Содержание

Предисловие

Теория алгоритмов имеет древнюю историю. Одна из основных задач математики - поиски алгоритмов для решения класса однотипных задач. Интуитивно алгоритм есть правило, способ, рекомендация, предписание, инструкция, программа для решения любой задачи из данного класса однотипных задач. Известен, например, алгоритм поиска наибольшего общего делителя двух натуральных чисел, алгоритм решения системы линейных алгебраических уравнений, другие алгоритмы. Задачи по разысканию алгоритмов продолжаются и поныне. Безуспешные длительные поиски некоторых алгоритмов привели к мысли, что дело тут не в недостатке изобретательности человеческого ума, а в отсутствии этих алгоритмов. Исследование вопроса об алгоритмически неразрешимых проблемах предполагает уточнение понятия алгоритма, его точное определение. Анализ уже известных алгоритмов позволил выделить его основные черты: 1) массовость, то есть алгоритм должен решать бесконечную серию однотипных задач; 2) детерминированность, то есть при любых обстоятельствах один и тот же алгоритм, примененный к одному и тому же объекту, должен давать один и тот же результат; 3) эффективность, то есть число шагов работы алгоритма конечно; при этом мы принимаем абстракцию потенциальной осуществимости: вычислительный процесс может продолжаться как угодно долго, но он обязан остановиться через конечное число шагов. На основании этих черт было дано точное определение алгоритма.

Мы подробно опишем два наиболее часто используемых уточнения понятия алгоритма: частично рекурсивная функция и машина Тьюринга. Будет построена частично рекурсивная функция, универсальная для класса всех частично рекурсивных функций, и приведены некоторые примеры алгоритмически неразрешимых проблем.

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 третьей 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 теории алгоритмов, комбинаторики, теории графов и связанных с ними практических алгоритмов.

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

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;
- $\overline{A} = U - A$, дополнение к 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:

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

Определим декартову степень множества

$$A^n = A \times A \times ... \times A \ (n \text{ раз}), A^0 = \varnothing.$$

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 $\mathbb{N} = \{0, 1, 2, ...\}$.

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

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

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

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.

Область определения функции $f : A \to B$ есть множество

$$D(f) = \{a \in A : \exists\, b \in B \ (f(a) = b)\}.$$

Область значений функции $f : A \to B$ есть множество

$$R(f) = \{b \in B : \exists\, a \in A \ (f(a) = b)\}.$$

Образ $\mathrm{Im}\, f = \{f(x) : x \in A\}$ *функции* $f : A \to B$ есть множество $f(A)$ всех значений функции f.

Заметим, что $\mathrm{Im}\, f = R(f) = f(A)$.

Если $f(a) = b$, то элемент b есть *образ элемента* a, а элемент a есть *прообраз элемента* b.

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 $\forall a \in S\ (g(a) = f(a))$.

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

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 $R(f) = \mathrm{Im}(f) = f(A) = \{1, 2, 3\}$.

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. Отношение

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

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

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) $(x_1, ..., x_n) \in \rho$ и предикатная (префиксная) $\rho(x_1, ..., x_n)$ 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 $a = (a_1, a_2, ..., a_n) \in \rho$ (допустима запись $\rho(a_1, a_2, ..., a_n)$) называется элементом отношения.

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

4. 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 $A = \bigcup\limits_{i \in I} A_i$, $\forall i \neq j \ (A_j \cap A_j = \varnothing)$.

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).

5. Каноническое разложение функции

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

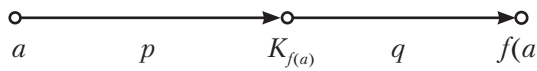
1) $a \sim a$, ибо $f(a) = f(a)$;

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 $\mathrm{Im}(f) = \{0, 1, 2, 3, 5\}$. 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:

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

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

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

6. 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 $B = \{a_0, a_1, a_2, ...\}$.

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, ... (их число может быть и конечным) в следующей таблице.

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

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

7. 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, ... из 0 и 1:

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

Построим последовательность $B: b_1, b_2, b_3, ...$, 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 так далее. 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: $|P(\mathbb{N})| = c$.

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 $A \cup B = (C \cup A_1) \cup B = C \cup (A_1 \cup B)$. 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.

8. 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 $A \sim B$.

$|A| \le |B|$, 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.

$|A| \ge |B|$, если $|B| \le |A|$.

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

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 $A \sim {}_f B_1$, $B \sim {}_g A_1$. С помощью функций f и g расслоим множества A и B на «кольца» следующим образом. Имеем:

$$A \sim_f B_1 \subset B, B \sim_g A_1 \subset A,$$
$$A_1 \sim_f B_2 \subset B_1, B_1 \sim_g A_2 \subset A_1,$$
$$A_2 \sim_f B_3 \subset B_2, B_2 \sim_g A_3 \subset A_2,$$
$$\ldots$$

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:

$K_0^A \sim_f K_1^B$, $K_0^B \sim_g K_1^A$,
$K_2^A \sim_f K_3^B$, $K_2^B \sim_g K_3^A$,

...

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

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

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

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:

$A_{\text{чет}} \sim_f B_{\text{неч}}$, $A_{\text{неч}} \sim_g B_{\text{чет}}$, $C \sim_{f \text{ или } g} D$.

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 $|A| \le |B|$.

Кардинальные числа можно сравнивать по величине.

Пусть A есть некоторое множество и $P(A)$ есть множество всех подмножеств множества A. Очевидно, что $|A| \le |P(A)|$, 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 $|A| \leq |P(A)|$, 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 выводимых 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

ТЕОРИЯ АЛГОРИТМОВ

В результате освоения учебного материала данной части студент должен:

- знать основные понятия и методы теории алгоритмов; основные варианты алгоритмов: частично рекурсивные функции, машины Тьюринга, нормальные алгоритмы Маркова, ассоциативные исчисления, системы подстановок, грамматики, продукции Поста, операторные алгоритмы; вопросы алгоритмической разрешимости и неразрешимости массовых проблем;
- уметь самостоятельно изучать методы работы с математической литературой и методику самостоятельного изучения новых разделов теории алгоритмов;
- иметь навыки расширения своих знаний в применении математического моделирования при разработке решений прикладных алгоритмических задач.

Глава 1

Частично рекурсивные функции

1.1. Арифметические функции и операции над ними

Пусть $\mathbb{N} = \{0, 1, 2, ...\}$ есть множество натуральных чисел.

Определение. *Арифметическая функция* $f(x_1, ..., x_n)$, $n = 0, 1, ..$, есть функция, аргументы и значения которой принадлежат множеству натуральных чисел.

Замечание. Константы 0, 1, 2, ... считаем нуль-местными функциями.

Пример.

$f_1(x, y) = x + y$, сложение.

$f_2(x, y) = x \cdot y$, умножение.

$f_3(x, y) = x^y$, возведение в степень.

$f_4(x, y) = x/y$, деление.

$f_5(x, y) = [x/y]$, целая часть частного. При $y = 0$ положим $[x/y] = x$.

Определение. Пусть $f(x_1, ..., x_m)$, $f_k(x_1, ..., x_n)$, $k = 1, 2, ..., m$, есть арифметические функции. *Подстановка* (*суперпозиция*) $\mathbb{S}(f^m, f_1^n, ..., f_m^n)$ функций $f_1, ..., f_m$ в функцию f есть оператор, который функциям $f, f_1, ..., f_m$ ставит в соответствие функцию $g(x_1, ..., x_n) = f(f_1(x_1, ..., x_n), ..., f_m(x_1, ..., x_n))$.

Замечание. В f^m верхний индекс m означает арность (местность) функции f.

Пример. 1. $f(x, y) = x + y$; $f_1^3 = I_1^3$; $f_2^3 = I_3^3$; $g(x, y, z) = \mathbb{S}(f^2, f_1^3, f_2^3) = f(I_1^3(x, y, z), I_3^3(x, y, z)) = I_1^3 + I_3^3 = x + z$.

2. $f(x, y) = x + y$; $I_1^3 = I_1^3$; $f_2^1 = s(x) = x + 1$. Подстановка $\mathbb{S}(f^2, f_1^3, f_2^1)$ не определена.

Определение. Пусть $g(x_1, ..., x_n)$ и $h(x_1, ..., x_n, y, z)$ есть n-местная и $(n+2)$-местная функции. *Примитивная рекурсия* $\mathbb{R}(g^n, h^{n+2})$ есть оператор, определенный на множестве пар функций, первая из которых n-местная, а вторая $(n+2)$-местная, сопоставляющий паре функций g и h $(n+1)$-местную функцию $f(x_1, ..., x_n, y)$, определяемую следующим образом:

$$f(x_1, ..., x_n, 0) = g(x_1, ..., x_n),$$
$$f(x_1, ..., x_n, y+1) = h(x_1, ..., x_n, y, f(x_1, ..., x_n, y)).$$

Замечание. Пусть q есть натуральное число. Одноместная функция $v(x)$ задается примитивной рекурсией $\mathbb{R}(C_q^0, h^2)$ следующим образом.

$f(0) = q = C_q^0(x)$,
$f(x + 1) = h(x, f(x))$.

Пример. 1. $f(x, y) = \mathbb{R}(I_1^1, s(I_3^3))$;
$f(x, 0) = I_1^1(x) = x$;
$f(x, y + 1) = s(I_3^3(x, y, f(x, y)) = f(x, y) + 1$.
Функция $v(x, y)$ есть сумма $x + y$.
2. $g(x, y) = \mathbb{R}(C_0^1, I_3^3 + I_1^3)$;
$g(x, 0) = C_0^1(x) = 0$;
$g(x, y + 1) = I_3^3(x, y, g(x, y)) + I_1^3(x, y, g(x, y)) = g(x, y) + x$.
Функция $g(x, y)$ есть произведение $x \cdot y$.

Замечание. Операции подстановки и примитивной рекурсии сохраняют всюду определенность функций.

Определение. Пусть $g(x_1, ..., x_n, y)$ есть арифметическая функция. *Операция минимизации* (оператор μ) есть оператор, сопоставляющий каждой $(n+1)$-местной функции $g(x_1, ..., x_n, y)$ n-местную функцию $f(x_1, ..., x_n)$, определяемую следующим образом:

$$f(x_1, ..., x_n) = (\mu y)(g(x_1, ..., x_n, y) = 0) =$$
$$\begin{cases} y, \text{ если } g(x_1, ..., x_n, y) = 0 \,\& \\ \quad (\forall t)_{<y}\ (g(x_1, ..., x_n, t) \neq 0 \,\& \\ \qquad \text{значение } g(x_1, ..., x_n, t) \text{ определено}); \\ \text{не опеределено в противном случае.} \end{cases}$$

Замечание. Ограниченный квантор $(\forall t)_{<y} A(t) \leftrightarrow (\forall t)(t < y \rightarrow A(t))$.

Пример. 1. $v(x) = (\mu y)(|x - 2 \cdot y| = 0)$; $v(0) = 0$, $v(1)$ не определено, $v(2) = 1$, $v(3)$ не определено и так далее.
2. Функция $w(x) = (\mu y)(x + y + 1 = 0)$ нигде не определена.

1.2. Примитивно рекурсивные функции

Определение. Функции

- $s(x) = x' = x + 1$ –функция следования;
- $I_k^n(x_1, ..., x_k, ..., x_n) = x_k$; $n = 1, 2, 3, ...$; $1 \le k \le n$ –функции выбора (или селекторные функции);
- $C_q^n(x_1, ..., x_n) \equiv q$; $n = 0, 1, 2, ...$; $q = 0, 1, 2, ...$ –функции-константы

назовем *исходными функциями*.

Определение. *Примитивно рекурсивное описание* (ПРО) есть конечная последовательность арифметических функций, каждая из которых есть либо исходная функция, либо получена из предыдущих функций последовательности с помощью операции подстановки или примитивной рекурсии.

Определение. Арифметическая функция f называется *примитивно рекурсивной функцией* (ПРФ), если существует ПРО, последней функцией которого является f.

Пример. 1. Покажем, что сложение $x + y$ есть ПРФ. Построим следующее ПРО.

- $f_1(x) = I_1^1(x) = x$ –исходная функция;
- $f_2(x, y, z) = I_3^3(x, y, z)$ –исходная функция;
- $f_3(x) = s(x) = x + 1$ –исходная функция;
- $f_4(x, y, z) = s(I_3^3(x, y, z))$, $\mathbb{S}(s^1, I_3^3)$;
- $f_5(x, y) = \mathbb{R}(f_1^1, f_4^3)$. Отсюда

$$\begin{cases} f_5(x,0) = f_1^1(x) = x, \\ f_5(x,y+1) = f_4^3(x,y,f_5(x,y)) = f_5(x,y)+1; \end{cases} \quad \begin{cases} f_5(x,0) = x, \\ f_5(x,y+1) = f_5(x,y)+1; \end{cases}$$

Обозначим f_5 через $+_5$:

$$\begin{cases} +_5(x,0) = x, \\ +_5(x,y+1) = +(x,y)+1; \end{cases} \quad \begin{cases} x+0 = x, \\ x+(y+1) = (x+y)+1; \end{cases} \quad \begin{cases} x+0 = x, \\ x+y' = (x+y)', \end{cases}$$

что есть рекурсивное задание Пеано для сложения $x + y$. Последовательность функций f_1, f_2, f_3, f_4, f_5 есть ПРО, последняя функция которого есть функция $f_5(x, y) = x + y$. Следовательно, сложение $x + y$ есть ПРФ.

2. Покажем, что умножение $x \cdot y$ есть ПРФ. Построим следующее ПРО.

- $f_1(x) = I_1^1(x) = x$, исходная функция;
- $f_2(x, y, z) = I_3^3(x, y, z)$, исходная функция;
- $f_3(x) = s(x) = x + 1$, исходная функция;
- $f_4(x, y, z) = s(I_3^3(x, y, z)) = \mathbb{S}(s^1, I_3^3)$;
- $f_5(x, y) = \mathbb{R}(f_1^1, f_4^3) = x + y$. Далее
- $f_6(x) = C_0^1(x) = 0$, исходная функция;
- $f_7(x, y, z) = I_1^3(x, y, z) = x$, исходная функция;
- $f_8^3(x, y, z) = \mathbb{S}(f_5^2, I_3^3, I_1^3) = \mathbb{S}(+, z, x) = z + x$;
- $f_9^2(x, y) = \mathbb{R}(f_6^1, f_8^3) = \mathbb{R}(C_0^1 \equiv 0, f_8^3(x, y, z) = z + x)$.

Отсюда

$$\begin{cases} f_9(x,0) = C_0^1(x) = 0, \\ f_9(x,y+1) = f_8^3(x,y,f_9(x,y)) = f_9(x,y)+x; \end{cases} \quad \begin{cases} f_9(x,0) = 0, \\ f_9(x,y+1) = f_9(x,y)+x; \end{cases}$$

Обозначим f_9 через $\cdot_9$:

$$\begin{cases} \cdot_9(x,0) = x, \\ \cdot_9(x,y+1) = \cdot(x,y)+x; \end{cases} \quad \begin{cases} x\cdot 0 = 0, \\ x\cdot(y+1) = x\cdot y + x; \end{cases} \quad \begin{cases} x\cdot 0 = 0, \\ x\cdot y' = x\cdot y + x, \end{cases}$$

что есть рекурсивное задание Пеано для умножения $x \cdot y$. Последовательность функций $f_1, f_2, ..., f_9$ есть ПРО, последняя функция которого есть функция $f_9(x, y) = x \cdot y$. Следовательно, умножение $x \cdot y$ есть ПРФ.

Отметим следующие свойства ПРО:

1) каждый начальный отрезок ПРО есть ПРО;
2) каждая функция в ПРО примитивно рекурсивна;
3) если в ПРО в любом его месте между двумя соседними функциями вставить ПРФ, то получим снова ПРО;
4) если в ПРО в любом его месте между двумя соседними функциями вставить другое ПРО, то получим снова ПРО.

Замечание. Всякая ПРФ всюду определена, ибо исходные функции всюду определены, и операции подстановки и примитивной рекурсии сохраняют всюду определенность функций.

Определение. Пусть H есть конечная совокупность функций. *Примитивно рекурсивное описание относительно совокупности функций H* есть конечная последовательность функций, каждая из которых есть либо исходная функция, либо функция из совокупности H, либо получена из предыдущих функций.

Определение. *Функция f примитивно рекурсивна относительно совокупности функций H*, если существует ПРО относительно совокупности H, последней функцией которого является f.

Отметим свойства ПРО относительно совокупности функций H:

1) если функция f примитивно рекурсивна относительно совокупности функций H, а функции из H входят в совокупность функций M, то функция f примитивно рекурсивна относительно совокупности M;
2) если функция f примитивно рекурсивна относительно совокупности функций H и совокупность функций G из H состоит только из ПРФ, то функция f примитивно рекурсивна относительно совокупности $H - G$;
3) если функция f примитивно рекурсивна относительно совокупности функций H и каждая функция из H примитивно рекурсивна относительно совокупности функций G, то функция f примитивно рекурсивна относительно совокупности G;
4) примитивно рекурсивная функция примитивно рекурсивна относительно любой совокупности функций;
5) если функция f примитивно рекурсивна относительно совокупности функций H и G есть совокупность ПРФ, то функция f примитивно рекурсивна относительно совокупности $H \cup G$.

К свойствам примитивно рекурсивного описания относительно совокупности функций следует добавить свойства ПРО.

1.3. Функции, представимые термами

Формальные символы

1. $f_1^{n_1}, f_2^{n_2}, ..., f_r^{n_r}$ –символы для арифметических функций с указанной вверху местностью.

2. 0, 1, 2, ... –символы натуральных чисел.

3. x, y, z, ... –символы переменных.
4. (,) есть скобки левая и правая и запятая.

Термы

1. Символ натурального числа есть терм ранга 1.
2. Символ переменной есть терм ранга 1.
3. Если f_k есть функциональный символ, а t_1, ..., t_{n_k} есть термы, максимальный ранг которых равен k, то выражение $f_k(t_1, ..., t_{n_k})$ есть терм ранга k+1.

Пример. x; 0; 1; 2; 10; 17; f_1(x, 1); f_2(17, x, 10); $f_1(f_1$(x, 2), f_2(17, x, 10)).

Замечание. Содержательно терм есть некоторая подстановка (суперпозиция) функций. Ранг терма называют также глубиной построения терма.

Определим индукцией по построению терма понятие функции, представимой термом (термальной функции). Пусть терму $f_k(x_1, ..., x_n)$ поставлена в соответствие функция $f_k(x_1, ..., x_n)$.

Определение (функции, представимой термом)

1. Терму x_k ранга 1 поставим в соответствие функции выбора $I_k^n(x_1, ..., x_k, ..., x_n) = x_k$; $n = 1, 2, 3, ...$; $1 \le k \le n$.

2. Терму первого ранга q (символу натурального числа) сопоставим функции-константы $C_q^n(x_1, ..., x_n) \equiv q$; $n = 0, 1, 2, ...$; $q = 0, 1, 2, ...$.

3. Если термам t_1, ..., t_{n_k} поставлены в соответствие функции t_1, ..., t_{n_k} и функциональному символу f_k поставлена в соответствие функция f_k, то терму $f_k(t_1, ..., t_{n_k})$ поставим в соответствие функцию $f_k(t_1, ..., t_{n_k})$.

Теорема. Функция, представимая термом, примитивно рекурсивна относительно функций, составляющих терм.

Доказательство. Индукция по рангу r терма. Пусть термы строятся из функциональных символов, соответствующих совокупности $F = \{f_1, ..., f_n\}$.

Базис. $r = 1$. Термам x_k и q поставлены в соответствие функции выбора I_k^n и функции-константы C_q^n соответственно, которые, будучи примитивно рекурсивными, примитивно рекурсивны относительно любой совокупности функций, в том числе относительно совокупности функций F.

Предположение индукции. Допустим, что функции, представимые термами ранга меньше r, примитивно рекурсивны относительно совокупности функций F.

Шаг индукции. Покажем, что функция $f_k(t_1, ..., t_{n_k})$, представимая термом $f_k(t_1, ..., t_{n_k})$ ранга r, примитивно рекурсивна относительно совокупности функций F.

Так как термы t_1, ..., t_{n_k} имеют ранг меньше r, то представимые ими функции $t_1, ..., t_{n_k}$ примитивно рекурсивны относительно совокупности F по предположению индукции. Подходящими подстановками в них функций выбора и констант мы придем к функциям одинаковой местности $u_1, ..., u_{n_k}$. Тогда функция $g = f_k(t_1, ..., t_{n_k}) = f_k(u_1, ..., u_{n_k})$. Так как функции $u_1, ..., u_{n_k}$ примитивно рекурсивны относительно F, то функция g примитивно рекурсивна относительно F, ибо получена подстановкой из функций, примитивно рекурсивных относительно F.

Пример. 1. Функция $f(x) = f_1(f_2(x, 0), 5)$, представимая термом $f_1(f_2$(x, 0), 5), примитивно рекурсивна относительно совокупности функций $F = \{f_1(x, y), f_2(x, y)\}$,

соответствующих термам $f_1(x, y)$, $f_2(x, y)$, ибо последовательность функций C_0^1; I_1^1; $g_1^1 = \mathbb{S}(f_2^2, C_0^1, I_1^1)$; C_5^1; $f = \mathbb{S}(f_1^2, g_1^1, C_5^1)$ есть ПРО относительно совокупности функций F.

2. Функция f, представимая термом $f_1(x, f_2(y, f_3(x)), 2)$, примитивно рекурсивна относительно совокупности функций $F = \{f_1^2, f_2^2, f_3^1\}$, соответствующих термам $f_1(x, y, z)$, $f_2(x, y)$, $f_3(x)$. Вот ПРО для f относительно F: I_1^3; I_2^3; I_3^3; C_2^3; $g_1^3 = \mathbb{S}(f_1^3, I_1^3)$; $g_2^3 = \mathbb{S}(f_2^2, I_2^3, g_1^3)$; $f = \mathbb{S}(f_1^3, I_1^3, g_2^3, C_2^3)$.

1.4. Конечные сумма и произведение

Определение. Пусть $f(x_1, ..., x_n, y)$ есть арифметическая функция. *Конечная сумма* относительно функции $f(x_1, ..., x_n, y)$ есть функция

$$\sigma(x_1, ..., x_n, y) = \sum_{t=0}^{y} f(x_1, ..., x_n, t) = f(x_1, ..., x_n, 0) + f(x_1, ..., x_n, 1) + ... + f(x_1, ..., x_n, y).$$

Теорема. Конечная сумма относительно функции f примитивно рекурсивна относительно f.

Доказательство. Пусть x есть $x_1, ..., x_n$. Тогда

$\sigma(x, 0) = f(x, 0)$;
$\sigma(x, y + 1) = \sigma(x, y) + f(x, y + 1)$.

Построим ПРО функции σ относительно функции f.

f^{n+1}; I_1^n; I_2^n; ...; I_n^n; C_0^n; $s(x)$; I_1^{n+2}; ...; I_{n+2}^{n+2}; $x + y$;
$g^n = f(x_1, ..., x_n, 0) = \mathbb{S}(f^{n+1}, I_1^n, I_2^n, ..., I_n^n, C_0^n)$;
$u_1^{n+2} = \mathbb{S}(s, I_{n+1}^{n+2}) = x_{n+1} + 1$;
$u_2^{n+2} = \mathbb{S}(f^{n+1}, I_1^{n+2}, ..., I_n^{n+2}, u_1^{n+2}) = f^{n+1}(I_1^{n+2}, ..., I_n^{n+2}, u_1^{n+2}) = f(x_1, ..., x_n, y + 1)$;
$h^{n+2} = \mathbb{S}(+, I_{n+2}^{n+2}, u_2^{n+2}) = I_{n+2}^{n+2} + u_2^{n+2} = x_{n+1} + f(x, y + 1)$;
$\sigma^{n+1} = \mathbb{R}(g^n, h^{n+2})$;

при этом

$\sigma(x, 0) = g(x) = f(x, 0)$;
$\sigma(x, y + 1) = h(x, y, \sigma(x, y)) = \sigma(x, y) + f(x, y + 1)$.

Определение. Пусть $f(x_1, ..., x_n, y)$ есть арифметическая функция. *Конечное произведение* относительно функции $f(x_1, ..., x_n, y)$ есть функция

$$\pi(x_1, ..., x_n, y) = \prod_{t=0}^{y} f(x_1, ..., x_n, t) = f(x_1, ..., x_n, 0) \cdot f(x_1, ..., x_n, 1) \cdot ... \cdot f(x_1, ..., x_n, y).$$

Теорема. Конечное произведение относительно функции f примитивно рекурсивно относительно f.

Доказательство. Пусть x есть $x_1, ..., x_n$. Тогда

$\pi(x, 0) = f(x, 0)$;
$\pi(x, y + 1) = \pi(x, y) + f(x, y + 1)$.

Построим ПРО функции π относительно функции f.

$f^{n+1}; I_1^n; I_2^n; ...; I_n^n; C_0^n; s(x); I_1^{n+2}; ...; I_{n+2}^{n+2}; x + y; x \cdot y;$

$g^n = f(x_1, ..., x_n, 0) = \mathbb{S}(f^{n+1}, I_1^n, I_2^n, ..., I_n^n, C_0^n);$

$u_1^{n+2} = \mathbb{S}(s, I_{n+1}^{n+2}) = x_{n+1} + 1;$

$u_2^{n+2} = \mathbb{S}(f^{n+1}, I_1^{n+2}, ..., I_n^{n+2}, u_1^{n+2}) = f^{n+1}(I_1^{n+2}, ..., I_n^{n+2}, u_1^{n+2}) = f(x_1, ..., x_n, y + 1);$

$h^{n+2} = \mathbb{S}(\cdot, I_{n+2}^{n+2}, u_2^{n+2}) = I_{n+2}^{n+2} + u_2^{n+2} = x_{n+1} \cdot f(x, y + 1);$

$\pi^{n+1} = \mathbb{R}(g^n, h^{n+2});$

при этом

$\pi(x, 0) = g(x) = f(x, 0);$

$\pi(x, y + 1) = h(x, y, \pi(x, y)) = \pi(x, y) \cdot f(x, y + 1).$

Примитивная рекурсивность некоторых функций

1. $sg(x) = \begin{cases} 0, \text{если } x = 0, \\ 1, \text{если } x > 0. \end{cases} \quad \begin{cases} sg(0) = 0 = C_0^0(x), \\ sg(x+1) = 1 = C_0^2(x, sg(x)). \end{cases}$

ПРО для $sg(x)$: C_0^0; C_1^2; $\mathbb{R}(C_0^0, C_1^2)$.

2. $\overline{sg}(x) = \begin{cases} 1, \text{если } x = 0, \\ 0, \text{если } x > 0. \end{cases} \quad \begin{cases} \overline{sg}(0) = 1 = C_1^0(x), \\ \overline{sg}(x+1) = 0 = C_0^2(x, \overline{sg}(x)). \end{cases}$

ПРО для $\overline{sg}(x)$: C_1^0; C_0^2; $\mathbb{R}(C_1^0, C_0^2)$.

3. $g(x) = x \dot{-} 1 = \begin{cases} 0, \text{если } x = 0, \\ x - 1, \text{если } x > 0. \end{cases}$

$g(0) = 0 = C_0^0$; $g(x + 1) = x = I_1^2(x, g(x))$.

ПРО для $g(x)$: C_0^0, I_1^2, $\mathbb{R}(C_0^0, I_1^2)$.

4. $f(x, y) = x \dot{-} y = \begin{cases} 0, \text{если } x < y, \\ x - y, \text{если } x \geq y. \end{cases}$

$f(x, 0) = x \dot{-} 0 = x = I_1^1$; $f(x, y+1) = x \dot{-} (y+1) =$
$(x \dot{-} y) \dot{-} 1 = f(x, y) \dot{-} 1 = g(f(x, y))$, где $g(x) = x \dot{-} 1$.

ПРО для $f(x, y)$: I_1^1; I_1^2, I_1^3; I_2^3; I_3^3; $g(x)$; $g_1^3 = \mathbb{S}(g(x), I_3^3)$; $f(x, y) = \mathbb{R}(I_1^1, g_1^3)$, при этом

$f(x, 0) = x = I_1^1(x)$;

$f(x, y+1) = g_1^3(x, y, f(x, y)) = g(I_3^3(x, y, f(x, y))) = g(f(x, y))$.

5. $h(x, y) = |x - y|$; $h(x, y) = (x \dot{-} y) + (y \dot{-} x)$. Функция $h(x, y)$ термальна относительно ПРФ $x + y$ и $x \dot{-} y$.

Следовательно, $h(x, y)$ есть ПРФ по теореме о функции, представимой термом.