различных элементарных конъюнкций называется дизъюнктивной нормальной формой (ДНФ). Аналогичные двойственные определения для элементарных дизъюнкций и СНФ.

24. Доказать, что любая монотонная функция, отличная от константы, имеет ДНФ из монотонных э.к. Аналогичное утверждение имеется для КНФ.

25. Доказать, что система $\{0,\ 1,\ x \cdot y,\ x \vee y\}$ образует базис в M.

26. Доказать, что всякий базис в M содержит не более четырёх и не менее трёх функций.

27. Доказать, что любая функция из $M \cap S$, существенно зависящая более чем от одной переменной, образует базис в $M \cap S$.

28. Доказать, что если функция f существенно зависит

более, чем от одной переменной и принадлежит классу $M \cap S$, то система $\{0, \bar{f}\}$ полна в B_2.

29. Привести пример шефферовой функции (то есть функции, являющейся базисом в B_2), зависящей существенно от минимального числа переменных и принимающей значение 1 ровно на половине всех наборов значений переменных.

30. Доказать, что базисами в T_0 являются следующие системы: $\{xy, x \oplus y\}$, $\{x \vee y, x \oplus y\}$, $\{xy \oplus z\}$.

31. Доказать, что базисами в T_1 являются следующие системы: $\{x \vee y, x \equiv y\}$, $\{xy, x \equiv y\}$.

32. Доказать, что базисом в S является следующая система:

$\{\overline{xy \vee xz \vee yz}\}$.

33. Привести примеры трёх базисов в L.

Решения, указания, ответы

Множества

1. Ответ: $A \cup B = A \triangle B \triangle (A \cap B)$.

Замечания. В ответе учтена ассоциативность симметрической разности (задача 9) и тот факт, что для непересекающихся множеств X и Y симметрическая разность совпадает с объединением: $X \overset{\bullet}{\cup} Y = X \triangle Y$ $\bullet$

14. Ответ: решение уравнения существует тогда и только тогда, когда $A \subseteq B$. В этом случае решением является любое множество X, удовлетворяющее условиям: $B \backslash A \subseteq X \subseteq B$.

Указание. Действительно, если решение при каких-то A и B существует, то, очевидно, $A \subseteq B$ и $X \subseteq B$. Кроме того, $B \backslash A \subseteq X$. Таким образом, все условия ответа выполнены. Обратное также легко проверяется: при выполнении условий ответа любое указанное множество X является решением $\bullet$

15. Ответ: решение уравнения существует тогда и только тогда, когда $A \subseteq B$. В этом случае решением является любое множество X, удовлетворяющее условию: $X \cap B = A$.

Решение. Пусть для некоторых множеств A и B существует решение X данного уравнения. Тогда $(A \backslash X) \cup (X \backslash A) = X \backslash B$ - верное равенство, и потому $A \backslash X = \emptyset$, то есть $A \subseteq X$, и потому $X \backslash A = X \backslash B$.

Докажем, что $A \subseteq B$. Действительно, если $x \in A \subseteq X$, то $x \in X$ и $x \notin X \backslash A = X \backslash B$, значит, $x \in B$.

Докажем, что $X \cap B = A$. Действительно, если $x \in X \cap B$, то $x \in X$ и $x \notin X \backslash B = X \backslash A$, откуда получаем: $x \in A$. Обратно, если $x \in A \subseteq X$, то снова $x \notin X \backslash A = X \backslash B$ и, значит, $x \in B$ и $x \in X \cap B$. Таким образом, если решение уравнения существует, то выполнены оба условия, указанные в ответе.

Проверим обратное утверждение: если выполнено условие на A и B, то любое множество X, удовлетворяющее условию $X \cap B = A$, является решением уравнения.

Действительно, рассмотрим любое множество X, удовлетворяющее условию $X \cap B = A$. Тогда $A \subseteq X$, и потому

$A \triangle X = (A \backslash X) \cup (X \backslash A) = X \backslash A.$

Так как $A \subseteq B$ получаем, что $X \backslash B \subseteq X \backslash A$, и остается доказать обратное включение. Пусть $x \in X \backslash A$. Тогда $x \in X \wedge x \notin A$. В силу равенства $A = X \cap B$ это означает, что $x \notin B$, и тогда $x \in X \backslash B$. Значит, $X \backslash A \subseteq X \backslash B$, и, следовательно, эти множества совпадают •

16. Ответ: Решение уравнения существует тогда и только тогда, когда $A \cap B = \emptyset$. В этом случае решением является любое множество X, удовлетворяющее условиям: $A \subseteq X \subseteq A \cup B$.

Решение. Пусть для некоторых множеств A и B существует решение X данного уравнения. Тогда, в силу верного равенства $(A \backslash X) \cup (X \backslash A) = B \cap X$ получаем $A \backslash X = \emptyset$, то есть $A \subseteq X$. Тогда $A \triangle X = X \backslash A = B \cap X$. Отсюда следует, что $A \cap B = \emptyset$.

Действительно, если $x \in A \cap B$, то $x \notin X \backslash A$ и в то же время $x \in B \cap X$ - противоречие. Докажем второе условие, указанное в ответе: $X \subseteq (A \cup B)$. Пусть $x \in X$. Тогда либо $x \in A$, либо $x \notin A$. В первом случае получаем, что $x \in (A \cup B)$, во втором - $x \in X \backslash A = B \cap X$. Таким образом, $x \in B$, и, значит, $x \in (A \cup B)$. Отсюда следует, что, второе условие выполнено в любом случае. С учетом полученного ранее включения A в X заключаем, что, оба условия, приведенные в ответе, необходимы. Можно доказать и обратное: любое множество X, удовлетворяющее отмеченным условиям, является решением уравнения.

Действительно, в этом случае $A \triangle X = X \backslash A$, и надо доказать, что $X \backslash A = B \cap X$. Пусть $x \in X \backslash A$. Тогда $x \in X$ и $x \notin A$.

Согласно условию, $x \in A \cup B$, значит, получаем, что $x \in B$ и тогда $x \in B \cap X$. Получили, что $(X \backslash A) \subseteq (B \cap X)$. Докажем обратное включение. Пусть $x \in B \cap X$. Тогда $x \in B$ и $x \in X$.

Так как $A \cap B = \emptyset$, получаем, что $x \notin A$. Значит, $x \in X \backslash A$, и получено обратное включение: $(B \cap X) \subseteq (X \backslash A)$. Значит, $X \backslash A = B \cap X$ •

17. Ответ: решение уравнения существует тогда и только тогда, когда $A \subseteq B$. В этом случае решением является любое множество X, удовлетворяющее условиям: $B \backslash A \subseteq X$ и $X \cap A = \emptyset$ •

21. Ответ: решение уравнения существует тогда и только тогда, когда $B \subseteq A$. В этом случае решением является любое множество X, удовлетворяющее условиям: $A \backslash B \subseteq X \subseteq A$ •

22. Ответ: единственное решение системы –

$$X = B \cup (C \backslash A),$$

существующее, если $B \subseteq A \subseteq C$.

Решение. Пусть система при некоторых A, B и C имеет решение X. Тогда выполнены следующие соотношения: $B = A \cap X \subseteq A \subseteq A \cup X \subseteq C$. Таким образом, $B \subseteq A \subseteq C$ - необходимые условия. Докажем, что эти условия являются и достаточными. То есть если они выполняются, существует (и даже единственное) решение X нашей системы. Если решение сушествует, то $B = A \cap X \subseteq X$ из первого уравнения. $C \backslash A \subseteq X$ - из второго уравнения. Таким образом, $B \cup (C \backslash A) \subseteq X$. Докажем, что $X = B \cup (C \backslash A)$. Пусть $x \in X$; тогда если $x \in A$, то $x \in A \cap X = B \subseteq B \cup (C \backslash A)$. Если же $x \in X \wedge x \notin A$, то $x \in X \cup A = C$, значит, $x \in C \backslash A \Rightarrow x \in B \cup (C \backslash A)$. Таким образом, если X - решение системы, то $X = B \cup (C \backslash A)$. Для завершения решения задачи остается только проверить, что приведенная выше формула для X действительно удовлетворяет системе, если множества A, B и C удовлетворяют приведенным ранее условиям включения. Подставим выражение для X, например, в первое уравнение:

$A \cap (B \cup (C \backslash A)) = (A \cap B) \cup (A \cap (C \backslash A)) = A \cap B = B.$

Первое равенство верно в силу дистрибутивности пересечения относительно объединения, последнее - в силу включения $B \subseteq A$.

Аналогично проверяется и второе уравнение $\bullet$

23. Ответ: единственное решение системы - $X = A \backslash B$, существующее, если $B \subseteq C \subseteq A$.

Решение. Пусть система при некоторых A, B и C имеет решение X. Тогда из первого уравнения получаем:

$A \triangle (A \triangle X) = A \triangle B = (A \triangle A) \triangle X = \emptyset \triangle X = X.$

Таким образом, $X = A \triangle B$. Кроме того, из второго уравнения заключаем, что $C \subseteq A$ и $X \subseteq A$. Как доказано,

$X = A \triangle B = (A \backslash B) \cup (B \backslash A) \subseteq A \Rightarrow B \backslash A = \emptyset.$

Отсюда следует, что $B \subseteq A$ и $X = A \backslash B$. А тогда, в силу равенства $C \cup (A \backslash B) = A$, получаем, что $B \subseteq C$. Действительно, если $x \in B$, то $x \in A$ и $x \notin A \backslash B$ и, значит, $x \in C$.

Таким образом, если решение системы существует, то все указанные в ответе условия выполнены. Остается проверить обратное: если все условия ответа выполнены, то $X = A \backslash B$ является решением системы. Это непосредственная проверка $\bullet$

24. Ответ: единственное решение системы - $X = C \backslash (A \cap B)$, существующее, если $C = A \cup B$ $\bullet$

25. Ответ: единственное решение системы - $X = C \cup (A \backslash B)$, существующее, если $C = B \backslash A$ $\bullet$

26. Ответ: единственное решение системы - $X = A \cup B$, существующее, если $A \subseteq C$ и $B \cap C = \emptyset$ $\bullet$

27. Ответ: единственное решение системы - $X = A \cup B$, существующее, если $A \subseteq C$ и $B \cap C = \emptyset$ $\bullet$

28. Ответ: единственное решение системы - $X = A \triangle B$, существующее, если $A \cap B = C$ •

30. Ответ: единственное решение системы - $X = C \backslash B$, существующее, если $B \subseteq A \subseteq C$ •

31. Ответ: решением системы является любое множество X, удовлетворяющее условиям: $C \subseteq X$ и $X \cap B = \emptyset$. Решение существует тогда и только тогда, когда $A = B \cup C$ и $B \cap C = \emptyset$ •

32. Ответ: единственное решение системы - $X = B \cup C$, существующее, если $C \subseteq A$ и $A \cap B = \emptyset$ •

33. Ответ: решением системы является любое множество X, удовлетворяющее условиям: $B \subseteq X \subseteq C$. Решение существует тогда и только тогда, когда $A \cap C = \emptyset$ и $A \cup B = C$ •

34. Ответ: единственное решение системы - $X = B \backslash A$, существующее, если $A \subseteq C \subseteq B$ •

41. Ответ: решением системы является любое множество X, удовлетворяющее условиям: $A \subseteq X \subseteq A \cup B$. Решение существует тогда и только тогда, когда $A = C$ и $A \cap B = \emptyset$.

Решение. Пусть для некоторых множеств A, B и C существует решение X данной системы. Тогда, в частности, X является решением первого уравнения системы. Из решения задачи 16 получаем, что $A \cap B = \emptyset$ и $A \subseteq X \subseteq A \cup B$. Тогда, с учетом включения A в X второе уравнение приобретает вид: $A \cap X = A = C$. То есть условия, приведенные в ответе, необходимы. Ясно, что они и достаточны •

44. Решение - непосредственная проверка совпадения

отношений в правой и левой частях равенства:

$$(a,c) \in (\bigcup_{i\in I} G_i) \circ H \Rightarrow \exists b \in B : (a,b) \in \bigcup_{i\in I} G_i, (b,c) \in H.$$

Это означает, что $\exists i_0 \in I : (a,b) \in G_{i_0}$. Тогда $(a,c) \in G_{i_0} \circ H$, а, значит,

$$(a,c) \in \bigcup_{i\in I} (G_i \circ H).$$

Тем самым доказано включение левой части равенства в правую. Обратное включение доказывается дословным воспроизведением выкладок в обратном порядке •

48. Решение. Считаем, что G_1, G_2, H – соответствия из A в A, где $A = \{a,b,c,d\}$. При этом

$$G_1 = \{(a,a),(b,b),(c,c),(d,d),(a,b)\},$$

то есть G_1 состоит из множества I диагональных пар и пары (a,b). G_2 аналогично состоит из диагонали I и пары (a,c); $H = I \cup \{(b,d),(c,d)\}$. Тогда $G_1 \cap G_2 = I$, и потому $(G_1 \cap G_2) \circ H = H$. Используя утверждение задачи 1, получаем:

$$G_1 \circ H = (I \cup \{(a,b)\}) \circ H = (I \circ H) \cup (\{(a,b)\} \circ H).$$

Значит, $G_1 \circ H = H \cup \{(a,b),(a,d)\}$. При этом пара (a,d) является суперпозицией пар (a,b) и (b,d). Аналогично $G_2 \circ H = H \cup \{(a,c),(a,d)\}$. Пара (a,d) является теперь суперпозицией пар (a,c) и (c,d). Таким образом, $(G_1 \circ H) \cap (G_2 \circ H) = H \cup \{(a,d)\} \neq H$. Это означает, что в задаче 2 не всегда имеется равенство. Аналогичный пример можно построить для задачи 4. Включения для обеих задач доказываются аналогично задаче 1 •

49. Решение. По определению обратного соответствия, пара $(a,b) \in G^{-1}$ тогда и только тогда, когда $(b,a) \in G$.

Это означает, что $b > 0$ и $a = log_2 b$, то есть $b = 2^a$. Другими словами, $(a, b) \in H$. Это означает, что $G^{-1} = H$.

Пусть $(a, c) \in G \circ H$. По определению суперпозиции отношений это означает, что $\exists b \in B$, такое, что $(a, b) \in G$ и $(b, c) \in H$. По определению G и H это, в свою очередь, означает, что $b = log_2 a$ и $c = 2^b$. Значит, $a > 0$ и $c = a$. Графически $G \circ H$ есть луч - биссектриса первой четверти.

Если $(a, c) \in H \circ G$, это аналогично означает, что некоторые пары $(a, b) \in H$ и $(b, c) \in G$. Значит, $b = 2^a$ и $c = log_2 b$. Получаем, что $H \circ G$ есть прямая $c = a$ - биссектриса первой и третьей координатных четвертей •

50. Решение. По определению отношения видно, что G симметрично, то есть $G^{-1} = G$. Графически, на плоскости R^2, G изображается следующей фигурой (рис. 3, а)):

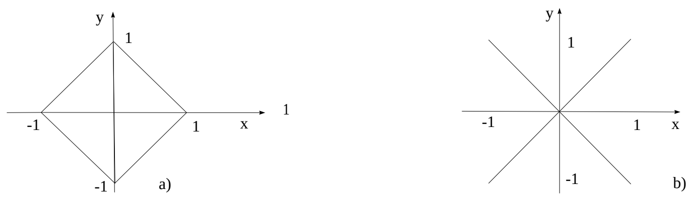

Рис. 3.

Рассмотрим суперпозицию $G \circ G$. По определению, пара $(x, y) \in G \circ G$ тогда и только тогда, когда существует такое $t \in R$, что $(x, t) \in G$ и $(t, y) \in G$. Это означает, что

$$\begin{cases} |x| + |t| = 1 \\ |t| + |y| = 1 \end{cases} \qquad (1)$$

Если выполняются уравнения (1), то $|x| \leq 1$, $|y| \leq 1$ и $|x| = |y|$. Обратно: если пара чисел (x, y) удовлетворяет указанным условиям, то существует число t такое, что пары (x, t) и (t, y) удовлетворяют уравнениям (1). В качестве t можно взять $t = 1 - |x|$. Таким образом, $G \circ G$ совпадает с множеством (x, y), для которых $|x| = |y|$ и

$|x| \leq 1$. Графически это множество представлено на рис. 3, b) $\bullet$

51. Решение. Бинарное отношение G изображено на плоскости на рис. 4 a). Если же пара чисел $(x, y) \in G \circ G$, это означает, что существует такое $t \in R$, что выполнены следующие условия:

$$\begin{cases} |x| + t \leq 1 \\ |t| + y \leq 1 \end{cases} \qquad (2)$$

Из этих условий следует, что $y \leq 1, t \leq 1-|x|, y-1 \leq t \leq 1-y$. В свою очередь, из полученных условий выводим, что $y - 1 \leq 1 - |x|$. Таким образом получаем, что если пара $(x, y) \in G \circ G$, то выполнена система неравенств:

$$\begin{cases} |x| + y \leq 2 \\ \quad y \leq 1 \end{cases} \qquad (3)$$

Докажем, что выполнено и обратное заключение, то есть, если пара (x, y) удовлетворяет (3), то она содержится в суперпозиции $G \circ G$. Действительно, пусть $t = y-1$. Тогда будут выполнены неравенства $y-1 \leq t \leq 1-y$, в силу того что $y \leq 1$. Но из полученных для t неравенств следует, что $|y| \leq 1 - y$. Кроме того, из первого неравенства системы (3) и определения t следует, что $t \leq 1-|x|$. Таким образом, для пар (x, t) и (t, y) выполнены условия (2). Это означает, что пары лежат в G, а пара (x, y) - в суперпозиции $G \circ G$. Другими словами, $G \circ G$ определяется неравенствами (3), графическое представление отношения дано на рис. 4 b).

Теперь рассмотрим произведение $G^{-1} \circ G$. Если пара (x, y) принадлежит произведению, это означает, что существует $t \in R$, такое, что $(x, t) \in G^{-1}$ и $(t, y) \in G$. Значит, $(t, x) \in G$ и $(t, y) \in G$, то есть выполнена система

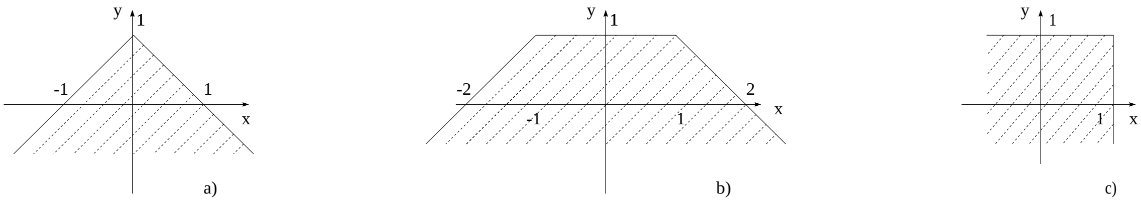

Рис. 4.

неравенств:

$$\begin{cases} |t| + x \leq 1 \\ |t| + y \leq 1 \end{cases} \qquad (4)$$

Из приведенных неравенств следует, что $x \leq 1, y \leq 1$. Легко понять, что верно и обратное: если пара (x, y) удовлетворяет двум последним неравенствам, то она удовлетворяет и системе (3), в которой можно положить $t = 0$. Таким образом, $G^{-1} \circ G$ есть угол, задаваемый неравенствами $x \leq 1, y \leq 1$ и изображенный на рис. 4 c).

Рассмотрим, наконец, произведение $G \circ G^{-1}$. Если пара (x, y) принадлежит произведению, это, аналогично предыдущим случаям, означает, что существует $t \in R$, такое, что $(x, t) \in G$ и $(t, y) \in G^{-1}$. Значит, $(y, t) \in G$, и выполнена система неравенств:

$$\begin{cases} |x| + t \leq 1 \\ |y| + t \leq 1 \end{cases} \qquad (5)$$

Ясно, что для любой пары (x, y) имеется подходящее t, такое, что полученная система неравенств (4) выполняется. Для этого в качестве t можно взять достаточно большое по абсолютной величине отрицательное число. Это означает, что $G \circ G^{-1} = R^2$ ●

53. Ответы. Отношение G графически представлено на рис. 5 а). $G^{-1} \circ G = R^2$. Отношение $G \circ G$ определяется

системой неравенств:

$$\begin{cases} |y| \leq x+2 \\ -1 \leq x \end{cases} \tag{6}$$

Графическое представление этого отношения дано на рис. 5 b). Отношение $G \circ G^{-1}$ задается системой неравенств $-1 \leq x, -1 \leq y$, его графическое представление - рис. 5 c) •

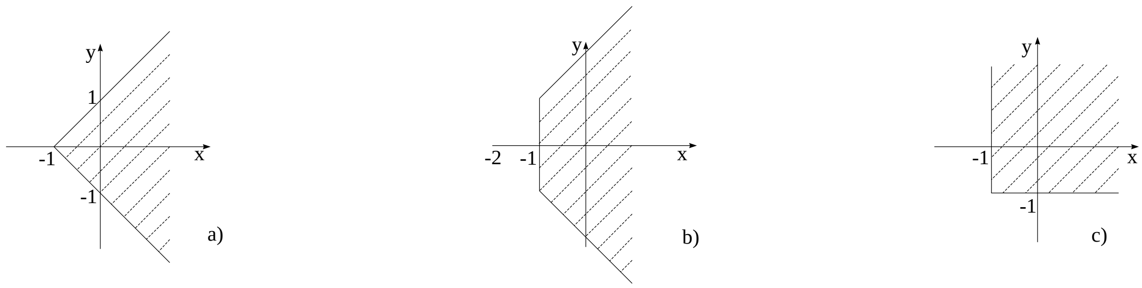

Рис. 5.

54. Ответы. $G \circ G^{-1} = R^2$, $G^{-1} \circ G = R^2$, $G \circ G = R^2$ •

58. Указание: рассмотреть отношение неравенства •

59. Решение. Пусть $A = \{a, b, c\}$ - произвольное множество из трех элементов. Определим отношение

$$G = \{(a,a),(b,b),(c,c),(a,b),(b,c)\}$$

на этом множестве. Тогда G является рефлексивным, так как содержит диагональ $I = \{(a,a),(b,b),(c,c)\}$. Кроме того, G является антисимметричным, так как не содержит пар вида (x, y) и (y, x), кроме диагональных. G не является транзитивным, так как не содержит пары (a, c) - транзитивного замыкания пар $(a, b), (b, c)$ •

60. Решение. Рассмотрим множество A и отношение G задачи 59. Дополним G двумя парами: $(b, a), (c, b)$. Рутинная проверка показывает, что полученное отношение $G_1 = G \cup \{(b, a), (c, b)\}$ удовлетворяет условиям задачи •

Замечание. Практически во всех задачах этого раздела можно приводить более интересные примеры отношений на основных математических множествах, таких как различные множества чисел, геометрических фигур или функций. Например, для задачи 3 в качестве примера можно взять отношение $G = \{(x, y) : |x - y| \leq 1\}$ на парах действительных чисел. Предлагаем построить подобные естественные и интересные примеры для других задач.

64. Решение. Пункт а). Пусть $A = \{a, b, c, d\}$ - произвольное множество из четырех элементов. Определим отношения:

$$G = \{(a, b), (b, c), (a, c), (d, a), (d, b), (d, c)\},$$

$$H = \{(a, b), (b, d), (a, d)\}$$

на данном множестве. Легко проверить, что, согласно определению суперпозиции, получим:

$$G \circ H = \{(a, d), (d, b), (d, d)\}.$$

Также легко убедиться, что G и H транзитивные, а $G \circ H$ - нет. Пункт б). На том же множестве A определим следующие отношения:

$$G = \{(a, b), (b, c), (a, c), (d, b), (d, c)\},$$

$$H = \{(a, b), (b, d), (a, d), (b, c), (a, c)\}.$$

Снова легко проверить, что

$$G \circ H = \{(a, d), (a, c), (d, c), (d, d)\}$$

и G, H и $G \circ H$ транзитивны •

78. Указание. Сначала рассмотреть случай $A \cap B = \emptyset$. Тогда, по условию, A равномощно интервалу $(0, 1)$, а B

равномощно интервалу $(1,2)$ и объединение $A \cup B$ равномощно интервалу $(0,2)$ с «выколотой» единицей. Если из несчетного множества $(0,2)$ исключается конечное или счетное множество, то остающееся множество равномощно исходному (т. 1 гл. 4).

Если же A и B имеют непустое пересечение, рассмотреть следующее представление: $A \cup B = A \cup (B \backslash A)$. В правой части равенства объединяемые множества уже не пересекаются. Далее строятся такие же биекции, как и ранее, но для заключения о равномощности надо применить теорему Кантора – Бернштейна (т. 5 гл. 4)$\bullet$

79. Решение. Сначала отметим, что множество всевозможных последовательностей из нулей и единиц является континуальным. Фактически это доказано в т. 2 гл. 5. Действительно, всякое число из интервала $(0,1)$ однозначно представляется своим двоичным разложением. При этом используются всевозможные последовательности, кроме стабилизирующихся на 1. Таких исключительных последовательностей - счетное множество. Поэтому, согласно т. 7 гл. 3, множество всех последовательностей равномощно множеству двоичных разложений и потому континуально. Далее можно отметить, что множество последовательностей из нулей и единиц и множество последовательностей из элементов a и b находятся в очевидном биективном соответствии $\bullet$

80. Решение. Согласно предыдущей задаче, множество всевозможных бинарных последовательностей континуально. Далее, между последовательностями чисел из $\mathbb{N}$ и 0-1-последовательностями устанавливаем соответствие по правилу:

$(3,1,5,\ldots,2,\ldots) \to (1,1,1,0,1,0,1,1,1,1,1,\ldots,1,1,\ldots)$,

записывая каждое число соответствующим количеством единиц и разделяя последовательности единиц нулями. Считаем при этом, что $0 \in \mathbb{N}$ и нулю соответствует пустое количество единиц. Тогда легко понять, что получается биекция множества $\mathbb{N}_\infty$ на $(F_2)_\infty$ •

81. Указание. Отметим, что если $f : A \to B$ - биекция множества A на множество B, то автоматически строится биекция f_∞ множества A_∞ на B_∞ по следующему правилу:

$f_\infty(a_1, a_2, a_3, \ldots) = (f(a_1), f(a_2), f(a_3), \ldots)$.

То есть попросту сказать - действие f_∞ на последовательность происходит покомпонентно с помощью f. Далее применяем предыдущую задачу •

82. Решение. Множество $\mathbb{R}$ действительных чисел континуально, как следует из т. 2 гл. 4. Поэтому, согласно задаче 5, если C - счётное множество, то $|\mathbb{R}| = |C_\infty|$. Значит, каждому $\alpha \in \mathbb{R}$ можно однозначно сопоставить элемент из C_∞ - последовательность элементов множества C:

$$\alpha \to (c_1, c_2, c_3, \ldots).$$

Тогда последовательности действительных чисел будет сопоставлена полубесконечная таблица:

$$T = \begin{cases} \alpha_1 & \to & (c_{11}, & c_{12}, & c_{13}, & \ldots) \\ \alpha_2 & \to & (c_{21}, & c_{22}, & c_{23}, & \ldots) \\ \alpha_3 & \to & (c_{31}, & c_{32}, & c_{33}, & \ldots) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{cases}$$

Теперь каждой такой таблице T можно сопоставить последовательность из C_∞ следующим образом:

$$T \to (c_{11}, c_{12}, c_{21}, c_{13}, c_{22}, c_{31}, \ldots).$$

Легко понять, что указанное соответствие является биекцией между множеством всевозможных таблиц и множеством всех последовательностей из C. Множество последовательностей из C, то есть C_∞ континуально, как отмечалось выше •

Замечание. Отметим, что соответствие, сопоставляющее таблице T последовательность из C_∞, использовалось в т. 5 гл. 3.

83. Указание. Рассмотреть множество функций на отрезке $[a, b]$, принимающих только два значения - 0 и 1. Множество таких функций находится в биективном соответствии с множеством всех подмножеств отрезка, то есть с булеаном $B([a, b])$. Согласно т. 1 гл. 5, $|[a, b]| < |B([a, b])|$. Тогда множество всех функций на отрезке тем более имеет мощность больше континуальной •

84. Указание. Доказать, что функция, непрерывная на отрезке $[a, b]$, однозначно определяется своими значениями в рациональных точках отрезка. После этого использовать результат задачи 82 •

Логика

1. Указание. Два раза применить МР и теорему о дедукции к следующему набору условий:

$$A \to B,\ B \to C,\ A \bullet$$

3. Решение.

1. $A \to B,\ A \vdash B$; МП
2. $B\ \vdash\ B \vee C$; введение дизъюнкции
3. $A \to B,\ A \vdash\ B \vee C$; т. о транз. выводимости 1, 2
4. $A \to B,\ C \vdash\ C$; тождественно
5. $C \vdash\ B \vee C$; введение дизъюнкции
6. $A \to B,\ C \vdash\ B \vee C$; т. о транзитивности 4, 5
7. $A \to B,\ A \vee C \vdash\ B \vee C$; удаление дизъюнкции 3, 6
8. $A \to B \vdash\ (A \vee C) \to (B \vee C)$; МР 7 ●

Замечание. Решение задачи 3 дано в виде последовательности некоторых утверждений о выводимости, каждое из которых снабжено комментарием - обоснованием. Эта форма соответствует требованиям, изложенным в п. 7.1. Предполагается, что решения других задач о выводимости должны оформляться в таком же виде.

5. Решение.

1. $A \to \neg B,\ B,\ A \vdash\ B$; тождественно
2. $A \to \neg B,\ B,\ A \vdash\ \neg B$; МР
3. $A \to \neg B,\ B \vdash \neg A$; введение отрицания 1, 2
4. $A \to \neg B \vdash B \to \neg A$; т. о дедукции 3 ●

7. Решение.

1. $A,\ \neg A \vdash A$; тождественно
2. $A,\ \neg A \vdash \neg A$; тождественно
3. $A \vdash \neg\neg A$; введение отрицания 1, 2 ●

9. Указание. Смотрите лемму о законе исключённого третьего - п. 8.3 ●

10. Решение.

1. $B \vdash A \to B$	; введение импликации
2. $A \to B \vdash (A \to B) \vee (B \to A)$	; введение дизъюнкции
3. $B \vdash (A \to B) \vee (B \to A)$	; т. о транзитивности 1. 2
4. $\neg B \vdash B \to A$	; лемма о противоречии
5. $B \to A \vdash (A \to B) \vee (B \to A)$	; введение дизъюнкции
6. $\neg B \vdash (A \to B) \vee (B \to A)$	; т. о транзитивности 4, 5
7. $B \vee \neg B \vdash (A \to B) \vee (B \to A)$	; удаление дизъюнкции 3, 6
8. $\vdash (A \to B) \vee (B \to A)$	; т. о транз-ти, задачи 9, 7 •

12. Указание. Докажем следующее утверждение:

$$\neg A \vee B \vdash A \to B$$

1. $\neg A,\ A \vdash B$	; лемма о противоречии
2. $B,\ A \vdash B$	; тождественно
3. $\neg A \vee B,\ A \vdash B$	; удаление дизъюнкции 1, 2
4. $\neg A \vee B \vdash A \to B$	; т. о дедукции 3

Для полного решения задачи требуется еще установить выводимость в обратном направлении, что предлагается для самостоятельного решения •

14. Указание. «Набросок» вывода в одном направлении:

1. $A \wedge B \vdash A,\ A \wedge B \vdash B$	; $\wedge$-удаление
2. $\neg A \vdash \neg(A \wedge B),\ \neg B \vdash \neg(A \wedge B)$	; л. о противоположной т.
3. $\neg A \vee \neg B \vdash \neg(A \wedge B)$	; $\vee$-удаление •

18. Указание. Рассмотрим для примера монотоннность дизъюнкции. Для этого требуется доказать, что если $\mathcal{A} \vdash \mathcal{B}$, то $X \vee \mathcal{A} \vdash X \vee \mathcal{B}$. Это утверждение легко следует из утверждения задачи 3. К аналогичным простым задачам о выводимости сводятся и остальные утверждения о монотонности •

19. Указание. Индукция по количеству связок в формуле $\mathcal{F}$ •

20. Указание. Пусть $\mathcal{G}$ - подформула $\mathcal{F}$ и $\mathcal{H}$ равносильна $\mathcal{G}$. Можно провести индукцию относительно количества k логических связок формулы $\mathcal{F}$, расположенных вне $\mathcal{G}$.

Если k равно 0, то $\mathcal{F} = \mathcal{G}$, $\mathcal{F}_1 = \mathcal{H}$, и всё доказано. Если $k > 0$, то $\mathcal{F}$ имеет вид $\mathcal{F} = (\mathcal{A} \vee \mathcal{B})$ или аналогичный с конъюнкцией, импликацией или отрицанием в качестве последней связки. Тогда подформула $\mathcal{G}$ является также подформулой $\mathcal{A}$ или $\mathcal{B}$. Для определённости можно считать, что $\mathcal{G}$ - подформула $\mathcal{A}$. По предположению индукции можно считать, что $\mathcal{A} \equiv \mathcal{A}_1$, где A_1 получена из $\mathcal{A}$ заменой $\mathcal{G}$ на $\mathcal{H}$. При этом, конечно, $\mathcal{F}_1 = (\mathcal{A}_1 \vee \mathcal{B})$. Теперь для доказательства равносильности $\mathcal{F}$ и $\mathcal{F}_1$ достаточно сослаться на результат задачи 18 - монотонность дизъюнкции •

21. Решение. Легко проверить, что все аксиомы системы ИВ2 являются тождественно истинными. Поэтому все доказуемые в ИВ2 формулы также являются тождественно истинными, что доказывается так же, как и для системы ИВ. Это значит, что все формулы, доказуемые в ИВ2, доказуемы и в исходной системе ИВ. Остаётся доказать обратное включение. Для этого достаточно доказать, что формула $\mathcal{A} \to (\mathcal{B} \to \mathcal{A} \wedge \mathcal{B})$, исключённая из списка аксиом, доказуема в системе ИВ2. Действительно, если выводимость из аксиом ИВ2 этой формулы будет доказана, то формулой можно будет пользоваться при построении любых выводов наряду с остальными аксиомами. Для доказательства указанной формулы сначала отметим, что в системе ИВ2 справедлива теорема о дедукции, так как её доказательство, данное в пункте 7.1, использует только две первые аксиомы, одинаковые для

систем ИВ и ИВ2. Установим для ИВ2 следующее отношение выводимости: $A,\ B \vdash A \wedge B$. В системе ИВ2 не доказаны теорема о десяти правилах и лемма о противоположной теореме, и потому строим вывод по определению.

1. A	; условие 1
2. B	; условие 2
3. $B \to (A \to B)$	; аксиома 1
4. $A \to B$	; MP 2, 3
5. $A \to A$	; см. п. 6.4, док-во сохраняется и для ИВ2
6. $(A \to A) \to ((A \to B) \to (A \to A \wedge B))$	; частный случай новой аксиомы 3
7. $(A \to B) \to (A \to A \wedge B)$	; MP 5, 6
8. $A \to A \wedge B$	; MP 4, 7
9. $A \wedge B$	; MP 1, 8

Теперь к полученному отношению выводимости дважды применяем теорему о дедукции и получаем, что в ИВ2 доказуема формула $A \to (B \to A \wedge B)$, что, как отмечалось, достаточно для решения задачи •

22. Решение. Рассуждая так же, как в предыдущей задаче, получаем, что достаточно доказать в системе ИВ3 исключённую аксиому:

$$(A \to B) \to ((A \to \neg B) \to \neg A).$$

Для ИВ3 справедлива теорема о дедукции, $\neg\neg X \equiv X$ и верна лемма о противоположной теореме (л. п. т.).

Действительно, теорема о дедукции доказывается одинаково для ИВ и для ИВ3, равносильность X и двойного отрицания X следует из аксиомы удаления отрицания и второй новой аксиомы, л. п. т. легко следует из теоремы о дедукции и первой введённой аксиомы.

Имея эти инструменты, докажем в ИВ3 следующее отношение выводимости:

$$A \to B,\ A \to \neg B \vdash \neg B.$$

1. $A,\ A \to \neg B \vdash \neg B$	; MP
2. $A,\ \neg\neg B \vdash \neg(A \to \neg B)$	; л. п. т. 1
3. $A,\ B \vdash \neg(A \to \neg B)$	; снятие двойного отрицания 2
4. $A,\ A \to B \vdash \neg(A \to \neg B)$	; MP и т. транзитивности
5. $A \to B,\ \neg\neg(A \to \neg B) \vdash \neg A$	; л. п. т. 4
6. $A \to B,\ A \to \neg B \vdash \neg A$	; снятие двойного отрицания 5

Теперь, дважды применив теорему о дедукции к полученному отношению, получаем, что в ИВ3 доказуема аксиома, исключённая из списка •

23. Указание. Как и в предыдущих двух задачах, достаточно доказать, что исключённые аксиомы доказуемы в ИВ4. Для этого достаточно доказать, что исключённая аксиома введения конъюнкции доказуема в ИВ4. Это доказывается точно так же, как в задаче 21. После этого можно утверждать, что все аксиомы ИВ3 доказуемы в системе ИВ4, а это значит, что все тождественно истинные формулы доказуемы в системе ИВ4 •

24. Решение. Для доказательства независимости аксиомы удаления отрицания применим ту же идею - идею инварианта, что и для доказательства непротиворечивости ИВ. Сопоставим каждой логической связке некоторую булеву функцию. Тогда и каждой формуле исчисления будет соответствовать некоторая функция. Сопоставление построим так, чтобы все аксиомы, кроме последней, были тождественно истинны, и чтобы формула, выводимая из тождественно истинных формул, также была тождественно истинна. При этом ясно, что последняя аксиома, не будучи тождественно истинной, не может быть выведена из остальных (тождественно истинных) аксиом.

Сопоставим всем логическим связкам, кроме отрицания, их стандартные булевы функции. Отрицанию сопоставим тождественную единицу, то есть считаем, что отрицание 0 есть 1 и отрицание 1 есть 1. Ясно, что все аксиомы, кроме двух последних, будут при этом тождественно истинными, так как они не содержат отрицания. Аксиома 9 - введение отрицания - тоже, как легко проверить, тождественно истинна, а последняя аксиома - нет •

25. Указание. Доказательсто независимости каждой из указанных аксиом проводится по той же схеме, как в предыдущей задаче. Все логические связки, кроме одной, определяются как в булевой алгебре, одна связка определяется по-другому. Дадим таблицу, в первом столбце которой указана аксиома, независимость которой доказывается, во втором - определяется исключительная связка, в третьем столбце указаны значения переменных, при которых проверяемая аксиома принимает значение 0:

Аксиома	Искл. операция	Знач. переменных
$A \wedge B \to A$	$A \wedge B = B$	$A = 0,\ B = 1$
$A \wedge B \to B$	$A \wedge B = A$	$A = 1,\ B = 0$
$A \to (B \to A \wedge B)$	$A \wedge B$	$A = 1, B = 1$
$A \to A \vee B$	$A \vee B = B$	$A = 1,\ B = 0$
$B \to A \vee B$	$A \vee B = A$	$A = 0,\ B = 1$
$(A \to C) \to$ $((B \to C) \to (A \vee B \to C))$	$A \vee B = 1$	$A = 0, B = 0$ $C = 0$
$(A \to B) \to ((A \to \overline{B}) \to \overline{A})$	$\overline{A} = 0$	$A = 0,\ B = 1$
$\overline{\overline{A}} \to A$	$\overline{A} = 1$	$A = 0$

Замечание. Две первые аксиомы также независимы, однако при доказательстве их независимости каждой логической связке сопоставляется функция, принимающая четыре значения, а не только 0 и 1. Отметим, что для решения задач 30 и 31 также требуется сопоставлять логическим связкам функции, принимающие больше двух значений •

26. Указание. Проверить, что доказательство теоремы о дедукции, имеющееся для ИВ, сохраняется и для ИИВ.

В доказательсто используются только две первые аксиомы, совпадающие для формальных теорий ИВ и ИИВ •

27. Указание. Доказательсто леммы о транзитивности импликации, имеющееся в п. 6.4., без изменений сохраняется для ИИВ •

28. Решение. С учетом справедливости для ИИВ теоремы о дедукции (задача 26), достаточно доказать в ИИВ следующее отношение выводимости:

$A \vdash \neg\neg A.$

Излагаем требуемый вывод:

1. A	; условие
2. $A \to (\neg A \to A)$	; аксиома ИИВ - введение импликации
3. $\neg A \to A$	;
4. $\neg A \to \neg A$	; MP 1, 2
5. $(\neg A \to A) \to ((\neg A \to \neg A) \to \neg\neg A)$	; аксиома ИИВ - введение отрицания
6. $(\neg A \to \neg A) \to \neg\neg A$	; MP 3, 5
7. $\neg\neg A$	; MP 4, 6 •

29. Решение. С учётом справедливости для ИИВ теоремы о дедукции (задача 26), достаточно доказать в ИИВ следующее отношение выводимости: $A \to B,\ \neg B \vdash \neg A$. Строим вывод:

1. $A \to B$; условие 1
2. $\neg B$; условие 2
3. $\neg B \to (A \to \neg B)$; аксиома ИИВ
4. $A \to \neg B$; МР 2, 3
5. $(A \to B) \to ((A \to \neg B) \to \neg A)$; аксиома ИИВ
6. $(A \to \neg B) \to \neg A$; МР 1, 5
7. $\neg A$; МР 4, 6 •

Замечание. Приведённый вывод не использовал новую аксиому ИИВ, поэтому он является выводом и в ИВ.

30. Решение. Сопоставим, как отмечалось выше, каждой логической связке функцию, принимающую три значения - 0, 1, 2:

X	Y	$X \wedge Y$	$X \vee Y$	$X \to Y$
0	0	0	0	2
0	1	0	1	2
0	2	0	2	2
1	0	0	1	0
1	1	1	1	2
1	2	1	2	2
2	0	0	2	0
2	1	1	2	1
2	2	2	2	2

Для отрицания считаем, что отрицание нуля есть два, а отрицание единицы и двух равны нулю. Теперь и любой формуле ИИВ можно сопоставить функцию, принимающую **три** значения. Просто проверить, что все аксиомы ИИВ тождественно равны двум, а формула $\neg\neg A \to A$ при $A = 1$ равна 1. Кроме того, также легко увидеть из приведённой таблицы, что из двух формул, равных двум, по правилу вывода МР также получится формула, равная двум. Другими словами, сохранение двойки наследуется при выводе из аксиом •

Замечания. В задаче попутно дано другое доказательство независимости последней аксиомы ИВ, то есть другое решение задачи 24, так как здесь доказано, что десятая аксиома не выводится не только из девяти остальных, но даже из девяти и ещё одной новой.

Из указанной таблицы следует также внутренняя непротиворечивость ИИВ. Свойством внутренней полноты ИИВ не обладает, что также следует из результата задачи.

31. Указание. Полностью используется решение предыдущей задачи •

32. Указание. Перебор.

33. Решение. Например:

$$\exists x(A(x)\wedge\neg B(x))\wedge\exists x(B(x)\wedge\neg A(x))\to\forall y(A(y)\vee B(y))\ \bullet$$

Конечно, имеется бесконечное множество 2-общезначимых формул.

Булевы функции

1. Решение. Как отмечалось в т. 1 гл. 12, каждой функции от n переменных можно сопоставить 0-1-вектор значений длины 2^n. Функциям, указанным в задаче, сопоставляются при этом векторы, симметричные относительно середины, так как противоположные наборы значений симметричны относительно середины таблицы. Это означает, что такие функции определяются своими значениями на первой половине таблицы, и им поэтому может быть сопоставлен 0-1-вектор значений длины 2^{n-1}. Указанное соответствие является биекцией, и потому количество функций, рассматриваемых в задаче, равно $2^{2^{n-1}}$ •

2. Решение. Докажем, что функций, указанных в задаче, не более двух. Действительно, легко доказать по

индукции, что все $0-1$-векторы можно расположить по окружности так, что рядом стоящие векторы смежны. Пусть теперь имеется функция, удовлетворяющая условиям задачи. Рассмотрим значение функции на некотором фиксированном наборе значений, например на нулевом. Имеется всего две возможности для значения функции в нуле - 0 или 1. В любом случае при движении по окружности от нулевого набора однозначно определяются значения функции на всех других векторах, если использовать условие перемены значения функции при переходе к смежному вектору. Таким образом, ясно, что функций, указанных в задаче, не более двух. Две функции можно всегда построить:

$$x_1 \oplus x_2 \oplus \ldots \oplus x_n,$$

$$x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1 \bullet$$

3. Указание. Подсчитать количество функций от n переменных, равных тождественно единице, количество функций, равных единице везде, кроме одного набора значений переменных, и так далее - до $m-k$, где $m=2^n$. Общее количество функций будет равно сумме подсчитанных величин. Количество функций, равных единице везде, кроме l наборов, равно (фактически по определению) числу сочетаний из m по l: C_m^l. Таким образом, общее количество функций равно сумме: $C_m^0 + C_m^1 + \ldots + C_m^{m-k}$, где $m = 2^n$ $\bullet$

4. Решения, ответы. Лего проверить, что $f = x \vee y = ((x \downarrow y) \downarrow (x \downarrow y))$, то есть f реализуется формулой глубины 2. Формулы глубины 0 - только переменные (констант в данном случае нет), формулы глубины 1 - формулы вида $f = (u \downarrow v)$, где u и v – произвольные различные

или совпадающие переменные. Ясно, что эти формулы не определяют дизъюнкцию. Аналогично проверяется, что

$$f = x \oplus y = ((x \downarrow y) \downarrow ((x \downarrow x) \downarrow (y \downarrow y)))$$

- формула минимальной глубины 3, реализующая сумму.

Минимальная реализация конъюнкции - $f = x \cdot y = ((x \downarrow x) \downarrow (y \downarrow y))$. Аналогично решаются вопросы реализации указанных функций через штрих Шеффера $\bullet$

5. Ответы, указания. Легко проверить, что $x \to y = \overline{x \cdot \overline{y}}$ - формула глубины 3, то есть на первый вопрос задачи ответ положителен. Заметим, что это формула минимальной глубины, представляющая импликацию.

На второй вопрос ответ отрицательный - тройная сумма не представляется формулой глубины 2 над указанной системой C. Для доказательства этого можно перебрать все виды формул глубины 2 над указанной системой C. Действительно, обозначив для единообразия $x \to y = f(x,y), x \cdot y = g(x,y)$ функции из C, можно выписать возможные формулы (с точностью до переименования переменных):

$$f(f(x,y),z),\ f(x,f(y,z)),\ f(f(x,y),f(z,t)),\ f(f(x,y),g(z,t)),$$

$$f(g(x,y),z),\ f(x,g(y,z)),\ f(g(x,y),g(z,t)),\ f(g(x,y),f(z,t)).$$

Здесь выписаны все формулы, в которых последней применяется функция f. Совершенно аналогичные формулы можно построить, поменяв ролями f и g. Всего 16 видов формул. Для представления функции от трёх переменных необходимо, чтобы из четырёх номинальных переменных x, y, z, t только три были различны. Далее можно проверить, что ни одна из представленных формул не может реализовать сумму $x \oplus y \oplus z$. Для уменьшения перебора можно использовать частные свойства суммы, например то, что при отождествлении любых двух переменных сумма вырождается в тождественную функцию, что сразу исключает из рассмотрения основную часть формул •

6. Ответ. Нет, не обязательно •

7. Решение. Если все формулы над C реализуют только константы, то утверждение справедливо. Пусть над C реализована функция $f(x_1, x_2, \cdots, x_n) \neq const$. Отождествим все переменные функции f и получим таким образом формулу и функцию $g(x)$ от одного переменного. Возможны только четыре случая: $g(x) \equiv x$, $g(x) = \bar{x}$, $g(x) \equiv 0$, $g(x) \equiv 1$. В первых двух случаях получена формула, задающая тожественную функцию x положительной глубины. Используя её для подстановки вместо переменных в имеющиеся формулы, будем получать для любой реализуемой функции новые представления с большей глубиной, чем любое заданное число. Пусть теперь $g(x) \equiv 0$. Так как $f(x_1, x_2, \cdots, x_n) \neq const$, существует набор 0-1-значений $(c_1, c_2, \dots c_n)$, на котором $f = 1$. В формуле, представляющей f, заменим все x_k, соответствующие $c_k = 1$ на x, остальные x_k на $0 = g(x)$. Получим новую формулу и функцию $\tilde{g}(x) \equiv x$, и все сводится к предыдущему случаю. Для последнего из четырёх - случая $g(x) \equiv 1$ - аналогичными построениями получаем функцию $\tilde{g}(x) \equiv \bar{x}$, а значит, и функцию x •

8. Ответ. Если k нечётно, таких многочленов нет. Если k чётно, то $C^k_{2^n-1}$ •

9. Указание. Максимальная длина многочлена от n переменных равна 2^n. Этим замечанием искомая функция определяется однозначно •

10. Указание. Индукция по n и учет того, что общее

количество функций от k переменных есть 2^{2^k} •

11. Решение. Если переменная x_i явно входит в многочлен $f(x_1, x_2, \dots x_n)$, то сгруппируем отдельно все одночлены, содержащие x_i, и в другую сумму - все остальные. Множитель x_i в первой сумме можно вынести за скобку. Получим следующее представление: $f = x_i \cdot g \oplus h$. По построению, g и h - многочлены от оставшихся переменных $x_1, \dots x_{i-1}, x_{i+1}, \dots, x_n$. При этом $g \neq 0$. Тогда, в силу нетривиальности g, существует определённый набор значений переменных $\tilde{c} = (c_1, c_2, \dots c_{i-1}, c_{i+1}, \dots, c_n)$, на котором $g(\tilde{c}) = 1$. Тогда

$$f(c_1, c_2, \dots, c_{i-1}, x_i, c_{i+1}, \dots, x_n) = x_i \oplus h(\tilde{c})$$

Из данного представления ясно, что значения многочлена f на наборах

$$(c_1, \dots, c_{i-1}, 0, c_{i+1}, \dots, x_n), (c_1, \dots, c_{i-1}, 1, c_{i+1}, \dots, x_n)$$

будут противоположны, и, значит, переменная x_i существенна •

13. Указание. По определению самодвойственности ясно, что такая функция определяется своими значениями на первой половине таблицы. Это значит, что общее количество самодвойственных функций равно $2^4 = 16$. При этом среди этих шестнадцати функций шесть будут иметь фиктивные переменные. Это будут функции $x, \bar{x}$, y, $\bar{y}$, z, $\bar{z}$. Остальные 10 следующие:

$$x^a \cdot y^b \vee y^b \cdot z^c \vee z^c \cdot x^a,\ a, b, c \in \{0, 1\}$$

- всего восемь функций. Здесь, как обычно, принято обозначение: $x^1 = x$ и $x^0 = \bar{x}$. Имеются еще две суммы:

$$x \oplus y \oplus z, 1 \oplus x \oplus y \oplus z$$

Отметим, что самодвойственных функций, существенно зависящих от двух переменных, нет, как получается из этого рассмотрения •

14. Ответ. Десять функций, указанных в предыдущей задаче •

15. Указание. Как уже отмечено выше, самодвойственная функция определяется своими значениями на первой половине таблицы. В первых 2^{n-1} строках таблицы функция может принимать произвольные значения, а в оставшихся противоположных строках значения определяются из условия самодвойственности. Поэтому общее количество таких функций - $2^{2^{n-1}}$. Среди них есть функции, имеющие фиктивные переменные. Как легко понять, если функция самодвойственна, то после удаления фиктивной переменной она останется самодвойственной. Фиктивной переменной может быть любая переменная от x_1 до x_n. Поэтому из указанного числа $2^{2^{n-1}}$ надо вычесть $n2^{2^{n-2}}$. При этом надо учесть, что мы вычли больше, чем нужно, так как среди того, что вычли, содержатся функции от $n-2$ существенных переменных. То, что вычли лишнее, надо добавить: $C_n^2 \cdot 2^{2^{n-2}}$. Полученный результат снова необходимо откорректировать и так далее. Короче говоря, работает принцип включений-исключений, и в результате выводится формула:

$$\sum_{k=0}^{n-1} (-1)^k C_n^k 2^{2^{n-k-1}} \bullet$$

16. Решение. Пусть задана некоторая функция $f(\tilde{x})$ от n переменных $\tilde{x} = (x_1, x_2, \ldots, x_n)$ и все они существенные. Докажем, что если f не является самодвойственной, то с помощью отождествления переменных можно полу-

чить функцию, зависящую ровно от двух существенных переменных. Так как f несамодвойственна, существуют два противоположных набора $\tilde{c} = (c_1, c_2, \ldots, c_n)$ и $\bar{\tilde{c}} = (\bar{c}_1, \bar{c}_2, \ldots, \bar{c}_n)$ таких, что $f(\tilde{c}) = f(\bar{\tilde{c}})$. Первый случай: $f(\tilde{0}) \neq f(\tilde{1})$. Тогда $\tilde{c} \neq \tilde{0}$ и $\tilde{c} \neq \tilde{1}$. Определим функцию $g(x, y)$, получаемую из f в результате замены на x всех x_k таких, что $c_k = 0$, и на y остальных переменных. Тогда, в нашем случае, получим: $g(0, 0) \neq g(1, 1)$, а по выбору $\tilde{c}$ - $g(0, 1) = g(1, 0)$ Ясно, что всякая функция g с такими свойствами существенно зависит от двух переменных.

Рассмотрим второй случай: $f(\tilde{0}) = f(\tilde{1})$. $f \neq const$, в силу неравенства $n \geq 3$, и потому существует такой набор $\tilde{a} = (a_1, a_2, \ldots, a_n)$, что $f(\tilde{a}) \neq f(\tilde{0})$. Определим функцию $h(x, y)$ с помощью набора $\tilde{a}$ аналогично первому случаю. Получим соотношения: $h(0, 0) = h(1, 1)$ и $h(0, 1) \neq h(0, 0)$. Всякая функция h с такими свойствами существенно зависит от двух переменных •

17. Указание. Подсчитать значение f на наборе, противоположном $\tilde{x}$, используя соотношение: $\bar{x} = 1 \oplus x$. Ответ: 2^n•

18. Решение. Если функция $f(x_1, x_2, \ldots, x_n)$ существенно зависит от всех n переменных и линейна, то это одна из следующих двух функций:

$x_1 \oplus x_2 \oplus \ldots \oplus x_n$,

$x_1 \oplus x_2 \oplus \ldots \oplus x_n \oplus 1$,

построенных в задаче 2. Действительно, очевидно, что если какая-то переменная x_k не входит явно в сумму, то она не может быть существенной. Также ясно, что обе эти функции удовлетворяют условию задачи о замещении переменных константами. Это значит, что необходимость условия доказана. Докажем достаточность от противного. Пусть функция существенно зависит от всех n переменных и удовлетворяет условию замещения. Предположим, что f не линейная. Тогда, как следует из задачи 2, существуют два смежных набора $\tilde{a} = (a_1, a_2, \ldots, a_n)$ и $\tilde{b} = (b_1, b_2, \ldots, b_n)$ таких, что $f(\tilde{a}) = f(\tilde{b})$. Пусть x_k - единственная компонента, в которой различаются наборы $\tilde{a}$ и $\tilde{b}$. Тогда $f(a_1, a_2, \ldots, a_{k-1}, x_k, a_{k+1}, \ldots, a_n)$ фиктивно зависит от x_k, что противоречит условию. Значит, f - линейная, то есть одна из двух указанных выше сумм •

19. Решение. Пусть $f(\tilde{x})$ - многочлен степени $k \geq 3$. Пусть одночлен наивысшей степени $s = x_1 \cdot x_2 \cdot \ldots \cdot x_k$ явно содержится в записи f. Положив $x_k = x_{k+1} = \ldots = x_n$, получим многочлен g от k переменных, в котором s - единственный одночлен степени k, так как степень всех других одночленов понизится в силу совпадения переменных. Рассмотрим одночлены g степени $k-1$. Возможны три случая: все k одночленов входят в состав g; входят все, кроме одного; отсутствуют хотя бы два одночлена.

В первом случае положим $x_k = x_{k-1}$. Степень s понизится, s преобразуется в $s_0 = x_1 \cdot x_2 \cdot \ldots \cdot x_{k-1}$. Еще ровно два одночлена степени $k-1$ из состава g преобразуются в s_0 - это одночлены степени $k-1$, в которых отсутствовали множители x_k и x_{k-1} соответственно. Остальные одночлены степени $k-1$ понизятся в степени. В результате получится многочлен степени $k-1$.

Второй случай. Пусть отсутствует одночлен $x_1 \cdot x_2 \cdot \ldots \cdot x_{k-1}$. Положим $x_1 = x_2$. Снова, как и в первом случае, получится ровно три одночлена степени $k-1$ и получится многочлен соответствующей степени.

Третий случай. Пусть отсутствуют два одночлена: $x_2 \cdot \ldots \cdot x_k$ и $x_1 \cdot x_3 \cdot \ldots \cdot x_k$, не содержащие x_1 и x_2 соответственно. Положим $x_1 = x_2$. Тогда s преобразуется в одночлен $x_1 \cdot x_3 \cdot \ldots \cdot x_k$, остальные понизятся в степени. Снова получается многочлен степени $k-1$ •

24. Указание. Проверить, что для всякой монотонной функции $f(x_1, x_2, \ldots, x_n)$ справедливы следующие разложения:

$$f(x_1, x_2, \ldots, x_n) = x_1 \cdot f(1, x_2, \ldots, x_n) \vee f(0, x_2, \ldots, x_n)$$

$$f(x_1, x_2, \ldots, x_n) = (x_1 \vee f(0, x_2, \ldots, x_n)) \cdot f(1, x_2, \ldots, x_n).$$

Аналогичные разложения справедливы и для остальных переменных. Отметим, что функции f_1 и f_0, указанные в разложении, зависят от меньшего, чем n, числа переменных и тоже монотонны •

25. Указание. Использовать результаты задачи 24 •

26. Решение. Всякий базис в M содержит обе константы. Действительно, все монотонные функции, кроме констант, на единичном наборе равны 1, а на нулевом - 0, и потому не могут образовывать полной в M системы. Кроме того, в любом базисе должна быть функция не менее чем от двух существенных переменных, так как функции одного переменного образуют замкнутый класс, не совпадающий с M. Значит, любой базис состоит не менее чем из трёх функций. Пусть, с другой стороны, B - базис в M, содержащий не менее пяти функций. Тогда, кроме двух констант, B содержит не меньше трёх функций, существенно зависящих хотя бы от одного переменного. Более того, функции от одного переменного (x и $\bar{x}$) не могут входить в базис M. Значит, в B содержатся три функции, зависящие не менее чем от двух переменных. Тогда

среди этих трёх функций имеется хотя бы одна, не являющаяся э.к., и одна, не являющаяся э.д. Действительно, с помощью подстановок констант в любую монотонную э.к. можно получить просто бинарную конъюнкцию: $x \vee y$. Значит, в базисе две э.к. не требуются. Двойственное утверждение для э.д. Таким образом, достаточно не более двух функций исходного базиса, кроме констант, для получения бинарной дизъюнкции и конъюнкции. Согласно предыдущей задаче, они уже образуют базис. Тогда, в силу неприводимости базиса, получаем утверждение, требуемое в задаче •

Список литературы

[1] Александров, П. С. Введение в теорию множеств и общую топологию
/ П. С. Александров. – М.: Наука, 1977.

[2] Клини, С. К. Математическая логика
/ С.К. Клини. – М.: Мир, 1973.

[3] Новиков, П. С. Элементы математической логики
/ П. С. Новиков. – М.: Наука, 1973.

[4] Лавров, И. А. Задачи по теории множеств, математической логике и теории алгоритмов
/ И. А. Лавров, Л. Л. Максимова. – М.: Наука, 1975.

[5] Хао Ван, Аксиоматические системы теории множеств
/ Ван Хао, Р. Мак-Нотон. – М.: ИЛ, 1963.

[6] Мендельсон, Э. Введение в математическую логику
/ Э. Мендельсон. – М.: Наука, 1971.

[7] Новиков, Ф. А. Дискретная математика для программистов
/ Ф. А. Новиков. – СПб.: Питер, 2000.

[8] Нефёдов, В. Н. Курс дискретной математики.
/ В. Н. Нефёдов, В. А. Осипова М.: Изд-во МАИ, 1992.

[9] Бардачев Ю. Н., Основы дискретной математики
/ Ю. Н. Бардачев, Н. А. Соколова, В. Е. Ходаков. – Херсон: Изд-во ХГТУ, 2000.

[10] Яблонский, С. В. Введение в дискретную математику
/ С. В. Яблонский. – М.: Наука, 1986.

[11] Акимов, О. Е. Дискретная математика. Логика, группы, графы

/ О. Е. Акимов – М.: Лаборатория Базовых Знаний, 2001.

[12] Кузнецов О. П. Дискретная математика для инженера

/ О. П. Кузнецов, Г. М. Адельсон-Вельский. – М.: Энергия, 1980.

Учебное издание

Белова Лариса Юрьевна
Белов Юрий Анатольевич

Элементы теории множеств
и математической логики
Теория и задачи

Учебное пособие

Редактор, корректор М. В. Никулина
Компьютерная верстка Ю. А. Белов

Подписано в печать 18.12.2012 г. Формат 60×84 1/16
Бумага тип. Усл. печ. л. 11,85, Уч.-изд. л. 8,0
Тираж 40 экз. Заказ

Оригинал-макет подготовлен редакционно-издательским отделом
Ярославского государственного университета им. П.Г. Демидова
Отпечатано на ризографе.
Ярославский государственный университет им. П. Г. Демидова
150000 Ярославль, ул. Советская, 14