Содержание

Предисловие

Философская логика есть наука о законах и формах отражения в мышлении развития объективного мира, о закономерностях познания истины.

Основная задача философской логики есть формулировка законов и принципов, соблюдение которых является необходимым условием получения истинных умозаключений.

Формальная логика есть наука, изучающая формы мысли (понятия, суждения, умозаключения, доказательства) со стороны их логической структуры, то есть отвлекаясь от конкретного содержания мыслей и вычленяя лишь общий способ связи частей этого содержания.

Начало формальной логики положил Аристотель.

Математическая логика есть область знания, в которой формальная логика изучается математическими методами.

Основные задачи математической логики есть: 1) построение формально-логических (аксиоматических) исчислений; 2) изучение связи логических исчислений с теми содержательными областями знаний, которые служат их интерпретациями и моделями.

Одно из крупнейших достижений математики первой половины XX века – оформление математической логики и теории алгоритмов в самостоятельные дисциплины. Три крупных результата определили характер всех последующих исследований этого направления: теорема Геделя о полноте аксиоматического исчисления предикатов относительно всех тождественно истинных формул такого исчисления (полнота относительно интерпретации); существование алгоритмически неразрешимых проблем, в частности теорема Черча об алгоритмической неразрешимости исчисления предикатов; теорема Геделя о неполноте аксиоматической арифметики относительно множества ее истинных формул.

Уже в древности предпринимались попытки строго изложить математические факты, которые стремились вывести из немногочисленных исходных посылок – аксиом. Замечательным примером такого подхода к изложению математических сведений были «Начала» древнегреческого математика Евклида, в особенности его геометрия. Изучались и законы правильного вывода следствий из исходных посылок (логика Аристотеля).

Первые попытки создать строгие математические теории восходят к работам Буля, Фреге, Пеано, других математиков. Исследователи руководствовались целью заложить такие основания математики, выделить такие аксиомы и правила вывода, с помощью которых можно было бы формально доказать любое содержательно истинное математическое утверждение. Подобные утверждения можно было бы доказывать автоматически. Эта связываемая с именем Гильберта программа в полной мере не удалась: австрийский мате-

матик Курт Гедель показал, что всякая достаточно богатая формальная система (например, аксиоматическая арифметика) не полна, т. е. в ней найдутся содержательно истинные утверждения, недоказуемые в системе. Пессимист угрюмо заметил бы: «Я же говорил вам, что из этой затеи Гильберта ничего хорошего не выйдет. Пойду наколю себе дров. Хотя я хорошо знаю заранее, что из этой моей затеи тоже ничего не выйдет». Оптимист скажет другое: «Мы надеялись на чудо. Его не произошло. Всевышний не дает нам того, чего мы очень хотим. Зато мы узнали много интересного, нам открылись огромные просторы для деятельности. О, сколько задач у нас впереди! За дело, коллеги!»

Аксиоматическая арифметика не полна. Тем не менее интерес к математической логике не убывает, исследования формально-логических систем продолжаются. Успешно описываются довольно большие фрагменты математических дисциплин. Использование алгебраического языка при проектировании узлов компьютера общеизвестно. В последнее время аппарат математической логики стал широко применяться в современных системах представления знаний.

Самое удивительное применение математическая логика нашла в вычислительной математике: формализм логического вывода в логике предикатов первого порядка был взят за основу при построении универсального языка программирования Пролог (акроним от PROgramming in LOGic). С появлением Пролог-подобных языков программирования математическая логика, которая совсем недавно была логикой сугубо теоретической, стала логикой вычисляющей. Классическая гильбертова логика доказательств истинных формул логики предикатов первого порядка для этой практической цели оказалась неподходящей. В 1965 г. Дж. А. Робинсон в качестве формализма, удобного для исполнения на компьютере, предложил использовать разработанный им метод резолюций. Замечательное открытие Робинсона оказалось необычайно плодотворным и уже в 70-х годах привело к построению универсального языка программирования Пролог и трансляторов для него. Это списковый язык для теоретико-множественных вычислений. Иногда его называют языком искусственного интеллекта. Задуманный как универсальный язык программирования для перевода с одного естественного языка на другой, Пролог оказался удобным инструментом при построении вычислительных моделей, возникающих при решении задач на графах, проектировании конечных автоматов, построении баз данных, баз знаний, экспертных систем, в задачах лингвистики при работе с естественными и искусственными языками (причем в числе последних могут выступать и языки программирования), в символьных преобразованиях, теории игр, системах представления знаний и т. д.

Несколько необычным в Прологе может показаться отсутствие привычного в традиционных языках программирования оператора присваивания. Вместо него в Прологе реализован более общий алгоритм унификации, построенный на основе операции сравнения с образцом. Необычен в Прологе также и отсутствующий в традиционных языках бэктрекинг, позволяющий обходить де-

рево вывода и собирать все возможные решения задачи. Реализация рекурсии в Прологе практически не отличается от общепринятой. В остальном Пролог довольно удобен, особенно в задачах, где основными обрабатываемыми объектами являются символ и список символов (множество).

Существует несколько версий трансляторов с Пролога: MicroProlog, DEC-System/Prolog, C-Prolog, IC-Prolog, M-Prolog, Sigma-Prolog, Chalcedony-Prolog, FF-Prolog, UNSW/Prolog, Prolog-6, Prolog-1 и Prolog-2 фирмы Expert Systems International, Quintus-Pro log, Turbo-Prolog, Arity-Prolog, SWI-Prolog, Visual-Prolog и другие. При написании программ мы ориентировались на версию языка SWI-Prolog (http://www.swi-prolog.org/).

Другое интересное направление применения математической логики есть разработка языков формальных спецификаций преобразований в алгебраических объектах и в анализе работы компьютерных программ.

Современный арсенал языков и инструментов, использующихся в данной области, известен как формальные методы разработки программ. Классическими методами и нотациями здесь являются VDM и Z. Если говорить о формальных моделях, то наиболее популярными являются Alloy, B и TLA. Среди средств моделирования и анализа программ на обычных языках программирования лидерами являются Isabelle (http://isabelle.in.tum.de/) и Frama-C (http://frama-c.com/jessie.html).

Для спецификаций преобразований в аксиоматически заданных алгебраических объектах, таких как полугруппы, группы, кольца, поля, линейные пространства и т. д., разработан функциональный язык программирования OBJ3. Сравнивая, например, OBJ3-программу для вычислений в полях, можно увидеть, что OBJ3-программа есть запись аксиом поля в терминах языка OBJ3. Вычисление преобразований в поле осуществляется в соответствии с аксиомами поля. OBJ3-программа моделирует эти преобразования. Иногда OBJ3 называют аксиоматическим языком программирования. Аксиоматический подход в языках программирования значительно облегчает задачу верификации программ. Предложенные в аксиоматических языках программирования подходы могут использоваться при создании других языков. Например, развитая в OBJ3 модульная система программ внедрена в языках программирования Ada, ML, C++, LOTOS (Language Of Temporal Oredering Specification). Параметризация из OBJ3 имплементирована в C#. Для решения аналогичных задач алгебраических спецификаций можно использовать родственный к OBJ3 язык программирования CafeOBJ из семейства OBJ (https://cafeobj.org/).

Книга написана по материалам лекций авторов по дисциплинам «Дискретная математика» и «Математическая логика и теория алгоритмов», читаемых на факультете бизнес-информатики, на факультете компьютерных наук Национального исследовательского университета Высшая школа экономики и на факультете автоматики и вычислительной техники Национального исследовательского университета Московский энергетический институт. Эти курсы (или им аналогичные) начинали в МЭИ Д. А. Поспелов, В. Н. Вагин, В. П. Кутепов,

А. А. Болотов, А. Б. Фролов, Е. А. Щегольков, повлиявшие на выбор и характер излагаемого авторами материала.

Настоящая книга является второй в серии задуманных авторским коллективом книг по дискретной математике. Она предназначается студентам бакалавриата, изучающим академический курс «Дискретная математика».

В предлагаемой книге авторы сосредоточились на изложении основ математической логики и связанных с ней формальных языков, представимых конечными автоматами.

Основные теоретические и практические положения, изложение и анализ практических алгоритмов, иллюстрируемых большим числом примеров, позволят сформировать прочную теоретическую базу, необходимую для дальнейшей работы практикующих программистов и ИТ-специалистов.

В приложении предлагаются задачи, которые могут быть использованы как для проведения практических занятий, так и для самостоятельной работы.

Авторы выражают глубокую благодарность рецензентам Калягину В. А., Петренко А. К. и научному редактору книги Захарову В. А. за замечания, позволяющие существенно улучшить качество книги. Мы также благодарны преподавателям департамента программной инженерии НИУ ВШЭ Ахметсафиной Р. З., Бересневой Е. Н., Горденко М. К., Гринкругу Е. М., Дворянскому Л. В., Дегтяреву К. Ю., Каленковой А. А., Ломазовой И. А., Подбельскому В. В., Шилову В. В., а также Амосову А. А., Вагину В. Н., Дубинскому Ю. А., Куликовой Н. Л., Фролову А. Б. из НИУ МЭИ за стимулирующие беседы. Авторы благодарят студентов Сапожкова Е. Д., Тимофееву Е. Э., Чичилеву Н. И. за активное участие в составлении и апробации задач и упражнений приложения. Авторы благодарны также корректору Синяевой Г. И. за внимательное прочтение рукописи и устранение ошибок.

Введение

1. Множество

Понятие множества неопределимо. Это простейшее исходное понятие человечество сформировало из опыта всего своего исторического развития. То же можно сказать о смысле простейшего отношения принадлежности: элемент a принадлежит множеству A (обозначение $a \in A$) – и о смысле отношения тождества (совпадения, равенства) двух элементов a и b из некоторого множества (обозначение $a = b$). Другими словами, предполагается, что читатель умеет распознавать совпадение или несовпадение двух элементов и устанавливать факт принадлежности или непринадлежности элемента множеству.

Пусть U есть некоторое множество. A есть подмножество множества U, если всякий элемент из множества A принадлежит множеству U. Множество U универсально (универсум), если все рассматриваемые множества есть подмножества множества U.

Пусть A, B, C есть произвольные подмножества множества U; a, b, c есть элементы множества U. Обозначим символом $\varnothing$ пустое множество, то есть множество без элементов.

Основными неопределяемыми отношениями в теории множеств являются следующие отношения:

- $a = b$, элементы a и b равны (совпадают);
- $a \in A$, элемент a принадлежит множеству A.

Пусть знак $\leftrightarrow$ означает «если и только если»; а знаки $\&$, $\vee$, $\neg$, $\rightarrow$, $\forall$, $\exists$ есть логические знаки конъюнкции, дизъюнкции, отрицания, импликации, квантора общности и квантора существования. Используем их в общепринятом содержательном смысле. Знак $\exists!$ означает квантор существования единственного элемента.

Обозначим через $a \notin A$ отношение «элемент a не принадлежит множеству A» и через $a \neq b$ отношение «элементы a и b не равны (не совпадают)».

Введем далее следующие отношения.

- $A \subseteq B \leftrightarrow \forall a\ (a \in A \rightarrow a \in B)$, отношение включения множеств, при этом множество A называется подмножеством множества B, а множество B называется надмножеством множества A;
- $A \supseteq B \leftrightarrow B \subseteq A$;
- $A = B \leftrightarrow A \subseteq B \,\&\, A \supseteq B$, отношение равенства множеств;
- $A \subset B \leftrightarrow A \subseteq B \,\&\, A \neq B$, отношение строгого включения множеств;
- $A \supset B \leftrightarrow B \subset A$.

Обозначим через $P(A)$ (или 2^A) множество всех подмножеств множества A. Введем следующие операции над множествами.

- $A \cup B = \{x \in U : x \in A \vee x \in B\}$, объединение множеств A и B;
- $A \cap B = \{x \in U : x \in A \,\&\, x \in B\}$, пересечение множеств A и B;
- $A - B = \{x \in U : x \in A \,\&\, x \notin B\}$, разность множеств A и B;
- $\bar{A} = U - A$, дополнение ко множеству A;
- $A \div B = (A \cup B) - (A \cap B)$, симметрическая разность множеств A и B;
- $A \times B = \{(a, b) : a \in A \,\&\, b \in B\}$, декартово произведение множеств A и B.

Под натуральным числом понимаем количество элементов конечного множества. Количество элементов пустого множества есть 0.

Распространим декартово произведение на несколько сомножителей:

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

Определим декартову степень множества:

$A^n = A \times A \times \ldots \times A$ (n раз), $A^0 = \varnothing$.

Множества $\varnothing$ и A называются несобственными (тривиальными) подмножествами множества A. Если $A \subset B \,\&\, A \neq \varnothing$, то A есть собственное подмножество множества B.

Иногда пишут $A \cdot B$ или AB вместо $A \cap B$.

Примем следующие обозначения.

Множество натуральных чисел $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Множество положительных натуральных чисел $\mathbb{N}_+ = \{1, 2, \ldots\}$.

Множество целых чисел $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Множество $\mathbb{Z}_n = E_n = \{0, 1, 2, \ldots, n-1\}$.

Множество рациональных чисел $\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}_+\}$.

Множество вещественных чисел $\mathbb{R} = (-\infty, +\infty)$.

Множество неотрицательных вещественных чисел $\mathbb{R}_+ = [0, +\infty)$.

Множество комплексных чисел $\mathbb{C} = \{x + i\,y : x \in \mathbb{R}, y \in \mathbb{R}\}$, здесь $i^2 = -1$.

2. Функция

Определение. Пусть A и B есть два множества. *Функция* f: $A \to B$ есть отображение, которое каждому элементу x из A ставит в соответствие некоторый элемент y из B. Это обстоятельство записывается как $y = f(x)$.

Замечание. В этом определении функция f всюду определена. Частично определенная функция $f : A \to B$ есть отображение, которое каждому элементу из множества A сопоставляет не более одного элемента из множества B. Всюду определенная функция является частным случаем частично определенной функции.

Если $f(a) = b$, то элемент b есть образ элемента a, элемент a есть прообраз элемента b. Область определения функции f есть множество $D(f) = \{a \in A : \exists\, b \in B\ (f(a) = b)\}$. Область значений функции f есть множество $R(f) = \{b \in B : \exists a \in A\ (f(a) = b)\}$.

Иногда множество $R(f)$ обозначают как $Im(f)$ или $f(A)$. Полный прообраз элемента $b \in B$ есть множество $f^{-1}(b) = \{a \in A : f(a) = b\}$. Полный прообраз множества $C \subseteq B$ есть множество $f^{-1}(C) = \{a \in A : f(a) \in C\}$.

Сужение функции f, заданной на множестве A, на подмножество S множества A есть функция g – такая, что $\leftrightarrow a \in S\ (g(a) = f(a))$.

Расширение функции f, заданной на множестве A, на надмножество T множества A есть функция h – такая, что $\leftrightarrow a \in A\ (h(a) = f(a))$.

Функцию с конечной областью определения удобно задавать таблицей. Например, пусть множества $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 4, 5\}$, функция $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & & 1 & 2 \end{pmatrix}$. Здесь $f(1) = 3$, $f(2)$ не определено, $f(3) = 1$, $f(4) = 2$. Порядок столбцов несуществен.

Область определения $D(f) = \{1, 3, 4\}$, область значений $R(f) = Im(f) = f(A) = \{1, 2, 3\}$.

Определение. Функция φ: $A \to B$ есть *взаимно-однозначное отображение* (1-1-отображение) между множествами A и B, если

1) $\forall b \in B\ \exists a \in A\ (f(a)=b)$,

2) $\forall a \in A\ \forall b \in A\ (a \neq b \to f(a) \neq f(b))$.

Замечание. Последнее условие можно заменить на условие

2′) $\forall a \in A\ \forall b \in A\ (f(a) = f(b) \to a = b)$.

Функции f: $A \to B$ и g: $C \to D$ равны, если $A = C$, $B = D$, $\forall x \in A\ (f(x) = g(x))$.

Функция I_A: $A \to A$, для которой $\forall x \in A\ (I(x) = x)$, называется *тождественной* функцией.

Функция f: $A \to B$ есть отображение *в* (*инъективная функция*, или *инъекция*), если $\forall a \in A\ \forall b \in A$ условие $a \neq b$ влечет $f(a) \neq f(b)$.

Инъективная функция различные элементы из области определения переводит в различные элементы из области значений.

Функция $f : A \to B$ есть отображение *на* (*сюръективная функция*, или *сюръекция*), если область значений B совпадает с образом $f(A)$, то есть если $f(A) = B$.

Функция $f : A \to B$ есть *взаимно-однозначная функция* (или *биекция*), если f является отображением *в* и отображением *на*, то есть является одновременно инъективной и сюръективной функцией: 1) $a \neq b \to f(a) \neq f(b)$, 2) $Im(f) = B$.

Определение. *Композиция* $g \circ f$ функций f: $A \to B$ и g: $B \to C$ есть функция $g \circ f : A \to C$, для которой $\forall x \in A\ ((g \circ f)(x) = g(f(x)))$.

Замечание. Символ композиции $\circ$ иногда опускается.

Утверждение. $(h \circ g) \circ f = h \circ (g \circ f)$.

Доказательство. Пусть $f : A \to B$, $g : B \to C$, $h : C \to D$. Тогда $((h \circ g) \circ f)(x) = (hg)f(x) = (h \circ g)f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

Замечание. Для тождественной функции $f \circ I_A = I_B \circ f = f$.

Определение. Функция f^{-1}: $B \to A$ называется *обратной* к функции f: $A \to B$, если $f \circ f^{-1} = I_B$ и $f^{-1} \circ f = I_A$.

Замечание. 1. g обратна к $f \leftrightarrow f$ обратна к g.

2. Функция f: $A \to B$ имеет обратную функцию, $\leftrightarrow$ функция f есть взаимно-однозначное отображение.

Утверждение. Если обратная функция для функции f существует, то она единственна.

Доказательство. Пусть функции f^{-1} и g обратны к функции $f : A \to B$. Тогда $f^{-1} \circ I_B = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_A \circ g = g$.

Следствие. Пусть для функций f и g существуют обратные функции f^{-1} и g^{-1}. Тогда справедливы утверждения:

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

Доказательство. 1. Так как f^{-1} обратна к f, то f обратна к f^{-1}, то есть $f = (f^{-1})^{-1}$.

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

Аналогично $(g^{-1} \circ f^{-1}) \circ (f \circ g) = I_B$. Тогда функция $g^{-1} \circ f^{-1}$ обратна к $f \circ g$, то есть $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Теорема. Функция $f : A \to B$ имеет обратную функцию тогда и только тогда, когда отображение f взаимно-однозначно.

Доказательство. Пусть функция f имеет обратную функцию f^{-1}. Покажем, что отображение f взаимно-однозначно, то есть что $a \neq b \to f(a) \neq f(b)$ и $B = Im(f)$. В самом деле, пусть $f(a) = f(b)$. Тогда $a = I_A(a) = f^{-1}(f(a)) = f^{-1}(f(b)) = I_A(b) = b$, то есть $f(a) = f(b) \to a = b$, откуда $a \neq b \to f(a) \neq f(b)$.

Пусть $b \in B$. Тогда $b = I_B(b) = (f \circ f^{-1})(b) = f(f^{-1}(b))$, то есть всякий b есть образ некоторого $a = f^{-1}(b) \in A$. Поэтому $B = Im(f)$.

Пусть теперь f есть взаимно-однозначное отображение. Покажем, что функция f имеет обратную функцию. В самом деле, так как $B = Im(f)$, то каждый элемент b из B есть образ в точности одного элемента a из A: $f(a) = b$. Пусть $g(b) = a$. Для соответствия $g : B \to A$ имеем:

$$(g \circ f)(a) = g(f(a)) = g(b) = a = I_A,$$
$$(f \circ g)(b) = f(g(b)) = f(a) = b = I_B.$$

Следовательно, g есть обратная функция для f. Теорема доказана.

3. Унарная функция

Напомним, что функция $f : A \to B$ есть правило (отображение), которое каждому элементу из множества A сопоставляет единственный элемент из множества B. Если $f(a) = b$, то элемент b есть образ элемента a, элемент a есть прообраз элемента b. Множество A есть область определения $D(f)$ функции f. Множество B есть область значений $V(f)$ функции f.

Образ $\mathrm{Im}\ f = \{f(x) : x \in A\}$ отображения $f : A \to B$ есть множество $f(A)$ всех значений функции f. *Полный прообраз элемента* $y \in B$ есть множество $f^{-1}(y) = \{x \in A : f(x) = y\}$. *Полный прообраз множества* $C \subseteq B$ есть множество $f^{-1}(C) = \{x \in A : f(x) \in C\}$.

На конечном множестве функцию удобно задавать таблицей. Например, пусть множества $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 4, 5\}$, функция $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 2 \end{pmatrix}$. Здесь

$f(1) = 3$, $f(2) = 2$, $f(3) = 1$, $f(4) = 2$. Порядок столбцов несуществен. Область определения $D(f) = A = \{1, 2, 3, 4\}$, область значений $V(f) = B = \{1, 2, 3, 4, 5\}$, $\mathrm{Im}\, f = f(A) = \{1, 2, 3\}$.

Функции $f : A \to B$ и $g : C \to D$ равны, если $A = C$, $B = D$, $\forall x \in A\ f(x) = g(x)$.

Функция $I_A : A \to A$, для которой $\forall x \in A\ I(x) = x$, называется *тождественной*.

Функция $f : A \to B$ есть *вложение* (*инъективная функция*, или *инъекция*), если $\forall a \in A\ \forall a' \in A$ условие $a \neq a'$ влечет $f(a) \neq f(a')$.

Инъективная функция различные элементы из области определения переводит в различные элементы из области значений.

Функция $f : A \to B$ есть отображение *на* (*сюръективная функция*, или *сюръекция*), если область значений B совпадает с образом $f(A)$, то есть если $f(A) = B$.

Функция $f : A \to B$ есть *взаимно-однозначная функция* (или *биекция*), если f является вложением и отображением *на*, то есть если 1) $a \neq a' \to f(a) \neq f(a')$, 2) $\mathrm{Im}\, f = B$.

Если $f : A \to B$ и $C \subset A$, то функция $f : C \to B$ называется *сужением* функции f на множество C и обозначается $f \mid C$. Функция f называется *расширением* функции $f \mid C$.

Композиция $g \circ f$ функций $f : A \to B$ и $g : B \to C$ есть функция $g \circ f : A \to C$, для которой $\forall x \in A\ (g \circ f)(x) = g(f(x))$.

Символ композиции $\circ$ иногда опускается.

Утверждение. $(h \circ g) \circ f = h \circ (g \circ f)$.

Доказательство. Пусть $f : A \to B$, $g : B \to C$, $h : C \to D$. Тогда $((h \circ g) \circ f)(x) = (hg)f)(x) = (h \circ g)f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

Замечание. Для тождественной функции $f \circ I_A = I_B \circ f = f$.

Определение. Функция $f : B \to A$ называется *обратной* к функции $f : A \to B$, если $f \circ f^{-1} = I_B$ и $f^{-1} \circ f = I_A$.

Замечание. g обратна к $f \leftrightarrow f$ обратна g.

Утверждение. Если обратная функция для функции f существует, то она единственна.

Доказательство. Пусть функции f^{-1} и g обратны к функции $f : A \to B$. Тогда $f^{-1} \circ I_B = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_A \circ g = g$.

Следствие. Пусть для функций f и g существуют обратные функции f^{-1} и g^{-1}. Тогда справедливы утверждения:

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

Доказательство.

1. Так как f^{-1} обратна к f, то f обратна к f^{-1}, то есть $f = (f^{-1})^{-1}$.
2. $(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ I_B \circ f^{-1} = f \circ f^{-1} = I_B$.

Аналогично $(g^{-1} \circ f^{-1}) \circ (f \circ g) = I_B$. Тогда функция $g^{-1} \circ f^{-1}$ обратна к $f \circ g$, то есть $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Теорема. Функция $f : A \to B$ имеет обратную функцию тогда и только тогда, когда отображение f взаимно-однозначно.

Доказательство. Пусть функция f имеет обратную функцию f^{-1}. Покажем, что отображение f взаимно-однозначно, то есть что $a \neq a' \to f(a) \neq f(a')$ и $B = \mathrm{Im}\, f$.

В самом деле, пусть $f(a) = f(a')$. Тогда $a = I_A(a) = f^{-1}(f(a)) = f^{-1}(f(a')) = I_A(a') = a'$, то есть $f(a) = f(a') \to a = a'$, откуда $a \neq a' \to f(a) \neq f(a')$.

Пусть $b \in B$. Тогда $b = I_B(b) = (f \circ f^{-1})(b) = f(f^{-1}(b))$, то есть всякий b есть образ некоторого $a = f^{-1}(b) \in A$. Поэтому $B = \mathrm{Im}\, f$.

Пусть теперь f есть взаимно-однозначное отображение. Покажем, что функция f имеет обратную функцию. В самом деле, так как $B = \mathrm{Im}\, f$, то каждый элемент b из B есть образ в точности одного элемента a из A: $f(a) = b$. Пусть $g(b) = a$. Для соответствия $g : B \to A$ имеем:

$$(g \circ f)(a) = g(f(a)) = g(b) = a = I_A,$$
$$(f \circ g)(b) = f(g(b)) = f(a) = b = I_B.$$

Следовательно, g есть обратная функция для f. Теорема доказана.

4. Отношение

Пусть $A_1, A_2, \ldots, A_n$ есть произвольные множества, вообще говоря, разнородные.

Определение. *n-арное отношение* p^n на множествах $A_1, A_2, \ldots, A_n$ есть подмножество p^n декартова произведения $A_1 \times A_2 \times \ldots \times A_n$.

Замечание. n-арное отношение p^n на множестве A есть подмножество p^n натуральной степени множества A^n, $n > 0$. Индекс n арности (местности) отношения p иногда опускается.

Возможна множественная (суффиксная) $(x_1, \ldots, x_n) \in \rho$ и предикатная (префиксная) $\rho(x_1, \ldots, x_n)$ формы записи отношений. В последнем случае отношение ρ называют также предикатом. Для бинарного отношения используется инфиксная запись $x \rho y$. Унарное отношение $\rho \subseteq E$ есть подмножество множества E. Предикат $\rho(x)$, соответствующий унарному отношению, называется свойством.

Набор $a = (a_1, a_2, \ldots, a_n) \in \rho$ (допустима запись $\rho(a_1, a_2, \ldots, a_n)$) называется элементом отношения.

Определение. Отношение *конечно*, если оно состоит из конечного числа элементов.

5. Отношение эквивалентности

Пусть A есть произвольное множество.

Определение. Бинарное отношение $\sigma \subseteq A \times A$ есть *отношение эквивалентности* (обозначение $a \sim b$), если оно удовлетворяет следующим аксиомам:

1) $a \sim a$, рефлексивность;
2) $a \sim b \to b \sim a$, симметричность;
3) $a \sim b \;\&\; b \sim c \to a \sim c$, транзитивность.

Обозначение. $a \sim b$, $\sigma(a, b)$, $(a, b) \in \sigma$, $a \sigma b$.

Определение. *Разбиение I множества A* есть семейство попарно непересекающихся непустых подмножеств множества A, таких, что: $A = \bigcup_{i \in I} A_i$, $\forall i \neq j$ $(A_i \bigcap A_j = \varnothing)$. Подмножества A_i называются *смежными классами* разбиения I.

Пример. $A = \{0, 1, 2, 3, 4, 5\} = \{0, 1, 5\} \cup \{2\} \cup \{3, 4\}$.

Теорема. 1. Каждому отношению эквивалентности, определенному на множестве A, соответствует некоторое разбиение множества A.

2. Каждому разбиению множества A соответствует некоторое отношение эквивалентности, определенное на множестве A.

Коротко: между классом всех определенных на множестве A эквивалентностей и классом всех разбиений множества A существует взаимно-однозначное соответствие.

Доказательство. 1. Пусть σ есть отношение эквивалентности, определенное на множестве A и $a \in A$. Построим множество $K_a = \{x \in A : x \sim a\}$ всех элементов x, эквивалентных a. Оно обозначается также через $[a]_\sigma$. Множества K_a называются *смежными классами A по* σ, или классами эквивалентности.

Заметим, что если $b \in K_a$, то $b \sim a$. Покажем, что $a \sim b \leftrightarrow K_a = K_b$. В самом деле, пусть $a \sim b$. Пусть произвольный элемент $c \in K_a$. Тогда $c \sim a$, $a \sim b$, $c \sim b$, $c \in K_b$, и потому $K_a \subseteq K_b$. Аналогично показываем, что $K_b \subseteq K_a$. Тогда $K_a = K_b$. Пусть теперь $K_a = K_b$. Тогда $a \in K_b$, и $a \sim b$. Утверждение доказано.

Если два класса K_a и K_b имеют общий элемент c, то они совпадают. В самом деле, если $c \in K_a$, $c \in K_b$, то $b \sim c$, $c \sim a$ и $b \sim a$, откуда $K_a = K_b$. Поэтому всякие два класса эквивалентности либо не пересекаются, либо (в случае непустого пересечения) совпадают. Всякий элемент c попадает в класс эквивалентности K_c. Поэтому система смежных классов есть разбиение множества A.

2. Пусть задано некоторое разбиение множества A. Определим на A отношение $\sim$, положив $a \sim b \leftrightarrow$ элементы a и b принадлежат одному и тому же классу разбиения. Отношение $\sim$ удовлетворяет аксиомам 1) $a \sim a$, 2) $a \sim b \to b \sim a$, 3) $a \sim b \ \& \ b \sim c$, и потому оно есть отношение эквивалентности.

Замечание. 1. Разбиение множества A на одноэлементные подмножества $A = \bigcup_{a \in A} \{a\}$ и разбиение A, состоящее из одного только множества A, называются тривиальными (несобственными) разбиениями.

2. Разбиение A на одноэлементные подмножества соответствует отношению эквивалентности, которое есть равенство.

3. Разбиение множества A, состоящее из одного только множества A, соответствует отношению эквивалентности, содержащему все множество $A \times A$.

4. $a \sigma b \leftrightarrow [a]_\sigma = [b]_\sigma$.

Определение. Совокупность классов эквивалентности множества A называется *фактор-множеством* A/σ множества A по эквивалентности σ.

Определение. Отображение $p : A \to A/\sigma$, при котором $p(a) = [a]_\sigma$, называется *каноническим* (естественным).

6. Каноническое разложение функции

Пусть $f : A \to B$ есть некоторая функция. Определим на A отношение $\sigma \in A \times A$, положив $\forall a \in A \ \forall b \in A \ (a \sim b \leftrightarrow f(a) = f(b))$. Отношение σ есть отношение эквивалентности, так как выполняются следующие свойства:

1) $a \sim a$, ибо $f(a) = f(a)$;
2) $a \sim b \to b \sim a$, ибо $f(a) = f(b) \to f(b) = f(a)$;
3) $a \sim b$ & $b \sim c \to a \sim c$, ибо $f(a) = f(b)$ & $f(b) = f(c) \to f(a) = f(c)$.

Введенное отношение σ называется ядерной эквивалентностью для отображения f. Классы эквивалентности A/σ есть полные прообразы элементов множества B при отображении f, то есть $A_b = f^{-1}(b)$.

Отображение f можно разложить в композицию двух отображений согласно следующему рисунку:

Имеет место равенство $f = q \circ p$, то есть $f(a) = q(p(a))$.

Представление $f = q \circ p$ называется каноническим разложением (представлением) функции f.

Пример. Получить каноническое разложение функции

$$f : E_{10} \to E_{10},\ f = 0112105533 = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 0\,1\,1\,2\,1\,0\,5\,5\,3\,3 \end{pmatrix}.$$

Область определения $D(f) = E_{10}$. Область значений $Im(f) = \{0, 1, 2, 3, 5\}$. Классы эквивалентности:

$K_0 = [0]_\sigma = f^{-1}(0) = \{0, 5\}$, $q(K_0) = 0$,
$K_1 = [1]_\sigma = f^{-1}(1) = \{1, 2, 4\}$, $q(K_1) = 1$,
$K_2 = [2]_\sigma = f^{-1}(2) = \{3\}$, $q(K_2) = 2$,
$K_3 = [3]_\sigma = f^{-1}(3) = \{8, 9\}$, $q(K_3) = 3$,
$K_5 = [5]_\sigma = f^{-1}(5) = \{6, 7\}$, $q(K_5) = 5$.

Функции p и q задаются следующим образом:

$$p(a) = K_{f(a)} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ K_0 & K_1 & K_2 & K_3 & K_4 & K_5 & K_6 & K_7 & K_8 & K_9 \end{pmatrix},$$

$$D(p) = E_{10},\ Im(p) = \{K_0, K_1, K_2, K_3, K_5\};\ q(K_a) = a = \begin{pmatrix} K_0 & K_1 & K_2 & K_3 & K_5 \\ 0 & 1 & 2 & 3 & 5 \end{pmatrix},$$

$D(q) = \{K_0, K_1, K_2, K_3, K_5\}$, $Im(q) = \{0, 1, 2, 3, 5\}$; $f(a) = q(p(a))$.

7. Мощность множества. Счетные и несчетные множества

Определение. *Множества A и B эквивалентны* ($A \sim B$), если между их элементами можно установить взаимно-однозначное соответствие. □

Отношение эквивалентности множеств обладает следующими свойствами.

1. $A \sim A$, рефлексивность.
2. $A \sim B \to B \sim A$, симметричность.
3. $A \sim B \,\&\, B \sim C \to A \sim C$, транзитивность.

Определение. *Мощность множества A* (обозначение $|A|$) есть класс эквивалентных ему множеств. *Мощность конечного множества* есть число его элементов.

Замечание. Эквивалентные множества A и B равномощны, то есть $A \sim B \leftrightarrow |A| = |B|$.

Определение. Множество A *счетно*, если A эквивалентно множеству $\mathbb{N}$ натуральных чисел. В противном случае множество A *несчетно*.

Утверждение. Из всякого бесконечного множества можно выделить счетное подмножество.

Доказательство. Пусть A есть бесконечное множество. Выделим в A произвольный элемент a_0. Множество $A - \{a_0\}$ бесконечно. Выделим в нем элемент a_1. Множество $A - \{a_0, a_1\}$ бесконечно. Выделим в нем элемент a_2. И так далее. В бесконечном множестве A выделено счетное подмножество $B = \{a_0, a_1, a_2, \ldots\}$.

Утверждение. Множество $\mathbb{Q}_+$ положительных рациональных чисел счетно.

Доказательство. Расположим элементы из $\mathbb{Q}_+$ в следующей таблице.

1, 1/2, 1/3, 1/4, 1/5, ...
2, 2/2, 2/3, 2/4, 2/5, ...
3, 3/2, 3/3, 3/4, 3/5, ...
4, 4/2, 4/3, 4/4, 4/5, ...
...

Выписываем элементы из $\mathbb{Q}_+$ по диагонали, сверху вниз, выпуская ранее встречавшиеся числа: 1, 1/2, 2, 1/3, 3, 2/3, ... Следовательно, множество $\mathbb{Q}_+$ счетно.

Утверждение. Объединение конечного или счетного множества счетных множеств счетно.

Доказательство. Расположим элементы множеств $A_1, A_2, A_3, \ldots$ (их число может быть и конечным) в следующей таблице.

$A_1 : a_{11}, a_{12}, a_{13}, a_{14}, \ldots$
$A_2 : a_{21}, a_{22}, a_{23}, a_{24}, \ldots$
$A_3 : a_{31}, a_{32}, a_{33}, a_{34}, \ldots$
$A_4 : a_{41}, a_{42}, a_{43}, a_{44}, \ldots$
...

Выписываем элементы из $A_1 \cup A_2 \cup A_3 \cup \ldots$ по диагонали, сверху вниз, выпуская ранее встречавшиеся элементы: $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \ldots$ Следовательно, множество $A_1 \cup A_2 \cup \ldots$ счетно.

Замечание. Объединение конечного множества и счетного множества счетно. Множество рациональных чисел счетно, ибо $\mathbb{Q} = \mathbb{Q}_- \cup \mathbb{Q}_+ \cup \{0\}$, где $\mathbb{Q}_-$ есть множество отрицательных рациональных чисел.

8. Мощность континуума

Утверждение. Множество C всех бесконечных последовательностей из 0 и 1 несчетно.

Доказательство. Допустим противное: существует пересчет всех бесконечных последовательностей $A_1, A_2, A_3, \ldots$ из 0 и 1:

$A_1 : a_{11}, a_{12}, a_{13}, a_{14}, \ldots$
$A_2 : a_{21}, a_{22}, a_{23}, a_{24}, \ldots$
$A_3 : a_{31}, a_{32}, a_{33}, a_{34}, \ldots$
$A_4 : a_{41}, a_{42}, a_{43}, a_{44}, \ldots$
$\ldots$

Построим последовательность $B : b_1, b_2, b_3, \ldots$, где

$$b_i = \begin{cases} 1, \text{ если } a_{ii} = 0, \\ 0, \text{ если } a_{ii} = 1, \end{cases} \quad i = 1, 2, 3, \ldots$$

Последовательность B лежит вне указанного пересчета. B отличается от A_1 элементом $b_1 \neq a_{11}$, от A_2 – элементом $b_2 \neq a_{22}$, от A_3 – элементом $b_3 \neq a_{33}$ и т. д. Следовательно, исходное множество C несчетно.

Определение. Множество A имеет *мощность континуума c*, если A эквивалентно множеству всех бесконечных последовательностей из 0 и 1.

Следствие. Множество C всех бесконечных последовательностей из 0 и 1 имеет мощность континуума: $|C| = c$ (в силу рефлексивности).

Утверждение. Множество $P(\mathbb{N})$ всех подмножеств множества натуральных чисел имеет мощность континуума.

Доказательство. Всякую бесконечную последовательность из 0 и 1 можно рассматривать как характеристическую функцию некоторого подмножества множества натуральных чисел. Следовательно, множество $P(\mathbb{N})$ имеет мощность континуума: $|P(\mathbb{N})| = \mathrm{c}$.

Следствие. Множество всех подмножеств множества натуральных чисел несчетно.

Утверждение. Если к бесконечному множеству добавить конечное или счетное множество элементов, то его мощность не изменится.

Доказательство. Пусть A есть бесконечное множество, а B есть конечное или счетное множество, причем $A \cap B = \varnothing$. Покажем, что $A \sim A \cup B$. Выделим из множества A счетное подмножество A_1. Тогда $A = C \cup A_1$, где $C = A - A_1$, и $A \cup B = (C \cup A_1) \cup B = \mathrm{C} \cup (A_1 \cup B)$. Так как $A_1 \cup B \sim A_1$, то $A \cup B = C \cup (A_1 \cup B)$, $C \cup (A_1 \cup B) \sim C \cup A_1$ в силу транзитивности, и с учетом того, что $A = C \cup A_1$, получаем $A \cup B \sim A$.

Утверждение. Если A есть несчетное множество, а B есть конечное или счетное его подмножество, то $A - B \sim A$.

Доказательство. Пусть $C = A - B$. Тогда $A = C \cup B$. Множество C несчетно, ибо в противном случае C конечно или счетно, и тогда $A = C \cup B$ конечно или счетно. Множество $C \cup B \sim C$, или $A \sim C$, то есть $A \sim A - B$.

Теорема. Множество $U = [0, 1]$ имеет мощность континуума c.

Доказательство. Множество U эквивалентно множеству всех последовательностей из 0 и 1.

Замечание. 1. $|[0,1]| = |(0,1)| = |(0,1]| = |[0,1)| = c$.

2. Если $a < b$, то $|[a, b]| = c$, ибо функция $y = a + x(b - a)$ отображает $[0, 1]$ на $[a, b]$ взаимно-однозначно.

3. $|[a, b]| = |(a, b)| = |(a, b]| = |[a, b)| = c$.

4. $|(-\infty, \infty)| = |\mathbb{R}| = c$, ибо функция $y = \operatorname{tg}(x)$ отображает интервал $(a, b) = (-\pi/2, \pi/2)$ на всю числовую ось $\mathbb{R}$ взаимно-однозначно.

9. Кардинальные числа. Сравнение мощностей

Определение. *Мощность множества* есть класс эквивалентных между собой множеств. *Кардинальное число*, или кардинал, есть знак (символ), приписываемый мощности как классу эквивалентных между собой множеств. Мощности конечных множеств называются *финитными кардиналами*. Мощности бесконечных множеств называются *трансфинитными кардиналами*.

Пример. Счетной мощности (мощность множества натуральных чисел) присваивается кардинальное число $\aleph_0$ (алеф-нуль). Мощности множества вещественных чисел присваивается кардинальное число c.

Замечание. Мощность множества A обозначается через $|A|$, а также через $card(A)$ или $c(A)$. Мощность конечного множества есть число его элементов.

Пусть A, B есть произвольные множества и $|A|$, $|B|$ есть их мощности.

Априори возможны четыре случая.

1. Множество A эквивалентно некоторому подмножеству множества B, а множество B эквивалентно некоторому подмножеству множества A.

2. Множество A эквивалентно некоторому подмножеству множества B, а множество B не эквивалентно никакому подмножеству множества A.

3. Множество B эквивалентно некоторому подмножеству множества A, а множество A не эквивалентно никакому подмножеству множества B.

4. Множество A не эквивалентно никакому подмножеству множества B, а множество B не эквивалентно никакому подмножеству множества A.

Определение.

$|A| = |B|$, если $A \sim B$.

$|A| \leqslant |B|$, если A эквивалентно некоторому подмножеству в B.

$|A| < |B|$, если A эквивалентно некоторому подмножеству в B, а множество B не эквивалентно никакому подмножеству множества A.

$|A| \geqslant |B|$, если $|B| \leqslant |A|$.

$|A| > |B|$, если $|B| < |A|$.

Замечание. Случай, когда множество A не эквивалентно никакому подмножеству множества B, а множество B не эквивалентно никакому подмножеству множества A, невозможен.

Теорема (Кантор–Бернштейн). Если множество A эквивалентно некоторому подмножеству B_1 множества B, а множество B эквивалентно некоторому под-

множеству A_1 множества A, то множества A и B эквивалентны (то есть имеют равную мощность). Коротко: $|A| \leqslant |B|$ & $|B| \leqslant |A| \to |A| = |B|$.

Доказательство. Случаи $B_1 = B$ и $A_1 = A$ можно исключить, ибо если $B_1 = B$, то условие теоремы утверждает, что $A \sim B$, из чего, естественно, следует $A \sim B$. Случай $A_1 = A$ аналогичен.

Итак, пусть $A_1 \subset A$, $B_1 \subset B$. Пусть функции $f : A \to B_1$, $g : B \to A_1$ устанавливают взаимно-однозначное соответствие между A и B_1 и между B и A_1, то есть $A \leftrightarrow_f B_1$, $B \leftrightarrow_g A_1$. С помощью функций f и g расслоим множества A и B на «кольца» следующим образом. Имеем:

$A \leftrightarrow_f B_1 \subset B, B \leftrightarrow_g A_1 \subset A,$
$A_1 \leftrightarrow_f B_2 \subset B_1, B_1 \leftrightarrow_g A_2 \subset A_1,$
$A_2 \leftrightarrow_f B_3 \subset B_2, B_2 \leftrightarrow_g A_3 \subset A_2,$
…

Сформируем множества («кольца»):

$K_0^A = A - A_1, K_0^B = B - B_1,$
$K_1^A = A_1 - A_2, K_1^B = B_1 - B_2,$
$K_2^A = A_2 - A_3, K_2^B = B_2 - B_3,$
…

Функции f и g устанавливают следующие взаимно-однозначные соответствия:

$K_0^A \leftrightarrow_f K_1^B, K_0^B \leftrightarrow_g K_1^A,$
$K_2^A \leftrightarrow_f K_3^B, K_2^B \leftrightarrow_g K_3^A,$
…

Пусть множества $C = \bigcap_{i=1}^{\infty} A_i$, $D = \bigcap_{i=1}^{\infty} B_i$. Функции f и g устанавливают взаимно-однозначные соответствия между C и D. Если бы это было не так, то возникли бы аналогичные кольца в C и D, что по построению C и D невозможно.

Пусть множества

$$A_{\text{чет}} = \bigcap_{i=1}^{\infty} K_{2i}^A = K_0^A \cup K_2^A \cup K_4^A \cup \ldots$$

$$A_{\text{неч}} = \bigcap_{i=1}^{\infty} K_{2i+1}^A = K_1^A \cup K_3^A \cup K_5^A \cup \ldots$$

Аналогично построим множества $B_{\text{чет}}$, $B_{\text{неч}}$. Тогда

$A = A_{\text{чет}} \cup A_{\text{неч}} \cup C, B = B_{\text{чет}} \cup B_{\text{неч}} \cup D.$

Функция f устанавливает взаимно-однозначные соответствия:

$A_{\text{чет}} \leftrightarrow_f B_{\text{неч}}, A_{\text{неч}} \leftrightarrow_g B_{\text{чет}}, C \leftrightarrow_{f \text{ или } g} D.$

Тогда функция $h : A \to B$, определенная как

$$h(x) = \begin{cases} f(x), \text{ если } x \in A_{\text{чет}} \cup C \\ g(x), \text{ если } x \in A_{\text{неч}} \end{cases},$$

устанавливает взаимно-однозначное соответствие между A и B. Следовательно, $|A| = |B|$. Теорема доказана.

Следствие. Если $A \subseteq B$, то $|A| \leqslant |B|$.

Кардинальные числа можно сравнивать по величине.

Пусть A есть некоторое множество и $P(A)$ есть множество всех подмножеств множества A. Очевидно, что $|A| \leqslant |P(A)|$, ибо взаимно-однозначное соответствие между A и частью $P(A)$ устанавливается, если каждому элементу a из A сопоставить одноэлементное множество $\{a\}$ из $P(A)$.

Теорема (Кантор). $|A| < |P(A)|$.

Доказательство. Покажем, что $|A| \neq |P(A)|$. Допустим противное: $|A| = |P(A)|$ для некоторого множества A. Тогда существует взаимно-однозначное соответствие $f : A \to P(A)$ между множествами A и $P(A)$. Пусть

$$A_1 = \{a \in A : a \in f(a)\}, A_2 = \{a \in A : a \notin f(a)\}.$$

Тогда $A_2 = A - A_1$. Множество $A_2 \in P(A)$. Пусть в нашем соответствии $f(b) = A_2$ для некоторого b из A. Каждый элемент из A попадает либо в A_1, либо в A_2. Если $b \in A_1$, то по построению A_1 будет $b \in f(b)$ и $f(b) = A_2$. Противоречие, ибо $b \in A_1$ и $b \in A_2$, что одновременно невозможно. Если $b \in A_2$, то по построению A_2 будет $b \notin f(b)$ и $f(b) = A_2$. Противоречие, ибо $b \in A_2$ и $b \notin A_2$, что одновременно невозможно. Следовательно, наше предположение о равенстве $|A|$ и $|P(A)|$ не верно. Остается взять $|A| \neq |P(A)|$, а так как $|A| \leqslant |P(A)|$, то $|A| < |P(A)|$. Теорема доказана.

Иногда множество $P(A)$ всех подмножеств множества A обозначается через 2^A, а мощность $P(A)$ через $2^{|A|}$. Тогда по теореме $|A| < 2^{|A|}$.

Отправляясь от произвольного множества A, по теореме Кантора можно построить возрастающую последовательность кардинальных чисел:

$$|A| < 2^{|A|} < 2^{2^{|A|}} < \ldots$$

Отправляясь от счетного множества $\mathbb{N}$ натуральных чисел, можно построить возрастающую последовательность кардиналов:

$$\aleph_0 < 2^{\aleph_0} = c = \aleph_1 < 2^{\aleph_1} = \aleph_2 < 2^{\aleph_2} = \aleph_3 < \ldots$$

Мощности $\aleph_0$, $\aleph_1 = c$, $\aleph_2 = 2^c$, $\aleph_3 = 2^{2^c}$, ... – это счетная мощность, континуум, гиперконтинуум, гипергиперконтинуум и т. д.

Кантор поставил проблему о существовании промежуточной мощности между $\aleph_0$ и $\aleph_1$ (континуум-гипотеза) и промежуточных мощностей между всякими $\aleph_i$ и $\aleph_{i+1}$ (обобщенная континуум-гипотеза). В работах К. Геделя и П. Коэна было установлено, что обе гипотезы не противоречат аксиоматической теории множеств (существует модель, в которой истинны аксиомы теории множеств, континуум-гипотеза, причем правила вывода сохраняют истинность выводи-

мых формул) и не могут быть в ней доказаны (существует модель, в которой истинны аксиомы теории множеств и ложна континуум-гипотеза, причем правила вывода сохраняют истинность выводимых формул, а потому континуум-гипотеза не может быть доказана в теории множеств). Отсюда следует, что обе гипотезы независимы в аксиоматической теории множеств.

Часть I

АЛГЕБРА ЛОГИКИ И ПРЕДИКАТЫ

В результате освоения учебного материала данной части студент должен:

- знать основные понятия и методы математической логики; функции алгебры логики; логику предикатов; формально-аксиоматические системы для логики высказываний и логики предикатов; теоремы Геделя о формальном выводе; принципы построения логических языков программирования на основе формализма метода резолюций и аксиоматических языков программирования; методику работы с математической литературой и методику самостоятельного изучения новых логических аксиоматических систем;
- уметь анализировать и представлять функции алгебры логики в нормальных дизъюнктивных и конъюнктивных нормальных формах; анализировать формулы логики предикатов на предмет их общезначимости, выполнимости, опровержимости, невыполнимости; анализировать правила вывода формул логики высказываний и логики предикатов и проверять их правильность; программировать на одной из версий языка программирования Пролог и на одной из версий аксиоматического языка программирования; применять свои знания к решению практических задач;
- иметь навыки минимизации функции алгебры логики в классе нормальных форм; навыки анализа данной системы функций алгебры логики на функциональную полноту; навыки упрощения формул логики предикатов; навыки математического описания явлений и процессов, используя элементы математической логики; навыки расширения своих знаний в применении математической логики при разработке алгоритмов решения прикладных задач программной инженерии.

Глава 1

Алгебра логики

1.1. Функции алгебры логики

Пусть $E_2 = \{0, 1\}$ есть двухэлементное множество. Набор длины n из 0 и 1 есть последовательность длины n, составленная из 0 и 1.

Пример. (0); (1) есть наборы длины 1;

(0,0); (0,1); (1,0); (1,1) есть наборы длины 2;

(0,0,0); (0,0,1); (0,1,0); (0,1,1); (1,0,0); (1,0,1); (1,1,0); (1,1,1) есть наборы длины 3;

(0,0,...,0,0); (0,0,...,1); ...; $(a_1,a_2,...,a_n)$; ...; (1,1,...,1,1) есть наборы длины n.

Пусть E_2^n есть множество всех наборов длины n из 0 и 1.

Теорема. Число $h(n)$ всех наборов длины n из 0 и 1 равно 2^n.

Доказательство. Индукция по n.

Базис. $n = 1$. $h(1) = 2$.

Предположение индукции. Пусть $h(n) = 2$.

Шаг индукции. Покажем, что $h(n + 1) = 2^{n+1}$. Разобьем все наборы длины $n + 1$ на два класса: класс наборов, начинающихся с 0, и класс наборов, начинающихся с 1.

0,0,...,0,0	1,0,...,0,0
0,0,...,0,1	1,0,...,0,1
0,0,...,1,0	1,0,...,1,0
...	...
0,1,...,1,1	1,1,...,1,1

Число всех наборов длины $n + 1$, начинающихся с 0 (так же как и число всех наборов, начинающихся с 1), равно числу всех наборов длины n и по предположению индукции равно 2^n. Тогда $h(n+1) = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$. Теорема доказана.

Определение. Функция алгебры логики есть функция, аргументы и значения которой принимают лишь два значения: 0 и 1.

Класс всех функций алгебры логики обозначим через P_2. Вместо слов «функция алгебры логики» будем иногда говорить просто «функция».

Теорема. Число всех n-местных функций алгебры логики равно 2^{2^n}.

Доказательство. В табл. 1.1 перечислены все n-местные функции.

Таблица 1.1

x_1	x_2	…	x_{n-1}	x_n	f_0	f_1	f_2	…	f_r
0	0	…	0	0	0	0	0	…	1
0	0	…	0	1	0	0	0		1
		…						…	
1	1	…	1	0	0	0	1		1
1	1	…	1	1	0	1	0		1

Число всех строк равно 2^n, т. е. равно числу всех наборов длины n из 0 и 1. Число всех функций алгебры логики от n переменных равно 2^{2^n}, т. е. равно числу всех наборов длины 2^n из 0 и 1.

Теорема доказана.

В табл. 1.2 приведены некоторые часто используемые в практике функции:

- 0, константа нуль;
- 1, константа единица;
- $\underline{x} \equiv 1$, тождественная функция;
- $\bar{x}$, отрицание;
- $x \vee y$, дизъюнкция;
- x & y, конъюнкция (обозначается также через $x \cdot y$ или xy);
- $x \to y$, импликация;
- $x + y$, сложение (по модулю два);
- $x \equiv y$, эквивалентность (равносильность);
- $x \mid y$, штрих Шеффера;
- $x \uparrow y$, стрелка Пирса.

Таблица 1.2

x	y	0	1	$x \vee y$	x & y	$x \to y$	$x + y$	$x \equiv y$	$x \mid y$	$x \uparrow y$	x	$\bar{x}$	$f(x) = x$	0	1
0	0	0	1	0	0	1	0	1	1	1	0	1	0	0	1
0	1	0	1	1	0	1	1	0	1	0	1	0	1	0	1
1	0	0	1	1	0	0	1	0	1	9					
1	1	0	1	1	1	1	0	1	0	0					

1.2. Формулы. Реализация функций формулами

Пусть F = $\{f_1^{n_1}, f_2^{n_2}, \ldots\}$ есть множество функциональных символов указанной вверху местности и $\{x_1, x_2, \ldots\}$ есть множество символов переменных. Верхние индексы $n_1, n_2, \ldots$ могут опускаться, если их значение предполагается известным.

Пусть F есть некоторое подмножество функций из P_2.

Определение. Формула (алгебры логики) над F определяется индуктивно следующим образом.

1. Символ переменной есть формула над F.

2. Если f есть функциональный символ арности m из F и $x_1, \ldots, x_m$ есть символы различных переменных, то выражение $f(x_1, \ldots, x_m)$ есть формула над F и $\{x_1, \ldots, x_m\}$ есть множество ее переменных.

3. Если $A(x_1, \ldots, x_m)$ есть формула над F, где $\{x_1, \ldots, x_m\}$ есть множество ее переменных, и если каждое из выражений $A_1, \ldots, A_m$ есть либо формула над F, либо символ переменной, то выражение $A(A_1, \ldots, A_m)$ есть формула над F, причем множество ее переменных есть объединение множеств переменных формул $A_1, \ldots, A_m$.

Примеры. $F = \{f_1(x,y), f_2(x,y,z), f_3(x)\}$. Следующие выражения являются формулами над F.

$f_1(x,y)$; $f_2(x,y,z)$; $f_3(x)$; $f_1(t,z)$; $f_2(t,t,t)$; $f_3(f_2(x,y,x))$; $f_1(f_2(y,t,z), f_3(f_1(x,x)))$.

Сопоставим каждому функциональному символу f^n из F некоторую функцию $f : E_2^n \to E_2$. Если множество функциональных символов $F = \{f_1^{n_1}, f_2^{n_2}, \ldots\}$, то обозначим множество соответствующих функций $F = \{f_1^{n_1}, f_2^{n_2}, \ldots\}$. Между F и F существует взаимно-однозначное соответствие, при котором $f_i^{n_i}$ соответствует $f_i^{n_i}$, $i = 1, 2, \ldots$

Каждой формуле над F сопоставим функцию следующим образом.

1. Переменной x сопоставим тождественную функцию x.

2. Формуле $f(x_1, \ldots, x_m)$ над F сопоставим функцию $f(x_1, \ldots, x_m)$ из F.

3. Если формуле $A(x_1, \ldots, x_m)$ над F сопоставлена функция $f(x_1, \ldots, x_m)$, а формулам $A_1, \ldots, A_m$ над F сопоставлены функции $f_1, \ldots, f_m$, то формуле $A(A_1, \ldots, A_m)$ над F сопоставим функцию $f(f_1, \ldots, f_m)$ из P_2.

Таким образом, каждая формула над F реализует некоторую функцию из P_2. Пусть формула $A(x_1, \ldots, x_n)$ реализует некоторую функцию $f(x_1, \ldots, x_n)$, и пусть $a = (a_1, \ldots, a_n)$ есть набор длины n из 0 и 1. Тогда значение формулы A на наборе a есть $f(a)$, т. е. $A(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$.

В дальнейшем формулу $A(x_1, \ldots, x_m)$ будем отождествлять с функцией $f(x_1, \ldots, x_n)$, которую формула A реализует, и обозначать эту функцию через $A(x_1, \ldots, x_m)$. Говоря о формуле A над F, будем говорить просто о формуле A, не упоминая об F, если из контекста ясно, о каком множестве F идет речь.

Имея в виду взаимно-однозначное соответствие между F и F, вместо слов «формула $A(x_1, \ldots, x_m)$ над множеством функциональных символов F» будем говорить «формула $A(x_1, \ldots, x_m)$ над множеством функций F».

Пример. Формула $\overline{xy} \vee \overline{x}$ реализует функцию $f(x,y)$, приведенную в табл. 1.3.

Таблица 1.3

x	y	$f(x, y)$
0	0	0
0	1	0
1	0	1
1	1	0

Определение. Функция f есть суперпозиция над F, если f реализуется некоторой формулой над F.

Определение. Пусть A есть некоторая формула над множеством F функций из P_2. Если A есть $f(x_1, \ldots, x_m)$ из F, то единственной подформулой формулы A является она сама. Если A есть формула $f(A_1, \ldots, A_m)$, где $f \in F$, а $A_1, \ldots, A_m$ есть некоторые формулы над F, то подформулами формулы A являются она сама и все подформулы формул $A_1, \ldots, A_m$.

Замечание. Пусть $A(B)$ означает, что B есть подформула формулы A.

Везде далее слова множество, система, класс будем считать синонимами.

Определение. Класс функций F называется *функционально замкнутым*, если вместе с любыми своими функциями он содержит и любую их суперпозицию.

Определение. Множество функций $[F]$ называется *замыканием класса функций F*, если оно содержит все суперпозиции функций над множеством F и не содержит никаких других функций.

Замечание. 1. $F \subseteq [F]$.

2. $[[F]] = [F]$.

3. $F_1 \subseteq F_2$ влечет $[F_1] \subseteq [F_2]$.

4. Множество функций F замкнуто, если $[F] = F$.

Определение. Система G функций из замкнутого класса F *полна* в F (является порождающей системой для F), если $[G] = F$. Система функций H *полна* (в P_2), если $[H] = P_2$. Полная в F система функций G называется *базисом* в F, если никакая собственная подсистема в G не является полной в F.

1.3. Равносильные преобразования формул

Пусть A_1 и A_2 есть формулы, а $x_1, \ldots, x_n$ есть полный список их переменных. Формулы A_1 и A_2 называются *равносильными* (*равными*, *эквивалентными*), если для любого набора значений аргументов $x_1, \ldots, x_n$ они принимают одинаковые значения.

Пример. $A_1(x,y) = \overline{xy \vee \bar{x}}$; $A_2(x,y) = \overline{x \to y}$; $A_3(x) = x$; $A_4(x,y) = x \vee y$. В табл. 1.4 приведены значения формул A_1–A_4, из чего видно, что $A_1 = A_2, A_2 \neq A_3; A_2 \neq A_4; A_3 \neq A_4$.

Таблица 1.4

$x\ y$	A_1	A_2	A_3	A_4
0 0	0	0	0	0
0 1	0	0	0	1
1 0	1	1	1	1
1 1	0	0	1	1

В инженерной практике наиболее распространены представления функций формулами, построенными с помощью конъюнкции, дизъюнкции, отрицания, констант 0 и 1, т. е. формулами над $F = \{x \,\&\, y, x \vee y, \neg, 0, 1\}$. Такие формулы называются *булевыми*. Иногда в F включают импликацию.

Примем соглашение об опускании скобок в соответствии со следующим приоритетом операций: $\neg$, $\&$, $\vee$, $\to$. Укажем некоторые свойства операций $\neg$, $\&$, $\vee$. Эти операции (как и их свойства) называются булевыми.

Пусть A, B, C есть произвольные формулы над F. Тогда справедливы следующие свойства булевых операций.

1. *Идемпотентность*

$A \,\&\, A = A$ $\qquad$ $A \vee A = A$

2. *Коммутативность*

$A \,\&\, B = B \,\&\, A$ $\qquad$ $A \vee B = B \vee A$

3. *Ассоциативность*

$A \,\&\, (B \,\&\, C) = (A \,\&\, B) \,\&\, C$ $\qquad$ $A \vee (B \vee C) = (A \vee B) \vee C$

4. *Правила поглощения*

$A \,\&\, (A \vee B) = A$ $\qquad$ $A \vee (A \,\&\, B) = A$

5. *Дистрибутивность*

$A \,\&\, (B \vee C) = (A \,\&\, B) \vee (A \,\&\, C)$ $\qquad$ $A \vee (B \,\&\, C) = (A \vee B) \,\&\, (A \vee C)$

6. *Инволюция*

$\overline{\overline{A}} = A$

7. *Свойства констант*

нейтральный элемент $\qquad$ *поглощающий элемент*

$A \,\&\, 1 = A;\ A \vee 0 = A$ $\qquad$ $A \,\&\, 0 = 0\ \ A \vee 1 = 1$

8. *Правила Аристотеля*

закон исключенного третьего $\qquad$ *закон противоречия*

$A \vee \overline{A} = 1$ $\qquad$ $A \,\&\, \overline{A} = 0$

9. *Правила де Моргана*

$\overline{A \,\&\, B} = \overline{A} \vee \overline{B}$ $\qquad$ $\overline{A \vee B} = \overline{A} \,\&\, \overline{B}$

10. *Связь импликации, дизъюнкции и конъюнкции*

$A \to B = \overline{A} \vee B$ $\qquad$ $\overline{A \to B} = A \,\&\, \overline{B}$

11. *Правила Порецкого*

$A \,\&\, (\overline{A} \vee B) = A \,\&\, B$ $\qquad$ $A \vee (\overline{A} \,\&\, B) = A \vee B$

12. *Правила склеивания*

$(A \vee B) \,\&\, (A \vee \overline{B}) = A$ $\qquad$ $(A \,\&\, B) \vee (A \,\&\, \overline{B}) = A$

Все эти равенства устанавливаются непосредственной проверкой.

Правило подстановки (замены равным). Если

1) A, C есть формулы;
2) B есть подформула формулы A, т. е. A есть $A(B)$;
3) $B = C$, то $A(B) = A(C)$. Коротко правило подстановки записывают так:

$$\frac{A(B), B = C}{A(B) = A(C)}.$$

Примем без доказательства следующее утверждение.

Теорема. Если A и B есть булевы формулы и $A = B$, то с помощью булевых равенств 1–12 и правила подстановки от формулы A можно перейти к формуле B за конечное число шагов.

Эта теорема широко используется при упрощении формул.

Пример. $\overline{x \,\&\, y} \vee xy = \bar{x} \vee \bar{y} \vee xy = x \vee \bar{y} \vee xy = x \vee xy \vee \bar{y} = x \vee \bar{y}$.

Замечание. Пусть M есть некоторое множество и $P(M)$ есть множество всех подмножеств множества M. Если A, B, C есть произвольные подмножества из M и $\neg A$ интерпретируется как $M - A$ (т. е. A есть дополнение A до M), A & B как $A \cap B$, $A \vee B$ как $A \cup B$, 0 как пустое множество $\varnothing$, а 1 есть все множество M, то при таком теоретико-множественном понимании операций $\neg$, &, $\vee$ булевы свойства 1–12 останутся справедливыми.

Множество M, в котором определены операции $\neg$, &, $\vee$ и константы 0 и 1, удовлетворяющие аксиомам 1–12, называется *булевой алгеброй*. Обозначим булеву алгебру через (M, &, $\vee$, $\neg$, 0, 1). Тогда системы ({0,1}, &, $\vee$, $\neg$, 0, 1) и {$P(M)$, $\cap$, $\cup$, $\neg$, $\varnothing$, M) являются булевыми алгебрами.

Множество M, в котором определены две операции & и $\vee$, удовлетворяющие аксиомам 1–4, называется *решеткой*. Решетка *дистрибутивна*, если дополнительно выполняется аксиома 5 дистрибутивности.

Пусть множество M' = {0,1,2,01,02,12,012}. Элемент 012 понимаем как 0 & 1 & 2. Аналогично другие элементы из M'. Множество M состоит из множества M' и всех дизъюнкций попарно различных элементов множества M'. При этом ни одно дизъюнктивное слагаемое, рассматриваемое как множество своих сомножителей, не содержится в другом его дизъюнктивном слагаемом. Например, элементом множества M является дизъюнкция 01 $\vee$ 12 $\vee$ 02. Множество M с операциями & и $\vee$, удовлетворяющими аксиомам 1–5, образует (свободную) дистрибутивную решетку с образующими 0,1,2. Приведем пример преобразований в такой решетке. Решеточное выражение

(0 $\vee$ 2)(01 $\vee$ 12 $\vee$ 012) = 001 $\vee$ 012 $\vee$ 0012 $\vee$ 201 $\vee$ 212 $\vee$ 2012 =
01 $\vee$ 012 $\vee$ 012 $\vee$ 012 $\vee$ 12 $\vee$ 012 = 01 $\vee$ 12.

1.4. Нормальные формы. Совершенные нормальные формы

Элементарная конъюнкция есть конъюнкция, составленная из попарно различных переменных или отрицаний переменных.

Пример. x, y, xy, $\bar{x}_1 x_2 \bar{x}_3$.

Дизъюнктивная нормальная форма (ДНФ) есть дизъюнкция, составленная из попарно различных элементарных конъюнкций.

Пример. xy, $xy \vee x$, $x_1 \bar{x}_2 x_3 \vee \bar{x}_1 x_2 \bar{x}_3$.

Элементарная дизъюнкция есть дизъюнкция, составленная из попарно различных переменных или отрицаний переменных.

Пример. x, $x \vee \bar{y}$, $\bar{x} \vee y \vee \bar{z}$.

Конъюнктивная нормальная форма (КНФ) есть конъюнкция, составленная из попарно различных элементарных дизъюнкций.