А. Н. Гамова

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

О Г Л А В Л Е Н И Е

ПРЕДИСЛОВИЕ

Данное учебное пособие представляет собой курс лекций, которые автор читает на механико-математическом факультете Саратовского государственного университета, начиная с 1993 года . Содержание курса составили два раздела математической логики: исчисления и алгоритмы. Подбор материала лекций определялся задачей развития у слушателей навыков использования методов математической логики для изучения других математических наук. Так, развитый в математической логике, современный аксиоматический метод сначала был применен для построения аксиоматической системы в исчислении высказываний и исчислении предикатов первого порядка, а затем для

построения теории первого порядка, содержащей нелогические аксиомы, - арифметики Пеано. В разделе теории алгоритмов представлены два направления уточнения алгоритма и вычислимости – машины Тьюринга и частично рекурсивные функции С.Клини. Полученные там результаты на примере построенных формальных систем использовались для изучения проблем полноты, непротиворечивости и разрешимости.

Многие важные теоремы не вошли в пособие из-за ограниченности объема курса, например, доказательство эквивалентности разных уточнений понятия алгоритма и др. Не ставилась задача изложения исчислений высших порядков и обобщенных вычислений, а также неклассических логик, что может составить предмет дальнейшего изучения. Из приложений выделим конечные автоматы, теорию формальных языков, определения случайности, алгоритмическую теорию информации, а также недетерминированные вычисления на машине Тьюринга, связанные с центральной проблемой теории сложности вычислений P=NP.

Обзор приложений и рекомендации для дальнейшего чтения можно найти в списке литературы [6-10].

ВВЕДЕНИЕ

Логика возникла в культуре Древней Греции. Первое дошедшее до нас сочинение по логике - “Аналитики” Аристотеля (384-322гг. до н.э.). Независимо развивалась буддистская логика, но достоянием европейской науки она стала сравнительно недавно, поэтому известная нам логика “вышла” из логики Аристотеля. Математическая логика отличается тем, что пользуется языком математических символов. Ее основоположниками были: Д.Буль (исчисление высказываний), Г.Фреге, Г.Пеано, Б.Рассел. Выдвинутая в 20-е годы X1X века программа Д.Гильберта обоснования математики с помощью логики привела к формализации математических теорий, много частных задач было решено. К настоящему времени доказана непротиворечивость элементарной геометрии, арифметики, анализа, аксиоматической системы теории множеств Цермело-Френкеля и т.д. Некоторые важные теории оказались полными: исчисление высказываний и исчисление предикатов, элементарная геометрия, теория векторных пространств и т.д. Но в других теориях

получены предложения, которые нельзя ни доказать, ни опровергнуть. Так, в аксиоматической теории множеств Цермело-Френкеля это аксиома выбора и континуум-гипотеза. Как следует из теорем Геделя о неполноте, всякая достаточно богатая теория необходимо содержит такие предложения.

В математической логике было дано точное определение алгоритма и вычислимости. Вопрос о существовании алгоритмов имеет для математики первостепенное значение (например, алгоритм существования решений для системы уравнений). Были получены разрешающие алгоритмы для ряда теорий, например, элементарной геометрии, упорядоченного поля действительных чисел, атомной булевой алгебры и т.д. Неразрешимы теории (т.е. не существует единого алгоритма для решения всех задач) элементарной арифметики, анализа, класса всех конечных симметрических групп (т.е.групп перестановок), аксиоматических систем теории множеств.

В последние годы большое внимание уделяется теории сложности алгоритмов и вычислений. Выяснилось, что одного только существования алгоритма, решающего ту или иную массовую проблему, далеко не достаточно для практики. После уточнения понятия сложности вычисления стали исследовать вопросы такого рода, как внутренняя сложность вычислимой функции, ее криптографическая стойкость, приобретающие особую актуальность с развитием сетей связи, вычислительной техники и автоматизированных систем управления.

РАЗДЕЛ 1. И С Ч И С Л Е Н И Я

Г л а в а 1

ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

1.1. Алгебра высказываний

Содержание любой науки составляют утверждения об объектах ее предметной области. Логика высказываний абстрагируется от конкретного содержания утверждений (высказываний) и изучает структуру сложных высказываний и их логические связи.

Высказывание есть повествовательное предложение, истинное или ложное.
Примеры высказываний: “Снег белый” , “2>3”, “Если идет дождь, то я беру зонт” и т.д.

Изучать математическую логику мы будем с помощью математических методов в некотором метаязыке, который будем отличать от предметного языка изучаемой логики. Предметный язык логики высказываний состоит из алфавита и формул:

А л ф а в и т: (1) P, Q, R, ... - переменные для простых высказываний (пропозициональные буквы);

(2) $\&$, $\vee$, $\rightarrow$, $\neg$, $\leftrightarrow$ - символы операций над высказываниями (логические связки);

(3) (,) - вспомогательные символы (скобки).

Ф о р м у л ы, или сложные высказывания: (1) P, Q,R, ... – пропозициональные буквы – элементарные формулы (атомы);
(2) если A, B - формулы, то A&B, A∨B, A→B, A ↔B, ¬A - формулы.
В определении формул использованы *метабуквы* A, B, т.е. символы, не принадлежащие предметному языку. Примеры формул: (P&Q), (R→ (P ∨ R)).

Подформула - это часть формулы, сама являющаяся формулой.

Задав язык, мы построили формальную систему. Представим теперь ее как содержательную *алгебру высказываний*, для чего придадим смысл символам алфавита и формулам. Пропозициональные буквы и логические операции определим на области из двух элементов {И, Л}:

P	Q	P&Q	P∨Q	¬P	P→Q	P↔Q
И	И	И	И	Л	И	И
И	Л	Л	И	Л	Л	Л
Л	И	Л	И	И	И	Л
Л	Л	Л	Л	И	И	И

Значение формулы $E[P_1, ..., P_n]$ *при данной интерпретации входящих в нее пропозициональных букв (входов)* $\gamma : \{P_1, ..., P_n\} \Rightarrow \{И,Л\}$

определим индукцией по построению формулы:. E = P : E[γ] = γ (P);
E = A&B : E[γ] = (A&B)[γ] = A[γ] & B[γ]; E = ¬A : E[γ] = ¬A[γ];
E = A∨B : E[γ] = (A∨B)[γ] = A[γ] ∨ B[γ];
аналогично для остальных логических связок.

Истинностная таблица формулы составлена из строк, задающих значения всех подформул данной формулы:

P	Q	R	P&Q	(P&Q) ∨R	P∨Q	¬(P∨Q)	(P&Q)∨R → ¬(P∨Q)
И	И	И	И	И	И	Л	Л
И	И	Л	И	И	И	Л	Л
И	Л	И	Л	И	И	Л	Л
И	Л	Л	Л	Л	И	Л	И
Л	И	И	Л	И	И	Л	Л
Л	И	Л	Л	Л	И	Л	И
Л	Л	И	Л	И	Л	И	И
Л	Л	Л	Л	Л	Л	И	И

Т а в т о л о г и я *(общезначимая формула, логический закон) - формула, истинная при всех интерпретациях входящих в нее пропозициональных букв,* другими словами, - столбец значений которой содержит одни истинные значения (обозначается знаком |=)**.**

ТЕОРЕМА 1 (*Подстановка вместо атомов*). Пусть формула $E[P_1, \ldots, P_n]$ содержит пропозиционные буквы $P_1, \ldots, P_n$, а формула $E^*[A_1, \ldots, A_n]$ получена одновременной подстановкой формул $A_1, \ldots, A_n$ вместо атомов $P_1, \ldots, P_n$, соответственно. Тогда если $\models E$, то $\models E^*$. Обратное неверно.

Доказательство проведем индукцией по построению формулы E: Рассмотрим случай $E = (A\&B)[P_1, \ldots, P_n]$. Пусть $\models (A\&B)[P_1, .., P_n]$, т.е. $(A\&B)[P_1, .., P_n][\gamma] = И$ для всех интерпретаций γ. Тогда по определению значения формулы: $A[P_1, .., P_n][\gamma] = И$ и $B[P_1, .., P_n][\gamma] = И$ для всех интерпретаций γ. Откуда $\models A[P_1, \ldots, P_n]$ и $\models B[P_1, \ldots, P_n]$ и, по индукционному допущению, $\models A^*[A_1, \ldots, A_n]$ и $\models B^*[A_1, \ldots, A_n]$. Таким образом, $\models A^* \& B^*$, т.е. $\models (A\&B)^*$, следовательно, $\models E^*$.

Пример применения теоремы 1 **:** Чтобы проверить, является ли формула $(P\&\neg Q)\&(R\rightarrow P)\rightarrow(P\&\neg Q)$ [1] тавтологией, достаточно убедиться в том, что общезначима формула $E(P,Q) = P\&Q \rightarrow P$. Поэтому в истинностной таблице на входы можно помещать метабуквы.

Упражнение

1) Сравните истинностные таблицы формул $\neg P \vee Q$ и $P\rightarrow Q$.
2) Будет ли тавтологией формула $(\neg P \vee Q)\&(R\rightarrow(P\leftrightarrow Q))$?
3) Найдите тавтологии среди следующих формул:
   $(P\& \neg P)\rightarrow(Q\vee R\rightarrow(R\rightarrow\neg P))$;
   $(P\rightarrow\neg P)\sim \neg P$;
   $P\rightarrow P$.
4) Вычислив только одну строку таблицы истинности, найдите формулы, не являющиеся тавтологиями:
   а) $P\vee Q\rightarrow P\&Q$;
   б) $(P\rightarrow Q)\rightarrow(Q\rightarrow P)$.
5) Найдите формулу, у которой в столбце значений стоит только ложь.
6) Существуют ли такие высказывания A, B и C, чтобы для них одновременно выполнялись следующие условия: для некоторой интерпретации γ

$$(A \rightarrow B)[\gamma] = И; \quad (B \vee C)[\gamma] = Л; \quad (B \leftrightarrow (A\&\neg C))[\gamma] = Л.$$

7) Найти значение формулы $(\neg B\rightarrow A)[\gamma]$, если $(A\vee B)[\gamma]=И$ и $(A\rightarrow B)[\gamma]=И$.

ТЕОРЕМА 2 (*Основные тавтологии*).

1а. $\models A\rightarrow(B\rightarrow A)$
1б. $\models(A\rightarrow B)\rightarrow((A\rightarrow(B\rightarrow C))\rightarrow(A\rightarrow C))$
2. $\models A\rightarrow(B\rightarrow A\&B)$
3а. $\models A\&B\rightarrow A$
3б. $\models A\&B\rightarrow B$
4а. $\models A\rightarrow A\vee B$
4б. $\models B\rightarrow A\vee B$
5. $\models(A\rightarrow C)\rightarrow((B\rightarrow C)\rightarrow(A\vee B\rightarrow C))$
6. $\models(A\rightarrow C)\rightarrow((A\rightarrow\neg C)\rightarrow \neg A)$

---

[1] Для сокращения количества скобок договоримся о приоритете логических операций: $\{\neg\}$, $\{\&,\vee\}$, $\{\rightarrow,\leftrightarrow\}$

7. $\models\neg\neg A \to A$
8. $\models(A \to B) \to ((B \to A) \to (A \leftrightarrow B))$
9а. $\models(A \leftrightarrow B) \to (A \to B)$
9б. $\models(A \leftrightarrow B) \to (B \to A)$
10. $\models(A \to (\neg A \to C)$

Д о к а з а т е л ь с т в о. Применяем теорему 1 и таблицы истинности формул.

Д р у г и е т а в т о л о г и и :

1) $\models A \vee \neg A$ (*закон исключённого третьего*)
2) $\models A \to A$ (*закон тождества*)
3) $\models \neg(A \vee B) \sim \neg A \& \neg B$ (*1-й закон де Моргана*)
4) $\models \neg(A \& B) \sim \neg A \vee \neg B$ (*2-й закон де Моргана*)
5) $\models A \& A \sim A$, $\models A \vee A \sim A$
6) $\models A \to B \sim \neg A \vee B$
7) $\models (A \leftrightarrow B) \sim (A \to B) \& (B \to A)$
8) $\models (A \to B) \sim (\neg B \to \neg A)$ (*закон контрапозиции*)
9) $\models A \& B \sim B \& A$ (*коммутативность конъюнкции*)
10) $\models A \vee B \sim B \vee A$ (*коммутативность дизъюнкции*)
11) $\models A \& (B \& C) \sim (A \& B) \& C$ (*ассоциативность конъюнкции*)
12) $\models A \vee (B \vee C) \sim (A \vee B) \vee C$ (*ассоциативность дизъюнкции*)
13) $\models A \& (B \vee C) \sim (A \& B) \vee (A \& C)$(*1-й закон дистрибутивности*)
14) $\models A \vee (B \& C) \sim (A \vee B) \& (A \vee C)$(*2-й закон дистрибутивности*)
15) $\models A \& (A \vee B) \sim A$, $\models A \vee (A \& B) \sim A$ (*законы поглощения*)
16) $\models A \& И \sim A$, $\models A \& Л \sim Л$, $\models A \vee И \sim И$, $\models A \vee Л \sim A$.
17) $\models A \to (B \to C) \sim A \& B \to C$

ТЕОРЕМА 3. Если $\models A$ и $\models A \to B$, то $\models B$.

Д о к а з а т е л ь с т в о. Пусть $\models A$ и $\models A \to B$ и $P_1, \ldots, P_n$ - все переменные, входящие в эти формулы. Допустим противное, что при некоторой интерпретации $\gamma : \{P_1, \ldots, P_n\} \Rightarrow \{И,Л\}$, $B[\gamma] = Л$. По условию, для всех интерпретаций, в частности, для интерпретации γ, $A[\gamma] = И$ и $(A \to B)[\gamma] = И$, что однако противоречит определению операции $\to$.

Формулы A и B назовем эквивалентными, если $\models A \leftrightarrow B$**.**

ТЕОРЕМА 4 (*Эквивалентность формул*). Формулы A и B эквивалентны т.и т.т., когда A и B имеют одинаковые истинностные таблицы.

Д о к а з а т е л ь с т в о. Для всех интерпретаций γ пропозициональных букв, $(A \leftrightarrow B)[\gamma] = И$ т.и т.т., когда $A[\gamma] = B[\gamma]$. Откуда следует утверждение теоремы.

ТЕОРЕМА 5(*О замене*). Пусть формула E[A] содержит подформулу A. Формула E[B] есть результат замены выделенного вхождения формулы A на формулу B. Тогда, если $\models A \sim B$, то $\models E[A] \sim E[B]$.
Д о к а з а т е л ь с т в о получается с помощью теоремы 4.

Следствие. Если $\models A \sim B$ и $\models E[A]$, то $\models E[B]$.

Пример. Упростить формулу $((P \vee S) \leftrightarrow \neg Q) \& \neg S \to \neg((S \to R \vee Q) \vee P)$:
$((P \vee S) \leftrightarrow \neg Q) \& \neg S \to \neg((S \to R \vee Q) \vee P) \sim$
$((P \vee S \to \neg Q) \& (\neg Q \to P \vee S) \& \neg S) \to \neg(\neg S \vee R \vee Q \vee P) \sim$

$\neg((P\vee S\to\neg Q)\,\&(\neg Q\to P\vee S)\&\neg S)\ \vee\ \neg(\neg S\vee R\vee Q\vee P)\ \sim$
$\neg((\neg(P\vee S)\vee\neg Q)\,\&(\neg\neg Q\vee P\vee S)\,\&\neg S)\vee\ \neg(\neg S\vee R\vee Q\vee P)\ \sim$
$\neg(\neg(P\vee S)\vee\neg Q)\vee\ \neg(Q\vee P\vee S)\vee\neg\neg S)\vee(\neg\neg S\,\&\neg R\,\&\neg Q\,\&\neg P)\sim$
$((P\vee S)\,\&\neg\neg Q)\vee(\neg Q\&\neg P\&\neg S)\ \vee\neg\neg S\vee(\neg\neg S\,\&\neg R\,\&\neg Q\,\&\neg P)\sim$
$(P\&Q)\vee(S\&Q)\vee(\neg Q\&\neg P\&\neg S)\ \vee\ S\ \sim\ (P\&Q)\vee(\neg Q\&\neg P\&\neg S)\vee S\ \sim$
$(P\&Q)\vee((\neg Q\vee S)\&(\neg P\vee S)\&(\neg S\vee S))\ \sim(P\&Q)\vee(\neg Q\&\neg P)\vee S.$

Формула называется формулой с тесными отрицаниями, если операция ¬ применяется только к атомам.

ТЕОРЕМА 6. Пусть E формула с тесными отрицаниями, не содержащая других операций, кроме ¬, &, ∨. Формула E^X есть результат замены в E (на всех местах) конъюнкции на дизъюнкцию, дизъюнкции на конъюнкцию и каждой пропозициональной буквы на ее отрицание. Тогда $\models \neg E\sim E^X$.

Доказательство теоремы проведем индукцией по построению фор мулы E. Базис индукции: E≡P : $\neg E\equiv\neg P$ и, по определению операции 'X', $E^X\equiv\neg P$, ч.т.д. Индукционный шаг : a) E ≡ A&B, b) E ≡ A∨B, c) E ≡¬A..

a) E≡A&B: $\models\neg E\sim\neg(A\&B)$ ~(по закону де Моргана) $\neg A\vee\neg B\sim$ (по индукционному допущению и теореме 5) $A^X\vee B^X\sim$ (по определению операции 'крест') $(A\&B)^X\equiv E^X$.

b) E≡A∨B: $\models\neg E\sim\neg(A\vee B)$ ~(по закону де Моргана и теореме 5) $\neg A\&\neg B\sim$ (по индукционному допущению и теореме 5) $A^X\&B^X\sim$ (по определению операции 'крест') $(A\vee B)^X\sim E^X$.

c) E≡¬A: тогда A≡P, $\neg E\equiv\neg\neg P\equiv P$ и $E^X\equiv P$, ч.т.д.

ТЕОРЕМА 7 (*Принцип двойственности*). Пусть формулы E, F такого же вида, как в теореме 6. Формулы E′, F′, полученные из E,F одновременной заменой всюду & на ∨ и ∨ на &, называются двойственными к формулам E, F, соответственно. Имеют место следующие утверждения:

a) Если $\models\neg E$, то $\models E'$. b) Если $\models E$, то $\models\neg E'$.
c) Если $\models E\sim F$, то $\models E'\sim F'$. d) Если $\models E\to F$, то $\models F'\to E'$.

Доказательство.

a): $\models\neg E$ (допущение)
$\models\neg E\sim E^X$ (теорема 6)
$\models E^X$ (следствие из теоремы 5)
$\models(E^X)^P_{\neg P}$ (теорема 1);
$\models((E^X)^P_{\neg P})^{\neg\neg P}_P$ (следствие из теоремы 5),т.е. $\models E'$.

b): $\models E$ (допущение)
$\models\neg\neg E$ (следствие теоремы 5)
$\models\neg(\neg E)\sim\neg(E^X)$ (теорема 6 и теорема 5)
$\models\neg(E^X)$ (следствие из теоремы 5)
$\models(\neg(E^X))^P_{\neg P}$ (теорема 1)
$\models\neg(E^X)^P_{\neg P}$ (по определению операции подстановки)
$\models(\neg(E^X)^P_{\neg P})^{\neg\neg P}_P$ (следствие из теоремы 5)
$\models\neg((E^X)^P_{\neg P})^{\neg\neg P}_P$ (по определению операции замены), т.е. $\models\neg E'$.

Назовем формулу B *логическим следствием формул* $A_1,A_2,...,A_m$ *(m≥1)*

(обозначается $A_1,A_2,...,A_m|=B$**),** *если в таблице истинности в строках, где формулы* $A_1,A_2,...,A_m$ *(посылки) одновременно истинны, истинна также и формула* B *(заключение).*

ТЕОРЕМА 8. a) $A \models B$ т.и т.т., когда $\models A \to B$.

b) $A_1,A_2,...,A_{m-1},A_m \models B$ т.и т.т., когда $A_1,A_2,...,A_{m-1} \models A_m \to B$ $(m \geq 1)$.

Следствие. $A_1,A_2,...,A_{m-1},A_m \models B$ т.и т.т.,когда $\models A_1 \to (...(A_{m-1} \to (A_m \to B))...)$ $(m \geq 1)$.

Упражнение

1. Применяя теорему 5 и известные эквивалентности, упростить формулы:

a) $(A \leftrightarrow B)\&(A \vee B)$; b) $(A \to B)\&(B \to \neg A)\&(C \to A)$; c) $\neg(\neg A\&\neg B) \vee ((A \to B)\&A)$.

2. Расположите формулы в порядке их логического следования:

$(A \to B) \vee A$; $\neg(A \to B)\&\neg(B \to A)$; $\neg(A \leftrightarrow B)$; $\neg(A\&B)$; $\neg A\&B$.

3. Методом от противного проверьте, верны ли следующие отношения логического следования:

a) $F \to G,\ K \to \neg H,\ H \vee \neg G \models F \to \neg K$;

b) $F \to (\neg K \to M),\ (\neg H \ \&\ L) \to \neg Q,\ Q \to F \models (F\&L) \to \neg M$.

1.2. Приложения алгебры высказываний

1.2.1. Функции алгебры высказываний (булевы функции)

Функцией алгебры высказываний (булевой функцией) называется n-местная операция на множестве $\{0,1\}$.

А л ф а в и т: (1) $x,y,...,x_1,x_2,...$ - предметные переменные;

(2) $f,g,...,f_1,f_2,...$ функциональные символы.

Т е р м: (1) $x,y,...,x_1,x_2,...$ - предметные переменные являются термами;

(2) если $f^{(n)}$ -функциональный символ, $t_1,...,t_n$ - термы, то $f^{(n)}(t_1,...,t_n)$ - терм.

Значение терма: **(**1) если t - предметная переменная x, то зн $t = \gamma(x)$;

(2) если $t = f^{(n)}(t_1,...,t_n)$, то зн $t = f^{(n)}$(зн t_1,..., зн t_n).

Функция $f^{(n)}(x_1,...,x_n)$ *представима термом* $t(v_1, ..., v_m)$, если $\{v_1, ..., v_m\} \subseteq \{x_1,...,x_n\}$ и $t[\gamma] = f^{(n)}[\gamma]$ для всех интерпретаций $\gamma : \{x_1,...,x_n\} \Rightarrow \{0,1\}$.

ТЕОРЕМА. Для каждой формулы A алгебры высказываний существует функция алгебры высказываний f(A) такая, что $A_1 \sim A_2 \Leftrightarrow f(A_1) = f(A_2)$.

Функция f *есть суперпозиция функций* $f_1, ..., f_m$, если f представима термом, все функциональные символы которого содержатся среди $f_1,...,f_m$.

Система функций $\mathfrak{R}$ *называется полной,* если любая функция алгебры высказываний может быть представлена суперпозицией функций из $\mathfrak{R}$.

Назовем *элементарной конъюнкцией (дизъюнкцией)* произвольную конъюнкцию (дизъюнкцию), составленную из пропозициональных букв или их отрицаний. *Дизъюнктивной нормальной формой* (д.н.ф.) называют дизъюнкцию элементарных конъюнкций. *Совершенной дизъюнктивной нормальной формой* (с.д.н.ф.) называется дизъюнктивная нормальная форма, каждая элементарная конъюнкция которой содержит все пропозициональные буквы (возможно с отрицанием), входящие в формулу.

ТЕОРЕМА. Всякая выполнимая (опровержимая) формула эквивалентна подходящей с.д.н.ф. (с.к.н.ф.)[1].

Доказательство теоремы следует из более общей формулы разложения функции по части входящих в нее переменных :

$$f(x_1,...,x_n) = \bigvee_{(\sigma_1,...,\sigma_m)} x_1^{\sigma_1}\&...\&x_m^{\sigma_m} \& f(\sigma_1,...,\sigma_m, x_{m+1},...,x_n),$$

где $\sigma_i \in \{0,1\}$, $x_i^0 = \neg x_i$, $x_i^1 = x_i$ $(i = 1,...,m)$.

В частности, $$f(x_1,...,x_n) = \bigvee_{f(\sigma_1,...,\sigma_n)=1} x_1^{\sigma_1}\&...\&x_n^{\sigma_n}.$$

Упражнение

1. Воспользовавшись формулой, разложить функцию $(x\to y\&z)\&x$ по переменным x, z.

Решение:

$(x\to y\&z)\&x = (x^0\&z^0\&((0\to y\&0)\&0))\vee(x^0\&z^1\&((0\to y\&1)\&0))\vee$
$(x^1\&z^0\&((1\to y\&0)\&1))\vee(x^1\&z^1\&((1\to y\&1)\&1)) =$
$= (\neg x\&\neg z\&o)\vee(\neg x\&z\&0)\vee(x\&\neg z\&0)\vee(x\&z\&y) = (x\&y\&z)$.

2. Используя истинностную таблицу функции f = (11100101), получить ее с.д.н.ф.

Решение:

x	y	z	f
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

$f(x,y,z) = (\neg x\&\neg y\&\neg z)\vee(\neg x\&\neg y\&z)\vee(\neg x\&y\&\neg z)\vee (x\&\neg y\&z)\vee(x\&y\&z)$.

3. Определим *конъюнктивную нормальную форму* (к.н.ф.) как конъюнкцию элементарных дизъюнкций. Аналогично определяется *совершенная конъюнктивная нормальная форма* (с.к.н.ф.) Используя понятие двойственной формулы, получить формулу для с.к.н.ф. :

$$f(x_1,...,x_n) = \&_{f(\sigma_1,...,\sigma_n)=0} x_1^{\neg\sigma_1} \vee ... \vee x_n^{\neg\sigma_n},$$

где $\sigma_i \in \{0,1\}$, $x_i^0 = \neg x_i$, $x_i^1 = x_i$ $(i = 1,...,n)$.

[1] определение в упр.3

4. Найти формулы F(x,y,z) так, чтобы выполнялось следующее отношение логического следования:

$$x \to y,\ F(x,y,z) \models x\&\neg z.$$

5. Доказать: если система функций (1) полна и каждая функция системы (2) выражается в виде формулы через функции системы (1), то система (2) полна.

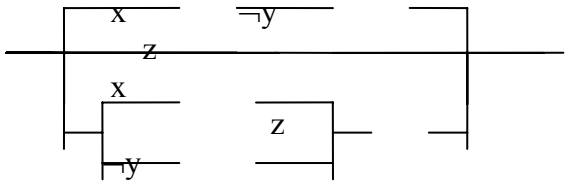
Доказать полноту систем: $\{\neg, \&, \vee\}$, $\{|\}$, $\{\downarrow\}$ [*)].

*) $x|y = \neg(x\&y)$ (штрих Шеффера), $x\downarrow y = \neg(x \vee y)$ (стрелка Пирса)

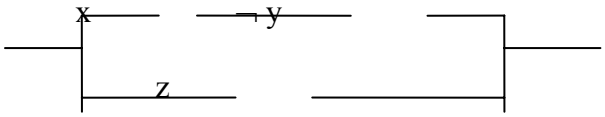
1.2.2. Метод синтеза релейно - контактных схем

Проинтерпретируем булевы функции как электрические сети, содержащие двухпозиционные переключатели x, $\neg x$ - соответственно, замыкающий и размыкающий контакты; &, $\vee$ - соответственно, последовательное и параллельное соединения контактов; 1 и 0 - соответственно, «ток прохо- дит» и «ток не проходит». Две цепи называются эквивалентными, если через одну из них ток проходит т.и т.т, когда он проходит через другую.

Пример 1. Упростить следующую релейно-контактную схему, получив ее функцию проводимости, и минимизировать ее.

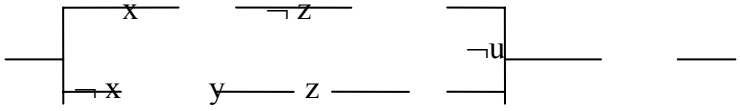


Решение: $(x,y,z) = (x\&\neg y) \vee z \vee ((x \vee \neg y)\&z)) = (x\&\neg y) \vee z$



Пример 2. Используя с.д.н.ф.(с.к.н.ф.), найти формулу для функции проводимости f и начертить соответствующую ей релейно-контактную схему, если $f(1,0,0,0) = f(1,1,0,0) = f(0,1,1,0) = 1$.

Решение: $f(x,y,z,u) = (x\&\neg y\&\neg z\&\neg u) \vee (x\&y\&\neg z\&\neg u) \vee (\neg x\&y\&z\&\neg u) =$
$((x\&\neg z\&\neg u)\&(\neg y \vee y)) \vee (\neg x\&y\&z\&\neg u) = (x\&\neg z\&\neg u) \vee (\neg x\&y\&z\&\neg u) =$.
$((x\&\neg z) \vee (\neg x\&y\&z))\&\neg u.$



Пример 3. Имеется одна лампочка в лестничном пролете двухэтажного дома. Постройте схему так, чтобы на каждом этаже своим выключателем можно было бы гасить и зажигать лампочку.

Решение. Функция проводимости такой схемы меняет свои значения, если меняет значение один из ее аргументов: $f(0,0) = f(1,1) = 1$, $f(0,1) = f(1,0) = 0$.

Воспользовавшись с.д.н.ф., получим функцию $f(x,y) = (x\&y) \vee (\neg x\&\neg y)$.

1.2.3. Приложение в теории множеств

Множеством называют вполне определенную совокупность различаемых объектов. Например, множество ‘всех книг данной библиотеки’, или множество ‘всех людей, живших в XX веке’.

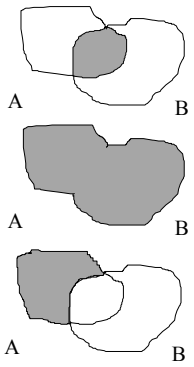
Имеются два способа задания множеств: (1) путем явного перечисления его элементов, например, целые числа между 0 и 5, т.е. {0,1,2,3,4,5};
(2) указанием свойства, определяющего принадлежность элемента данному множеству, т.е. {x; φ (x)}.

Рассмотрим язык, предназначенный для описания свойств множеств.
А л ф а в и т содержит переменные x,y,z,..., пробегающие множества, символ принадлежности ‘$\in$’ и символы логики высказываний.
Т е р м ы и ф о р м у л ы определим одновременно:

1. x,y,z,... - предметные переменные, пробегающие множества, - термы;
2. если t, r - термы, то $t \in r$ элементарная формула (атом) ;
3. если φ, ψ - формулы, то $\varphi\&\psi$, $\varphi\vee\psi$, $\neg\varphi$, $\varphi \to \psi$, $\varphi \leftrightarrow\psi$ - формулы;
4. если x - переменная, и φ - формула, то {x; φ(x)} - терм.

Определим *операции (пересечение, объединение, разность, дополнение) и отношения (включение, равенство) над множествами* (для удобства объекты-множества будем обозначать заглавными буквами, а объекты, являющиеся элементами множеств, малыми буквами):

1. $A\bigcap B = \{x : x \in A \& x \in B\}$
   $x \in A\bigcap B \Leftrightarrow x \in A \& x \in B$



2. $A\bigcup B = \{x : x \in A \vee x \in B\}$
   $x \in A\bigcup B \Leftrightarrow x \in A \vee x \in B$

3. $A \setminus B = \{x : x \in A \& x \notin B\}$
   $x \in A \setminus B \Leftrightarrow x \in A \& \neg(x \in B)$

4. $A \subset B \Leftrightarrow \forall^{1)}x\ (x \in A \to x \in B)$
5. $A = B \Leftrightarrow \forall x\ (x \in A \leftrightarrow x \in B)$
6. $U = \{x : x = x\}$, $\varnothing = \{x : x \neq x\}$
7. $\overline{A} = \{x : x \in U \& x \notin A\}$

(перечеркнутые символы = и $\in$ означают, что соответствующие = - и $\in$ - отношения не имеют места).

Свойства операций и отношений

1) $A\bigcap B = B\bigcap A$, $A \bigcup B = B \bigcup A$
2) $(A \bigcap B)\bigcap C = A \bigcap(B \bigcap C)$, $(A \bigcup B)\bigcup C = A \bigcup(B \bigcup C)$

[1] Квантор всеобщности

3) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

4) $A \subset A \cup B$, $A \cap B \subset A$, $A \setminus B \subset A$, $A \cap A = A$, $A \cup A = A$,
$\overline{\overline{A}} = A$, $\varnothing \subset A$, $A \subset U$, $A \setminus \varnothing = A$

5) $A \subset B \leftrightarrow A \cup B = B \leftrightarrow A \cap B = A$

6) $A \subset B \ \& C \subset D \rightarrow A \cup C \subset B \cup D$

$A \subset B \ \& C \subset D \rightarrow A \cap C \subset B \cap D$

$A \subset B \ \& C \subset D \rightarrow A \setminus D \subset B \setminus C$

Можно заметить, что существует тесная связь, между множествами и высказываниями, между операциями над множествами и логическими операциями. Пусть мы имеем несколько высказываний. Образуем множество всех логических возможностей для рассматриваемых высказываний и назовем его универсальным множеством. Поставим каждому высказыванию в соответствие подмножество тех логических возможностей универсального множества, для которых это высказывание истинно - его множество истинности. Очевидно, что множествами истинности высказываний $P\&Q$, $P \vee Q$, $\neg P$ будут, соответственно, множества $P \cap Q$, $P \cup Q$, $\overline{P}$, где P, Q - множества истинности высказываний P, Q.
Пусть булева функция $f(x_1,...,x_n)$ представима термом, содержащим только логические символы $\&, \vee, \neg$. Обозначим через $f^{\in}(x)$ формулу теории множеств, полученную из терма f подстановками вместо переменных $x_1,..., x_n$ формул $x \in A_1,..., x \in A_n$, соответственно. Обозначим через Z_f выражение, полученное из терма для $f(x_1,..., x_n)$ заменой переменных $x_1,...,x_n$ символами $Z_1,...,Z_n$, и символов $\&, \vee, \neg$ символами $\cap$, $\cup$, $\overline{}$, соответственно. При интерпретации Z_f символы Z_i будут обозначать подмножества универсума U (множества, содержащего в качестве подмножеств все другие множества).

Упражнение

1. Доказать, пользуясь кругами Эйлера, что высказывание $P \ \& \ Q \rightarrow Q$ является тавтологией.
2. Используя истинностные таблицы соответствующих высказываний, проверить следующее свойство множеств: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

1.3. Аксиоматическая система в исчислении высказываний

А к с и о м а м и[1)] (классического) исчисления высказываний объявляем тавтологии из теоремы 2. В качестве единственного п р а в и л а в ы в о д а принимаем процедуру перехода от двух формул вида A, $A \rightarrow B$ (посылок) к формуле B (заключению):

$$\frac{A,\ A \rightarrow B}{B} \quad \text{(modus ponens)}$$

(Требования, которым должны удовлетворять правила вывода, – из истинных посылок должны получаться истинные заключения.)

[1] Схемами аксиом

Доказательством формулы Ф (теоремы) называют конечный список формул $B_1,...,B_l$, заканчивающийся формулой Ф ($Ф = B_l$), где каждая формула B_i ($i=1,...,l$) есть аксиома или получена из предыдущих формул по одному из правил вывода (обозначается $\vdash Ф$).

Пример 1 (*Доказательство теоремы*).
$\vdash A\to A$:
1. $A\to(A\to A)$ (аксиома 1а)
2. $A\to((A\to A)\to A)$ (аксиома 1а)
3. $(A\to(A\to A))\to((A\to((A\to A)\to A))\to(A\to A))$ (аксиома 1б)
4. $(A\to((A\to A)\to A))\to(A\to A)$ (modus ponens, 2,3)
5. $A\to A$ (modus ponens, 1,4)

Выводом формулы Ф из гипотез $A_1, ..., A_m$ ($m \geq 1$) называют конечный список формул $B_1,...,B_l$, заканчивающийся формулой Ф ($Ф = B_l$), где каждая формула B_i ($i=1,...,l$) есть аксиома или одна из гипотез $A_1,... ,A_m$,
или получена из предыдущих формул по правилу вывода ($A_1,... ,A_m \vdash Ф$).

Пример 2 (*Вывод формулы из гипотез*). $A\&B\to C, A \vdash B\to C$:
1. $A\&B\to C$ (гипотеза)
2. $(B\to A\&B) \to ((B\to(A\&B\to C)) \to(B\to C))$ (аксиома 1б)
3. $(A\&B\to C) \to(B\to(A\&B\to C))$ (аксиома 1а)
4. $B\to(A\&B\to C)$ (modus ponens,1,3)
5. A (гипотеза)
6. $A \to(B\to A\&B)$ (аксиома 2)
7. $B\to A\&B$ (modus ponens,5,6)
8. $(B\to(A\&B\to C)) \to(B\to C)$ (modus ponens,7,2)
9. $B\to C$ (modus ponens,4,8)

ТЕОРЕМА 9 (*Свойства вывода)*
1. $A_1,...,A_m \vdash A_i$ ($i=\overline{1,m}$)
2. $A_1,...,A_m \vdash B_j$ ($j=\overline{1,k}$) и $B_1,...,B_k \vdash C \Rightarrow A_1,...,A_m \vdash C$
3. $A_1,... ,A_i, ..., A_j, ..., A_m \vdash B \Rightarrow A_1,...,A_j, ..., A_i, ..., A_m \vdash B$.
4. $A_1, ..., A_m \vdash B \Rightarrow A_1, ..., A_m , A_{m+1} \vdash B$.

ТЕОРЕМА 10. (1) Если $\vdash A\to B$, то $A \vdash B$.
(2) Если $A_{1, ... , }A_{m-1} \vdash A_m\to B$, то $A_{1, ... , }A_m \vdash B$ ($m\geq 1$).

Следствие. Если $\vdash A_1\to(A_2\to ... (A_m\to B) ...)$, то $A_1, ..., A_m \vdash B$ ($m\geq 1$).

ТЕОРЕМА 11 *(О дедукции*). (1) Если $A \vdash B$, то $\vdash A\to B$.
(2) Если $A_1, ..., A_m \vdash B$, то $A_1, ..., A_{m-1} \vdash A_m\to B$ ($m\geq 1$).
Доказательство (2):

Формулы данного вывода (I):$A_1,..., A_m \vdash B$ обозначим списком $B_1, ..., B_l$. Переделаем вывод (I) в схему :

$A_m \to B_1$

. . .

$A_m \to B_i$

. . .

$A_m \to B_l$,

а затем в вывод (11), обосновав выводимость каждой импликации $A_m \to B_i$ (i=1,...,l) из списка гипотез $A_1,...,A_{m-1}$.

1случай: Если B_i есть аксиома или одна из гипотез A_j (j=1,...,m-1) в вы воде (I), то B_i также входит и в вывод (II), так что вхождение импликации $A_m \to B_i$ в вывод (II) имеет обоснование с помощью аксиомы 1а:

B_i

$Bi \to (A_m \to B_i)$ (аксиома 1а)

$A_m \to B_i$ (modus ponens)

2 случай: Если B_i есть гипотеза A_m в выводе (I), то доказательство импликации $A_m \to A_m$ приведено в примере 1.

3 случай: B_i получена в выводе (I) из предыдущих формул B_p, $B_q = B_p \to B_i$ по правилу modus ponens. Обоснование вхождения импликации $A_m \to B_i$ в вывод (II) проводится с помощью аксиомы 1б индукцией по построению вывода (11) :

. . .

$A_m \to B_p$ (по индукционному допущению)

. . .

$A_m \to (B_p \to B_i)$ (по индукционному допущению)

$(A_m \to B_p) \to ((A_m \to (B_p \to B_i)) \to (A_m \to B_i))$ (аксиома 1б)

$(A_m \to (B_p \to B_i)) \to (A_m \to B_i)$ (modus ponens)

$A_m \to B_i$ (modus ponens)

Пример, иллюстрирующий доказательство теоремы о дедукции :

Если $A \to B$, $C \to A$, $C \vdash B$, то $A \to B$, $C \to A \vdash C \to B$.

Вывод (I):

1. $A \to B$ (гипотеза из списка $A_1,...,A_{m-1}$)
2. $C \to A$ (гипотеза из списка $A_1,...,A_{m-1}$)
3. C (гипотеза A_m)
4. A (modus ponens, 3,2)
5. B (modus ponens, 4,1)

Вывод (II):

$A \to B$ (гипотеза из списка $A_1,...,A_{m-1}$)

$(A \to B) \to (C \to (A \to B))$ (аксиома 1а)

1^* $C \to (A \to B)$ (modus ponens)

$C \to A$ (гипотеза из списка $A_1,...,A_{m-1}$)

$(C\to A)\to(C\to(C\to A))$ (аксиома 1а)

2^* $C\to(C\to A)$ (modus ponens)

$C\to(C\to C)$ (аксиома 1а)

$(C\to(C\to C))\to((C\to((C\to C)\to C))\to(C\to C))$ (аксиома 1б)

$(C\to((C\to C)\to C))\to(C\to C)$ (modus ponens)

$C\to((C\to C)\to C)$ (аксиома 1а)

3^* $C\to C$ (modus ponens)

$(C\to C)\to((C\to(C\to A))\to(C\to A))$ (аксиома 1б)

$(C\to(C\to A))\to(C\to A)$ (modus ponens)

4^* $C\to A$ (modus ponens)

$(C\to A)\to((C\to(A\to B))\to(C\to B))$ (аксиома 1,б)

$(C\to(A\to B))\to(C\to B)$ (modus ponens)

5^* $C\to B$ (modus ponens)

Следствие. Если $A_1,...,A_m \vdash B$, то $\vdash A_1\to(A_2\to...(A_m\to B)...)$ $(m\geq 1)$.

ТЕОРЕМА 12 *(Непротиворечивость исчисления высказываний*). Всякая доказуемая формула общезначима, т.е., если $\vdash B$, то $\models B$.

Доказательство следует из того, что аксиомы выбираются среди тавтологий, а правила вывода сохраняют истинность заключения при истинных посылках.

Следствие. Не существует формулы B, такой, что $\vdash B$ и $\vdash \neg B$.

ТЕОРЕМА 13 *(Производные правила вывода).*

Аксиомы:

$A \,\&\, B \to A$

$A \,\&\, B \to B$

$A \to (B \to A \,\&\, B)$

$A \to A \vee B$

$B \to A \vee B$

$(A\to C)\to((B\to C)\to(A\vee B\to C))$

$(A\leftrightarrow B)\to(A\to B),\ (A\leftrightarrow B)\to(A\to B)$

$(A\to B)\to((B\to A)\to(A\leftrightarrow B))$

$\neg\neg A\to A$

$(A\to B)\to((A\to\neg B)\to\neg A)$

Производные правила вывода:

$\dfrac{A \,\&\, B}{A};\ \dfrac{A \,\&\, B}{B}$ (удаление &)

$\dfrac{A, B}{A \,\&\, B}$ (введение &)

$\dfrac{A}{A \vee B};\ \dfrac{B}{A \vee B}$ (введение $\vee$)

$\dfrac{A \vdash C,\ B \vdash C}{A \vee B \vdash C}$ (удаление $\vee$)

$\dfrac{A\leftrightarrow B}{A\to B};\ \dfrac{A\leftrightarrow B}{B\to A}$ (удаление $\leftrightarrow$)

$\dfrac{A\to B,\ B\to A}{A\leftrightarrow B}$ (введение $\leftrightarrow$)

$\dfrac{\neg\neg A}{A}$ (удаление $\neg$)

$\dfrac{A \vdash B,\ A \vdash \neg B}{\vdash \neg A}$ (введение $\neg$)

$A\to(\neg A\to C)$ $\qquad\qquad$ $\dfrac{A,\neg A}{C}$ (слабое удаление $\neg$)

Доказательство.

1) $\dfrac{\neg\neg A}{A}$:

$\neg\neg A$ (допущение)

$\neg\neg A\to A$ (аксиома)

A (modus ponens)

3) $\dfrac{A|-B,\ A|-\neg B}{|-\neg A}$ (введение $\neg$)

A (допущение)

•••

B (из первой посылки)

$A\to B$ (теорема о дедукции)

A (допущение)

2) $A,\neg A\ |-C$:

$\neg C,A,\neg A\ |-\ A$ (теорема 9(1))

$\neg C,A,\neg A\ |-\ \neg A$ (теорема 9(1))

$A,\ \neg A\ |-\ \neg\neg C$ (введение $\neg$)

$A,\neg A\ |-\ C$ (удаление $\neg$)

•••

$\neg B$ (из второй посылки)

$A\to \neg B$ (теорема о дедукции)

$(A\to B)\to((A\to \neg B)\to \neg A)$

$\neg A$ (modus ponens 2раза)

Примеры построения доказательств

1) ***Первый закон де Моргана*** **:** $|-\neg(A\vee B)\sim\neg A\&\neg B$:

$\neg(A\vee B),A\ |-\ \neg(A\vee B)$ $\qquad$ $\neg(A\vee B),\ B\ |-\ \neg(A\vee B)$

$\neg(A\vee B),A\ |-\ A\vee B$ $\qquad$ $\neg(A\vee B),\ B\ |-\ A\vee B$

$\neg(A\vee B)\ |-\ \neg A$ $\qquad$ $\neg(A\vee B)\ |-\ \neg B$

$\neg(A\vee B)\ |-\ \neg A\&\neg B$

$|-\ \neg(A\vee B)\to\neg A\&\neg B$

$\neg A\&\neg B,A\ |-\ A$ $\qquad$ $\neg A\&\neg B,\ B\ |-\ B$

$\neg A\&\neg B,A\ |-\ \neg A$ $\qquad$ $\neg A\&\neg B,\ B\ |-\ \neg B$

$\neg A\&\neg B,A\ |-\ \neg(A\vee B)$ $\qquad$ $\neg A\&\neg B,\ B\ |-\ \neg(A\vee B)$

$\neg A\&\neg B,A\vee B\ |-\ \neg(A\vee B)$

$\neg A\&\neg B,A\vee B\ |-\ (A\vee B)$

$\neg A\&\neg B\ |-\ \neg(A\vee B)$

$|-\ \neg A\&\neg B\to\neg(A\vee B)$

$|-\ \neg(A\vee B)\sim\neg A\&\neg B$

2) $|-A\to B\sim\neg A\vee B$

1. $A\to B$ (допущение)
2. $\neg(\neg A\vee B)$ (допущение противного)

3. $\neg(\neg A \vee B) \sim \neg\neg A \& \neg B$ (1-ый закон де Моргана)

4. $\neg(\neg A \vee B) \rightarrow \neg\neg A \& \neg B$ (удаление $\sim$, 3)

5. $\neg\neg A \& \neg B$ (удаление $\rightarrow$, 2,4)

6. $\neg\neg A$ (удаление &,5)

7. A (удаление $\neg$,6)

8. B (удаление $\rightarrow$,7,1)

9. $\neg B$ (удаление &, 5)

10. $\neg\neg (\neg A \vee B)$ (введение $\neg$, 2,8,9)

11. $(\neg A \vee B)$ (удаление $\neg$, 10)

12. $(A \rightarrow B) \rightarrow \neg A \vee B$ (теорема о дедукции, 1,11)

13. $\neg A \vee B$ (допущение)

14. A (допущение)

15a. $\neg A$ (допущение) 15b. B (допущение)

16a. B (слабое удаление $\neg$)

17. B (удаление $\vee$, 13)

18. $A \rightarrow B$ (теорема о дедукции, 14,17)

19. $\neg A \vee B \rightarrow (A \rightarrow B)$ (теорема о дедукции, 11,18)

20. $(A \rightarrow B) \sim \neg A \vee B$ (введение $\sim$, 12,19)

3) ***Второй закон де Моргана*** **:** $\vdash \neg(A \& B) \sim \neg A \vee \neg B$

$\neg(A \& B), A, B \vdash A \& B$ (введение &)

$\neg(A \& B), A, B \vdash \neg(A \& B)$ (теорема 9(1))

$\neg(A \& B), A \vdash \neg B$ (введение $\neg$)

$\neg(A \& B) \vdash A \rightarrow \neg B$ (теорема о дедукции)

$\vdash (A \rightarrow \neg B) \sim \neg A \vee \neg B$ (теорема из примера 2)

$\vdash (A \rightarrow \neg B) \rightarrow \neg A \vee \neg B$ (удаление $\sim$)

$(A \rightarrow \neg B) \vdash \neg A \vee \neg B$ (теорема 10(1))

$\neg(A \& B) \vdash \neg A \vee \neg B$ (теорема 9(2))

$\vdash \neg(A \& B) \rightarrow \neg A \vee \neg B$ (теорема о дедукции)

$\neg A, A \& B \vdash \neg A$ $\neg B, A \& B \vdash \neg B$ (теорема 9(1))

$\neg A, A \& B \vdash A$ $\neg B, A \& B \vdash B$ (удаление &)

$\neg A \vdash \neg(A \& B)$ $\neg B \vdash \neg(A \& B)$ (введение $\neg$)

$\neg A \vee \neg B \vdash \neg(A \& B)$ (удаление $\vee$)

$\vdash \neg A \vee \neg B \rightarrow \neg(A \& B)$ (введение$\rightarrow$)

$\vdash \neg A \vee \neg B \sim \neg(A\&B)$ (введение ~)

4) ***Первый закон дистрибутивности*:** $\vdash A\&(B\vee C) \sim (A\&B)\vee(A\&C)$:

1. $A\&(B\vee C)$ (допущение)
2. A (удаление &)
3. $B\vee C$ (удаление &)

4а. B (допущение) 4б. C (допущение)
5а. A&B (введение &) 5б. A&C (введение &)
6а. $(A\&B)\vee(A\&C)$ (введение $\vee$) 6б. $(A\&B)\vee(A\&C)$ (введение $\vee$)

7. $(A\&B)\vee(A\&C)$ (удаление $\vee$, 3)
8. $A\&(B\vee C)\rightarrow(A\&B)\vee(A\&C)$ (теорема дедукции,1,7)
9. $(A\&B)\vee(A\&C)$ (допущение)

10а. A&B (допущение) 10б. A&C (допущение)
11а. A (удаление &) 11б A (удаление &)
12а. B (удаление &) 12б. C (удаление &)
13а. $B\vee C$ (введение $\vee$) 13б. $C\vee B$ (введение $\vee$)
14а. $A\&(B\vee C)$ (введение &) 14б. $A\&(B\vee C)$ (введение &)

15. $A\&(B\vee C)$ (удаление $\vee$,9)
16. $(A\&B)\vee(A\&C)\rightarrow A\&(B\vee C)$ (теорема дедукции,9,15)
17. $A\&(B\vee C) \sim (A\&B)\vee(A\&C)$ (введение ~)

5). Для множеств A,B,C верно утверждение $\vdash A\cap B \subset C \leftrightarrow A\subset \overline{B}\cup C$:

1. $A\cap B \subset C$ (допущение)
2. $x \in A\cap B \rightarrow x \in C$
3. $x\in A$ (допущение)
4. $\neg (x\in \overline{B}\cup C)$ (допущение противного)
5. $\neg(x\in \overline{B} \vee x\in C)$
6. $\neg(x\in \overline{B})\&\neg(x\in C)$ (закон де Моргана)
7. $\neg(x\in \overline{B})$ (удаление &)
8. $\neg(x\in C)$
9. $x\in B$

10. $x\in A\&x\in B$ (введение &)
11. $x\in A\cap B$
12. $x\in C$ (modus ponens,11,2)
13. $\neg\neg(x\in \overline{B}\cup C)$ (введение $\neg$,12,8)
14. $x\in \overline{B}\cup C$ (удаление $\neg$,13)
15. $x\in A\rightarrow x\in \overline{B}\cup C$ (введение $\rightarrow$,3,14)
16. $A\subset \overline{B}\cup C$
17. $A\cap B \subset C \rightarrow A\subset \overline{B}\cup C$(введение $\rightarrow$)

18. $A\subset \overline{B}\cup C$ (допущение)
19. $x\in A \rightarrow x\in \overline{B}\cup C$
20. $x\in A\cap B$ (допущение)
21. $x\in A\&x\in B$
22. $x\in A$ (удаление &)
23. $x\in B$ (удаление &)
24. $x\in \overline{B}\cup C$ (удаление $\rightarrow$,22,18)
25. $x\in \overline{B}\vee x\in C$

26а.$x\in \overline{B}$ (допущение) 26б.$x\in C$(допущение)

27а. $x\in C$ (сл. уд.$\neg$,23,26а)

28. $x\in C$ (удаление $\vee$,25)
29. $x\in A\cap B \rightarrow x\in C$
30. $A\cap B\subset C$
31. $A\subset \overline{B}\cup C \rightarrow A\cap B\subset C$
32. $A\cap B \subset C \leftrightarrow A\subset \overline{B}\cup C$

ТЕОРЕМА 14*(Теорема о полноте исчисления высказываний).* $\models E \Rightarrow \vdash E$.

Доказательство будет получено с помощью следующих лемм:

ЛЕММА 1. Для каждой из логических связок имеют место выводимости:

A	B	A&B		A∨B		¬A	
И	И	И	$A, B \vdash A\&B$	И	$A, B \vdash A\vee B$	Л	$A \vdash \neg\neg A$
И	Л	Л	$A, \overline{B} \vdash \overline{A\&B}$	И	$A, \overline{B} \vdash A\vee B$	Л	$A \vdash \neg\neg A$
Л	И	Л	$\overline{A}, B \vdash \overline{A\&B}$	И	$\overline{A}, B \vdash A\vee B$	И	$\neg A \vdash \neg A$
Л	Л	Л	$\overline{A}, \overline{B} \vdash \overline{A\&B}$	Л	$\overline{A}, \overline{B} \vdash \overline{A\vee B}$	И	$\neg A \vdash \neg A$

Доказательство.

$\overline{A}, B \vdash \overline{A\&B}$:

1. $\overline{A}$ (допущение)
2. B (допущение)
3. A&B (допущение противного)
4. A (удаление &, 3)
5. $\overline{A\&B}$ (введение ¬)

$\overline{A}, \overline{B} \vdash \overline{A\vee B}$:

1. $\overline{A}$ (допущение)
2. $\overline{B}$ (допущение)
3. A∨B (допущение противного)

4а. A (допущение) 4б. B (допущение)

5а. $\overline{A\vee B}$ (сл. уд.¬) 5б. $\overline{A\vee B}$ (сл.уд. ¬)

6. $\overline{A\vee B}$ (удаление ∨,3)
7. $\overline{A\vee B}$ (введение ¬, 3, 6)

ЛЕММА 2. Соответствующий вывод имеется для любой интерпретации (строки таблицы истинности) любой формулы.

Доказательство на примере формулы P→(Q∨R→(R→¬P)):

P	Q	R	Q∨R	¬P	R→¬P	Q∨R→ (R→¬P)	P→ (Q∨R→ (R→¬P))
0	0	0	0	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	1	1	1	1
0	1	1	1	1	1	1	1
1	0	0	0	0	1	1	1
1	0	1	1	0	0	0	0
1	1	0	1	0	1	1	1
1	1	1	1	0	0	0	0

для шестой строки:

1. P,¬Q,R |– Q∨R (лемма 1)
2. P,¬Q,R |– ¬¬P (лемма 1)
3. P,¬Q,R |– R→¬P (допущение противного)
4. P,¬Q,R |– ¬P (*)
5. P,¬Q,R |– ¬(R→¬P) (введение ¬,3)
6. P,¬Q,R |– Q∨R→(R→¬P) (допущение противного)
7. P,¬Q,R |– R→¬P (теорема 1(2))
8. P,¬Q,R |– ¬P (*)
9. P,¬Q,R |– ¬ (Q∨R→(R→¬P)) (введение ¬,6)
10. P,¬Q,R |– P→(Q∨R→(R→¬P)) (допущение противного)
11. P,¬Q,R |– Q∨R→(R→¬P) (*)
12. P,¬Q,R |– R→¬P (теорема 1(2))
13. P,¬Q,R |– ¬P (*)
14. P,¬Q,R |– ¬ (P→(Q∨R→(R→¬P))) (введение ¬,10)

ЛЕММА 3. Если |= E[P_1,...,P_n], где P_1,...,P_n список всех переменных, входящий в формулу E, то $P_1 \vee \neg P_1$,..., $P_n \vee \neg P_n$ |– E.

Д о к а з а т е л ь с т в о проведем на примере формулы E[P_1,P_2]:

P_1	P_2	E(P_1, P_2)		
0	0	1	$\overline{P_1}, \overline{P_2} \mid - E$	$\overline{P_1}, P_2 \vee \overline{P_2} \mid - E$
0	1	1	$\overline{P_1}, P_2 \mid - E$	
1	0	1	$P_1, \overline{P_2} \mid - E$	$P_1, P_2 \vee \overline{P_2} \mid - E$
1	1	1	$P_1, P_2 \mid - E$	

$P_1 \vee \overline{P_1}, P_2 \vee \overline{P_2} \mid - E$

ЛЕММА 4. |– A∨¬A .

Д о к а з а т е л ь с т в о.

A, ¬(A∨¬A) |– A∨¬A (введение ∨)

A, ¬(A∨¬A) |– ¬(A∨¬A) (теорема 9(1)) •••

¬(A∨¬A) |– ¬A (введение ¬) ¬(A∨¬A) |– ¬¬A

– |– ¬¬(A∨¬A) (введение ¬)

|– A∨¬A (удаление ¬)

Д о к а з а т е л ь с т в о *теоремы о полноте:* Пусть |= E[P_1,...,P_n].

По лемме 3 существует вывод $P_1 \vee \neg P_1, \ldots, P_n \vee \neg P_n \mid - E$. Вставляя в этот вы- вод доказательство каждой из формул $P_i \vee \neg P_i$ (i=1,...,n), получим доказательство формулы E.

Г л а в а 2

ИСЧИСЛЕНИЕ ПРЕДИКАТОВ

2.1. Предикаты

В логике высказываний изучается структура сложных высказываний, составленных из элементарных неделимых высказываний. Логика предикатов анализирует субъектно-предикатную структуру простых суждений. Например, структура элементарного суждения «снег белый» может быть представлена предикатом (свойством) «быть белым» и субъектом «снег», а, к примеру, структура элементарного суждения «два делит пять» - предикатом «х делит у» и субъектами «два» и «пять».

Абстрагируясь от конкретного содержания предикатов и субъектов, будем называть *предикатами функции истинности* $J^{(n)}(x_1,...,x_n)$*, заданные на непустой области* D *(натуральных чисел) и принимающие значения во множестве* {И,Л}. Предикат $J^{(n)}(x_1,...,x_n)$ становится высказыванием после означивания входящих в него переменных на элементах множества D.

А л ф а в и т: (1) x,y,z,...,x_1,x_2,... - предметные переменные;
(2) $P^{(n)}(x_1,...,x_n)$,... - предикатные буквы (n=0,1,...);
(3) &, $\vee$, $\neg$, $\rightarrow$, $\leftrightarrow$, $\forall$, $\exists$ - логические связки и кванторы;
(4) (,) - вспомогательные символы.

Ф о р м у л ы: (1) $P^{(n)}(x_1,...,x_n)$, …- элементарные формулы или атомы;
(2) если A, B - формулы, то A&B, A$\vee$B, $\neg$A, A$\rightarrow$B, A$\leftrightarrow$B - формулы;
(3) если A(x) - формула со свободной переменной x, то $\forall$x A(x), $\exists$x A(x) - формулы.

Свободные и связанные вхождения переменных

Переменные, находящиеся в области действия квантора по этой переменной называются *связанными, иначе - свободными.*

Примеры:

1) $\sum_{n=0}^{\infty} \frac{x^n}{n!} = f(x)$: x - свободная переменная, n - связанная переменная.

2) $\int_0^y \sin x dx = f(y)$: y - свободная переменная, x - связанная переменная.

3) μx (rm(y, x)=0)=f(y): y - свободная переменная, x - связанная переменная.

4) $\forall y\, P(y)\ \&\ \exists x\, Q(x,z) \rightarrow \exists z\, (P(y,z) \vee Q(z))$: первое вхождение переменной y - связанное, второе – свободное; x - связанная переменная; первое вхождение переменной z - свободное, второе -связанное.

Значение формулы $E[P_1,...,P_m ; x_1,...,x_n]$ при интерпретации предикатных букв $\tau : P^{(n)} \Rightarrow J^{(n)}$ и означивании γ: $\{x_1,...,x_n\} \Rightarrow D$ $(D \neq \varnothing)$ предметных переменных, обозначается $E[\tau,\gamma]$, определим индукцией по построению формулы E :

1) $E = P^{(n)}(x_1,...,x_n)$, то $E[\tau,\gamma] = J[\gamma]$;
2) $E = (A\&B)[P_1,...,P_m ; x_1,...,x_n]$, то $E[\tau,\gamma] = A[\tau,\gamma]\ \&\ B[\tau,\gamma]$.

Аналогично для остальных логических связок.

3) $E=\forall x_1\, A[P_1,...,P_m;x_1,...,x_n]$, то $E[\tau,\gamma] = \forall x_1 A[\tau,x_1,\gamma]$=И, где $\gamma : \{x_2,...,x_n\} \Rightarrow D$, если $A[\tau,a,\gamma]$ = И для любого $a \in D$.
4) $E=\exists x_1 A[P_1,...,P_m; x_1,...,x_n]$, то $E[\tau,\gamma] = \exists x_1 A[\tau,x_1,\gamma]$ = И, где γ: $\{x_2,...,x_n\} \Rightarrow D$, если $A[\tau,a,\gamma]$ = И для некоторого $a \in D$.

Формула $E[P_1,...,P_m; x_1,...,x_n]$ называется о б щ е з н а ч и м о й и л и т а в т о л о г и е й, если для любой области $D \neq \varnothing$, для любых интерпретаций τ предикатных букв и любом означивании γ предметных переменных в области D, $E[\tau,\gamma]$ = И.

Сразу становится понятным, что проверка общезначимости для предикатных формул с помощью таблиц истинности невозможна. Однако можно говорить, соответственно, об 1-общезначимости, 2-общезначимости и т.д. предикатных формул.

Пример 1. Покажем, что формула $P(x,y) \rightarrow Q(x)$ не 1-общезначима, следовательно, не общезначима.

Решение. D={1} - одноэлементная область, I_1 и I_2 - интерпретации буквы P, а J_1 и J_2 - интерпретации буквы Q:

X	y	I_1	I_2	J_1	J_2
1	1	и	л	и	л

Истинностная таблица формулы $P(x,y) \rightarrow Q(x)$:

x	y	P(x,y)	Q(x)	$P(x,y) \rightarrow Q(x)$
1	1	и	и	и
1	1	и	л	л
1	1	л	и	и
1	1	л	л	и

Пример 2. Покажем, что формула $\forall x(\exists x\, P(x) \rightarrow P(x))$ не 2-общезначима.

Решение. D={1,2}, J_1, J_2, J_3, J_4 - интерпретации буквы P :

x	J_1	J_2	J_3	J_4
1	и	и	л	Л
2	и	л	и	Л

Истинностная таблица формулы $\forall x\,(\exists x\,P(x)\to P(x))$:

x	P(x)	$\exists x\,P(x)$	$\exists x\,P(x)\to P(x)$	$\forall x(\exists x P(x)\to P(x))$
1	J_1	И	И	И
2	J_1		И	
1	J_2	И	И	Л
2	J_2		Л	
1	J_3	И	Л	Л
2	J_3		И	
1	J_4	Л	И	И
2	J_4		И	

ПРИМЕР 3. Покажем, что формула $\forall x\,\exists y\,P(x,y)\to\exists y\,\forall x\,P(x,y)$ не общезначима.

Решение. Пусть $D=\{1,2\}$, тогда интерпретации предикатной буквы P(x,y) зададим следующей таблицей:

X	y	J_1	J_2	J_3	J_4	…	J_7	…
1	1	и	и	и	и	…	И	…
1	2	и	и	и	и	…	Л	…
2	1	и	и	л	л	…	Л	…
2	2	и	л	и	л	…	И	…

В частности, для интерпретации J_7 получим: при x=1: $\exists y\,J_7(1,y)\equiv$И;

при x=2: $\exists y\,J_7(2,y)\equiv$И, тогда $\forall x\,\exists y\,J_7(x,y)=$И. При y=1: $\forall x\,J_7(x,1)=$Л,

при y=2: $\forall x\,J_7(x,2)=$Л, тогда $\exists y\forall x\,J_7(x,y)=$Л.

Откуда $\forall x\,\exists y\,J_7(x,y)\to\exists y\,\forall x\,J_7(x,y)=$Л.

Перенесение теорем об общезначимых формулах исчисления высказываний на исчисление предикатов требует осторожности.

Частный случай теоремы 1 имеет место, если $E[P_1,...,P_n]$ - формула исчисления высказываний, а $A_1,...,A_n$ - произвольные формулы исчисления предикатов. Доказательство остается прежним. Поэтому будут верны и теоремы 2,3, где A, B, C - произвольные формулы исчисления предикатов.

Из определения логических операций с кванторами следует общезначимость следующих формул: $\models P(y)\to\exists x\,P(x)$, $\models\forall x\,P(x)\to P(y)$.

Чтобы распространить эти результаты на произвольные формулы A исчисления предикатов, необходимо соблюдение следующего условия: *'подстановки переменной 'y' вместо всех свободных вхождений переменной 'x' в формулу* A(x) *остаются свободными в формуле* A(y) *'.*

Назовем такую *подстановку 'y' свободной для 'x' в* A(x).

УТВЕРЖДЕНИЕ 1. а) $\models A(y)\to\exists x\,A(x)$, б) $\models\forall x\,A(x)\to A(y)$,

где 'y' свободна для 'x' в A(x).

УТВЕРЖДЕНИЕ 2. а) $\models A(x)\to C\ \Rightarrow\ \models\exists x\,A(x)\to C$,

б) $\models C\to A(x)\Rightarrow\models C\to\forall x\,A(x)$,

где формула ‘C’ не содержит свободных вхождений переменной ‘x’.

Приведем набросок доказательства для случая б):

Обозначим через FV(E) список свободных переменных формулы E. Допустим, что существует область $D \neq \varnothing$, такая, что при некоторой интерпретации τ предикатных букв и некотором означивании предметных переменных γ : $FV(C \to \forall x\ A(x)) \Rightarrow D$ имеем $(C \to \forall x\ A(x))\ [\tau,\gamma] = Л$,

т.е.$C[\tau,\gamma] = И$ и $(\forall x\ A(x))\ [\tau,\gamma] = Л$. Тогда $(A(a))\ [\tau,\gamma] = Л$ для некоторого

$a \in D$, но $(C \to A(x))\ [\tau,\gamma] = И$ для всех τ, γ, что противоречит общезначимости формулы $C \to A(x)$.

Подстановка формулы $A(w_1,...,w_n)$ *вместо предикатной буквы* $P(w_1,...,w_n)$ на всех местах вхождения $P(y_1,...,y_n)$ в формулу $E[P(y_1,...,y_n)]$ называется *свободной,* если: (1) переменные $y_1,...,y_n$, соответственно, свободны для $w_1,...,w_n$, в формуле $A(w_1,...,w_n)$; (2) после подстановки $y_1,...,y_n$ вместо $w_1,...,w_n$, соответственно, ни одна свободная переменная формулы $A(y_1,...,y_n)$ не окажется связанной в формуле $E^*[A(y_1,...,y_n)]$.

Примеры подстановки формулы A(w) *вместо предиката* (атома) P(w) в формулу $P(y) \to \exists x\ P(x)$: (в примерах 1,3,5 подстановка будет свободной).

	A(w):	$P(y) \to \exists x\ P(x)$:
1.	$\forall z\ Q(w,z,w)$	$\forall z\ Q(y,z,y) \to \exists x \forall z\ Q(x,z,x)$
2.	$\forall y\ Q(w,y,w)$	$\forall y\ Q(y,y,y) \to \exists x \forall y\ Q(x,y,x)$
3.	$Q(w,u,w)$	$Q(y,u,y) \to \exists x\ Q(x,u,x)$
4.	$Q(w,x,w)$	$Q(y,x,y) \to \exists x\ Q(x,x,x)$
5.	$\forall w\ P(w) \vee Q(w)$	$\forall w\ P(w) \vee Q(y) \to \exists x\ (\forall w\ P(w) \vee Q(x))$

ТЕОРЕМА 1 *(Подстановка вместо атомов)*. Если подстановка формул $A_1(x_1,\ldots,x_{n_1})$, …, $A_m(x_1,\ldots,x_{n_m})$ свободна в формуле $E[P_1,\ldots,P_m]$ для предикатных букв $P_1(x_1,\ldots,x_{n_1}),\ldots,P_m(x_1,\ldots,x_{n_m})$, соответственно. Тогда, если $\models E[P_1,...,P_m]$, то $\models E^*[A_1,\ldots,A_m]$.

Следствие. Если подстановка переменных $y_1,...,y_n$ свободна для $w_1,...,w_n$, соответственно, в формуле $A(w_1,\ldots,w_n)$, то $\models A(w_1,\ldots,w_n) \Rightarrow \models A(y_1,\ldots,y_n)$.

ТЕОРЕМА 4 (*Эквивалентность формул*). $\models A \sim B$ т.и т.т., когда для любой предметной области $D \neq \varnothing$ и при любой интерпретации τ предикатных букв, и любом означивании γ предметных переменных на элементах области D, $A[\tau,\gamma] = B[\tau,\gamma]$.

Формулы называются *конгруентными*, если после стирания в них всех связанных вхождений переменных, получаем одно и то же выражение.

УТВЕРЖДЕНИЕ 3**.** Для конгруентных формул A и B верно $\models A \sim B$.

*Основные тавтологии исчисления предикатов (с кванторами)***:**

$$\neg\forall x\ A(x) \sim \exists x \neg A(x)$$
$$\neg\exists x\ A(x) \sim \forall x \neg A(x)$$
$$\forall x \forall y\ A(x,y) \sim \forall y \forall x\ A(x,y)$$
$$\exists x \exists y\ A(x,y) \sim \exists y \exists x\ A(x,y)$$
$$\forall x\ A(x)\ \&\ \forall x B(x) \sim \forall x\ (A(x)\ \&\ B(x))$$
$$\exists x\ A(x) \vee \exists x\ B(x) \sim \exists x\ (A(x) \vee B(x))$$

$\forall x\, A(x) \vee \forall x\, B(x) \to \forall x\, (A(x) \vee B(x))$

$\exists x\, (A(x) \& B(x)) \to \exists x\, A(x)\ \&\ \exists x\, B(x)$

$\exists x\, (A(x) \to B(x)) \sim (\forall x\, A(x) \to \exists x\, B(x))$

Если формула C не содержит свободно x, то :

$\forall x\, C \sim C$

$\exists x\, C \sim C$

$\forall x\, A(x) \vee C \sim \forall x\, (A(x) \vee C)$

$\exists x\, A(x)\ \& C \sim \exists x\, (A(x) \& C)$

Теоремы 6 и 7 могут быть обобщены в исчислении предикатов, если в описание операций 'X'('крест') и '/' ('штрих') включить замену $\forall$ на $\exists$ и $\exists$ на $\forall$.

Формула B *является логическим следствием формул* $A_1,...,A_m$, если для любой области $D \neq \varnothing$ и любых интерпретаций τ, γ, входящих в формулы $A_1, \ldots, A_m$, B предикатных букв и свободных предметных переменных, в строках таблицы истинности, где $A_1[\tau,\gamma] = \ldots = A_m[\tau,\gamma] = И$, также и $B[\tau,\gamma] = И$. Обозначим как $A_1, \ldots, A_m \models B$.

Данное определение соответствует условной интерпретации переменных в математике, при которой предикатные буквы и предметные переменные остаются фиксированными в контексте доказательства :

$\forall x\, (x^2-5x-6=0 \to x=6 \vee x=-1)$, в отличие от интерпретации всеобщности переменных : $\forall x \forall y (x+y=y+x) \to 2+3=3+2$.

При таком определении логического следствия теорема 8 и ее следствие обобщаются на исчисление предикатов. Доказательства там и здесь по сути совпадают.

Примеры отношений логического следования:

$\neg P(x) \models \neg P(x)$; $\neg P(x) \models \forall x \neg P(x)$; $\neg P(x) \models \neg P(y)$;

$\neg P(x) \models \neg \forall x P(x)$; $\forall x \neg P(x) \models \neg P(x)$; $P(x) \models \forall x P(x)$.

Из таблицы истинности увидим, какие из них имеют место. Пусть $D=\{0,1\}$, проинтерпретируем на D предикатную букву $P^{(1)}$, так что:

x y	P(x)	$\neg$P(x)	$\forall x \neg$ P(x)	$\neg$P(y)	$\forall x$ P(x)	$\neg\forall x$ P(x)
0 0	J_1=и	Л		л		
0 1	J_1=и	Л	Л	л	И	Л
1 0	J_1=и	Л		л		
1 1	J_1=и	Л		л		
0 0	J_2=и	Л		л		
0 1	J_2=и	Л	Л	и	Л	И
1 0	J_2=л	И		л		
1 1	J_2=л	И		и		
0 0	$J_{3=}$л	И		и		
0 1	$J_{3=}$л	И	Л	л	Л	И
1 0	J_3=и	Л		и		
1 1	J_3=и	Л		л		
0 0	J_4=л	И		и		
0 1	J_4=л	И	И	и	Л	И
1 0	J_4=л	И		и		
1 1	J_4=л	И		и		

Очевидно, что верны следующие отношения логического следования: $\neg P(x) \models \neg P(x)$, $\neg P(x) \models \neg \forall x P(x)$, $\forall x \neg P(x) \models \neg P(x)$. Убедиться, что они верны без ограничений на число элементов области D. А отношения $\neg P(x) \models \forall x \neg P(x)$; $\neg P(x) \models \neg P(y)$; $P(x) \models \forall x P(x)$ не имеют места.

Упражнение

1. Построить истинностные таблицы над областью D = {1,2} следующих формул:
(a) $\forall z\,(P(x) \to \neg Q \vee P(z))$; (b) $P(x,y) \to \forall x\,(P(x,y) \to \exists x\, P(x,x))$.
2. Докажите, что формула $\forall x \exists y\, P(x,y) \to \exists y \forall x\, P(x,y)$ 1-общезначима.
3. Докажите, что следующие формулы не общезначимы:
   (a) $\neg(\forall x \exists y\, P(x,y) \to \exists y \forall x\, P(x,y))$;
   (b) $\exists x \exists y\, P(x,y) \to \exists x\, P(x,x)$;
   (c) $\exists x\, P(x) \,\&\, \exists x\, Q(x) \to \exists x\,(P(x) \,\&\, Q(x))$.
4. Общезначимы ли следующие формулы?
   (a) $P(x) \to \forall x\, P(x)$, (b) $\exists x\, P(x) \to P(x)$, (c) $\forall x\, P(x) \to \exists x\, P(x)$,
   (d) $\exists x\, P(x) \to \forall x\, P(x)$, (e) $\exists y\,(P(y) \vee \forall x\,(P(x) \to Q)) \sim \exists y\,(P(y) \vee \forall x (P(x) \to Q))$.
5. Доказать УТВЕРЖДЕНИЕ 1 и УВЕРЖДЕНИЕ 2(a).
6. Применимо ли УТВЕРЖДЕНИЕ 1 к доказательству общезначимости следующих формул или установите это другим способом:
   (a) $\forall x \exists y\, P(x,y) \to \exists y\, P(y,y)$; (d) $\forall x \exists z\, P(x,z) \to \exists z\, P(y,z)$;
   (b) $\exists y\, P(y,y) \to \exists x \exists y\, P(x,y)$, (e) $P(x,x) \to \exists y\, P(x,y)$;
   (c) $P(x,x) \to \exists y\, P(y,y)$; (f) $\forall y\, P(x,y) \to P(y,y)$.
7. Выполнить указанные подстановки и выяснить, свободны ли эти подстановки:
(a) $\exists z P(z,w,y)$, Q вместо P(w), Q в $P(z) \to Q$;
(b) $\exists x P(x,w,y)$, Q(w) вместо P(w), Q(w) в $\forall y(P(z) \to Q(y))$;
(c) $\exists z P(z,w,y)$, Q(w) вместо P(w), Q(w) в $\forall x(P(x) \to Q(x))$;
(d) P(w,v,x), Q вместо P(v,w),Q(w) в $\forall x(P(x,y) \vee Q(x) \to P(y,x))$;
(e) $\exists z Q(z,w,w,y)$, $\forall x P(v,w,x)$ вместо P(w),Q(v,w) в $\forall x(P(x) \to Q(x,x))$;
(f) $\exists z Q(z,w,w,y)$, $\forall x P(v,w,x)$ вместо P(w),Q(v,w) в $\forall x(P(x) \to \forall y\, Q(y,y))$;
(g) $\exists z \forall w P(z,w,y)$, $Q(z,w) \,\&\, \exists w R(w)$ вместо P(w), Q(w) в $\exists z P(z) \to Q(z)$.
8. Найти эквивалентные формулы с тесными отрицаниями:
(a) $\neg \forall x ((P(x) \vee \exists y \neg Q(x,y)) \,\&\, \forall y R(y))$;
(b) $\neg(\neg(\exists x P(x) \to \forall x Q(x,y)) \vee \forall x \neg P(x))$.
9. Доказать УТВЕРЖДЕНИЕ 3.
10. Замкнутая формула $\forall x_1 \ldots \forall x_n \exists z_1 \ldots \exists z_m A$, где $m \geq 0$, $n \geq 1$ и A - бесквантерная формула, не содержащая предметных констант, общезначима тогда и только тогда, когда она n – общезначима, и, соответственно, замкнутая формула $\exists z_1 \ldots \exists z_m A$ общезначима, если она 1- общезначима.
11. Найдите: (a) формулу, которая была бы 1-общезначимой и 2-общезначимой, но не была бы 3-общезначимой; (b) формулу, которая была бы 1-, 2-, 3-общезначимой, но не 4-общезначимой.
12. Доказать тавтологии исчисления предикатов с кванторами.
13. Сформулировать условия перенесения теорем об общезначимых формулах исчисления высказываний на исчисление предикатов.

14.Установить истинность (ложность) следующих отношений логического следования:
a) $\forall x\, P(x) \models P(x)$, b) $\forall x P(x) \models P(y)$, c) $P(x) \models \forall x P(x)$.
15. Доказать, что для произвольных ‘x’ и ‘A’ : $\forall x\, A(x) \models A(x)$,
$\models A$ т. и т. т., когда $\models \forall x\, A$, а $A \models \forall x\, A$ не всегда имеет место.
16. Обосновать, что утверждение “$A \models B$” является более сильным, чем утверждение “если $\models A$, то $\models B$”.

2. 2. Система аксиом в исчислении предикатов

Схемы аксиом и правил вывода остаются теми же, что и для исчисления высказываний, с формулами языка исчисления предикатов, к которым добавляются схемы аксиом и правил вывода, связанные с кванторами.

А к с и о м ы:

1а $A\to(B\to A)$
1б $(A\to B)\to((A\to(B\to C))\to(A\to C))$
2 $A\to(B\to A\&B)$
3а $A\&B\to A$
3б $A\&B\to B$
4а $A\to A\vee B$
4б $B\to A\vee B$
5. $(A\to C)\to((B\to C)\to(A\vee B\to C))$
6. $(A\to B)\to((A\to\neg B)\to \neg A)$
7. $\neg\neg A\to A$
8. $(A\to B)\to((A\to B)\to (A \sim B))$
9а. $A \sim B \to (A\to B)$
9б. $A \sim B \to (B\to A)$
10. $A \to(\neg A\to C)$

и п р а в и л о в ы в о д а modus ponens .

Н о в ы е а к с и о м ы и п р а в и л а в ы в о д а:

11 $C\to A(x) \vdash C\to \forall x\, A(x)$ ($\forall$- введение)
12 $\forall x\, A(x)\to A(t)$ ($\forall$- удаление)
13 $A(x)\to C \vdash \exists x\, A(x)\to C$ ($\exists$ - удаление)
14 $A(t)\to\exists x\, A(x)$ ($\exists$ - введение),

где подстановка терма t свободна для переменной x в формуле A(x), и формула C не содержит свободно x.

Ф о р м у л а B *в ы в о д и м а и з ф о р м у л* $A_1, \dots, A_m$, если существует список формул $B_1,\dots,B_l$ такой, что $B_l=B$, и каждая формула B_i есть аксиома или одна из формул $A_1, \dots, A_m$, или получается из предыдущих формул по одному из правил вывода, где все *свободные переменные* формул $A_1, \dots, A_m$ *остаются фиксированными*, т.е. правила с кванторами ($\forall$, $\exists$) не применяются ни к какой переменной, входящей свободно в формулы $A_1, \dots, A_m$, кроме случаев, когда эти правила применялись до использования формул $A_1, \dots, A_m$ в качестве допущений.

ТЕОРЕМА (*О дедукции*)**.** Если $A_1, \dots, A_m \vdash B$, то $A_1, \dots, A_{m-1} \vdash A_m\to B$, где применение правил $\forall$-введения и $\exists$-удаления фиксированно для свободных переменных формул $A_1, \dots, A_m$.

Д о к а з а т е л ь с т в о:

Пусть вывод (I) - цепочка формул : $\begin{cases} B_1 \\ \vdots \\ B_n = A_m \text{ - первое вхождение } A_m \text{ в качестве допущения} \\ B_j \\ \vdots \\ B_l \end{cases}$.

По выводу (1) строим схему: $\begin{cases} \left.\begin{matrix} B_1 \\ \vdots \\ B_{n-1} \end{matrix}\right\} \text{из I} \\ A_m \to B_n \\ \vdots \\ A_m \to B_1 \end{cases}$

Переделаем эту схему в вывод (II):

1 случай: B_j – аксиома или одна из гипотез $A_1,\ldots,A_m$ в выводе (I).

Если $j < n$, вывод (1) формулы B_j остается выводом (11).

Для $j > n$ и $j = n$ доказательство как в исчислении высказываний.

Рассмотрим вывод (11) для случая $j > n$:

$\begin{cases} \left.\begin{matrix} B_1 \\ \vdots \\ B_{n-1} \end{matrix}\right\} \text{из (I)} \\ A_m \to A_m \\ \vdots \\ B_j, \text{ где } B_j - \text{аксиома или одна из гипотез } A_1,\ldots,A_{m-1} \\ \vdots \\ B_j \to (A_m \to B_j) \text{ (аксиома 1a)} \\ \vdots \\ A_m \to B_j \end{cases}$

2 случай. Если B_i получена в выводе (I) по правилу modus ponens, то рассмотрим следующие случаи:

(1) B_j появилась до B_n , т.е. $j<n$, тогда $\dfrac{B_i, B_g}{B_j}$ (I) и $i,g<n$. Поэтому вывод (1) есть вывод (11).

(2) $j>n$:

а) Если i,g<n, то $\dfrac{B_i,(B_i \to B_j) = B_g}{B_j}$ (I) и в схеме: $\dfrac{B_i, B_g}{A_m \to B_j}$.

Обоснуем вхождение $A_m \to B_j$ в вывод (II) :

$$\begin{cases} \vdots \\ B_i \\ B_i \to (A_m \to B_i) \\ A_m \to B_i \\ B_i \to B_j \\ (B_i \to B_j) \to (A_m \to (B_i \to B_j)) \\ A_m \to (B_i \to B_j) \\ (A_m \to B_i) \to ((A_m \to (B_i \to B_j)) \to (A_m \to B_j)) \\ (A_m \to (B_i \to B_j)) \to (A_m \to B_j) \\ A_m \to B_j \end{cases}$$

б) Если i>n и g<n, то в схеме соответственно имеем :
$A_m \to B_i$ и $B_i \to B_j$ и $A_m \to B_j$.

Тогда в (II):
$$\begin{cases} \vdots \\ A_m \to B_i \\ \vdots \\ B_i \to B_j \\ (B_i \to B_j) \to (A_m \to (B_i \to B_j)) \\ A_m \to (B_i \to B_j) \\ (A_m \to B_i) \to ((A_m \to (B_i \to B_j)) \to (A_m \to B_j)) \\ (A_m \to (B_i \to B_j)) \to (A_m \to B_j) \\ A_m \to B_j \end{cases}$$.

Аналогично получается вывод (11), для c) g>n и i<n и d) i,g >n.

3 случай. B_j получена в выводе (I) по правилу $\forall$- введения из формулы B_i:
а) Если j<n, то i<n: обоснование формул $B_i = C \to A(x)$, $B_j = C \to \forall x\, A(x)$ в выводе (1) и выводе (II) совпадают.

b) Если i<n и j>n, тогда в (II) : $\begin{cases} C \to A(x) \\ (C \to A(x)) \to (A_m \to (C \to \text{A(x)})) \\ A_m \to (C \to \text{A(x)}) \\ A_m \ \& \ C \to \text{A(x)} \\ A_m \ \& \ C \to \forall x \text{A(x)} \\ A_m \to (C \to \forall x \text{A(x)}) \end{cases}$

(правило ∀- введения применимо в выводе (II): ‘x’ не входит свободно в формулы C и A_m , т.к., соответственно, оно применялось в выводе (1) и переменная ‘x’ фиксированна относительно A_m в выводе (1) для j>n).

c) Если i>n, то j>n, тогда в схеме имеем $A_m \to B_i$ и $A_m \to B_j$. Дальше доказательство $A_m \to B_j$ строится, используя индукционное допущение, как в случае b).

4 случай. Формула B_j получена из B_i по правилу ∃ - удаления. Вывод (11) строится аналогично 3 случаю.

Теорема дедукции на примере:

$\forall x\,(P(x)\to Q(x)), \forall x\,P(x) \vdash \forall x\,Q(x) \ \Rightarrow\ \forall x\,(P(x)\to Q(x)) \vdash \forall x\,P(x)\to \forall x\,Q(x)$

Вывод (1):

1. $\forall x\,(P(x)\to Q(x))$ (гипотеза A_j, $j\neq m$)
2. $\forall x\,(P(x)\to Q(x))\to (P(x)\to Q(x))$ (аксиома)
3. $P(x)\to Q(x)$ (modus ponens, 1 и 2)
4. $\forall x\,P(x)$ (гипотеза A_m)
5. $\forall x\,P(x)\to P(x)$ (аксиома)
6. $P(x)$ (modus ponens, 4,5)
7. $Q(x)$ (modus ponens, 6,3)
8. $Q(x)\to((\neg\neg P\to P)\to Q(x))$ (аксиома 1a)
9. $(\neg\neg P\to P)\to Q(x)$ (modus ponens, 7,8)
10. $(\neg\neg P\to P)\to \forall x\,Q(x)$ (∀-введение, 9)
11. $\neg\neg P\to P$ (аксиома)
12. $\forall x\,Q(x)$ (modus ponens, 11,10).

Переделаем вывод (I) в схему:

1. $\forall x\,(P(x)\to Q(x))$
2. $\forall x\,(P(x)\to Q(x))\to (P(x)\to Q(x))$
3. $P(x)\to Q(x)$
4. $\forall x\,P(x)\to \forall x\,P(x)$ ($A_m\to A_m$)
5. $\forall x\,P(x)\to(\forall x\,P(x)\to P(x))$
6. $\forall x\,P(x)\to P(x)$
7. $\forall x\,P(x)\to Q(x)$
8. $\forall x\,P(x)\to(Q(x)\to((\neg\neg P\to P)\to Q(x)))$
9. $\forall x\,P(x)\to((\neg\neg P\to P)\to Q(x))$
10. $\forall x\,P(x)\to((\neg\neg P\to P)\to \forall x\,Q(x))$

11. $\forall x\, P(x)\to((\neg\neg P\to P))$
12. $\forall x\, P(x)\to \forall x\, Q(x)$.

Построим вывод (II):

1. $\forall x\,(P(x)\to Q(x))$ (гипотеза A_j, $j \neq m$)
2. $\forall x\,(P(x)\to Q(x))\to (P(x)\to Q(x))$ (аксиома)
3. $P(x)\to Q(x))$ (modus ponens, 1,2)

●●●

4. $\forall x\, P(x)\to\forall x\, P(x)$ (доказательство теоремы $A\to A$)

$$\begin{cases}\forall x\, P(x) \to P(x)\ (\text{аксиома})\\ (\forall x\, P(x) \to P(x)) \to (\forall x\, P(x) \to (\forall x\, P(x) \to P(x))\ (\text{аксиома (1a)})\\ 5.\ \forall x\, P(x) \to (\forall x\, P(x) \to P(x))\ (\text{m.p.})\end{cases};$$

$\forall x\, P(x)\to\forall x\, P(x)$ (4)
$\forall x\, P(x)\to(\forall x\, P(x)\to P(x))$ (5)
$(\forall x\, P(x)\to\forall x\, P(x)) \to ((\forall x\, P(x)\to(\forall x\, P(x)\to P(x)))\to(\forall x\, P(x)\to P(x)))$

6. $\forall x\, P(x)\to P(x)$ (modus ponens 2 раза)
$P(x)\to Q(x)$ (3)
$(P(x)\to Q(x)) \to (\forall x\, P(x)\to(P(x)\to Q(x)))$ (аксиома 1a)
$\forall x\, P(x)\to(P(x)\to Q(x))$ (modus ponens)
$\forall x\, P(x)\to P(x)$ (6)
$(\forall x\, P(x)\to P(x))\to((\forall x\, P(x)\to(P(x)\to Q(x)))\to(\forall x\, P(x)\to Q(x)))$

7. $\forall x\, P(x)\to Q(x)$ (modus ponens 2 раза)

$$\begin{cases}Q(x)\to((\neg\neg P\to P)\to Q(x))\\ Q(x)\to((\neg\neg P\to P)\to Q(x))\to(\forall x\, P(x)\to(Q(x)\to((\neg\neg P\to P)\to Q(x))))\\ 8.\forall x\, P(x)\to(Q(x)\to((\neg\neg P\to P)\to Q(x))).\end{cases}$$

$$\begin{cases}\forall x\, P(x) \to Q(x) & (7)\\ \forall x P(x) \to (Q(x) \to ((\neg\neg P \to P) \to Q(x)))\\ (\forall x P(x) \to Q(x)) \to (\forall x P(x) \to (Q(x) \to ((\neg\neg P \to P) \to Q(x)))\\ \to (\forall x P(x) \to ((\neg\neg P \to P) \to Q(x))))\\ 9.\ \forall x\, P(x) \to ((\neg\neg P \to P) \to Q(x))\ (\text{modus ponens 2 раза})\end{cases}$$

$$\begin{cases}\forall x\, P(x) \to ((\neg\neg P \to P) \to Q(x)) & (9)\\ \forall x\, P(x)\ \&\ (\neg\neg P \to P) \to \forall x\, Q(x) & (\forall\text{ - введение})\\ 10.\forall x\, P(x) \to ((\neg\neg P \to P) \to \forall x\, Q(x))\end{cases};$$

$$\begin{cases}\neg\neg P \to P\ (\text{аксиома})\\ (\neg\neg P \to P) \to (\forall x\, P(x) \to (\neg\neg P \to P))\ (\text{аксиома (1a)})\\ 11.\ \forall x\, P(x) \to (\neg\neg P \to P)\end{cases};$$

$\forall x P(x)\to(\neg\neg P\to P)$ (11)

$\forall xP(x)\to((\neg\neg P\to P)\to\forall xQ(x))$ (10)

$(\forall xP(x)\to(\neg\neg P\to P))\to((\forall xP(x)\to((\neg\neg P\to P)\to\forall xQ(x)))\to$

$\to(\forall xP(x)\to\forall xQ(x)))$ (аксиома 1б)

12. $\forall xP(x)\to\forall xQ(x)$ (modus ponens 2 раза)

ТЕОРЕМА *(Производные правила вывода).* Производные правила исчисления высказываний с формулами исчисления предикатов и новые правила с кванторами.

●●●

$\dfrac{\forall x\,A(x)}{A(t)}$ (∀-удаление) $\qquad \dfrac{\Gamma\vert- A(x)}{\Gamma\vert-\forall xA(x)}$ (∀ - введение)

$\dfrac{A(t)}{\exists x\,A(x)}$ (∃ - введение) $\qquad \dfrac{\Gamma, A(x)\vert- C}{\Gamma,\exists x\,A(x)\vert- C}$ (∃ -удаление),

где t свободно для x в A(x). где x не входит свободно в Γ,C.

ТЕОРЕМА 5*(О замене).* Если |- A ~ B и E[A] -формула с выделенным вхождением подформулы A, а $E[B]=E[A]^{A}_{B}$ - результат замены этого вхождения на формулу B, $x_1,...,x_p$ - свободные переменные формул A, B, попадающие в область действия кванторов формул E[A] или E[B] при построении их, начиная с A, B, соответственно. Тогда если Γ |– A ~ B,
то Γ |- E[A] ~ E[B], где Γ список формул, не содержащих свободно переменные $x_1,...,x_p$.
ЛЕММА. Пусть x – некоторая переменная, A(x) – произвольная формула, а y произвольная переменная, не обязательно отличная от x, такая, что:

(h) ‘y’ свободна для ‘x’ в A(x), (ii) ‘y’ не входит свободно в A(x) (кроме случая, когда ‘y’ есть ‘x’), а A(y) есть результат подстановки ‘y’ вместо свободных вхождений ‘x’ в A(x).

Тогда: (a) |– ∀x A(x) ~ ∀y A(y); (b) |– ∃ x A(x) ~ ∃y A(y).

УТВЕРЖДЕНИЕ. Если формулы A и B конгруентны, то |- A ~ B.

Примеры построения доказательств :

1). |- ¬ ∀x A(x)~∃x ¬ A(x) :

1. ¬∀x A(x) (допущение)
2. A(x) (допущение противного)
3. ∀x A(x) (∀ - введение)
4. ¬A(x) (¬ - введение,2)
5. ∃x ¬A(x) (∃ - введение, 4)
6. ¬∀A(x)→∃x ¬ A(x) (теорема дедукции,1,5)
7. ∃x ¬ A(x) (допущение)
8. ∀x A(x) (допущение противного)
9′. ¬ A(x) (допущение)
10′ A(x) (∀- удаление,8)
11′. ¬ ∀x A(x) (слабое удаление ¬)

12. $\neg\forall x\, A(x)$ ($\exists$ - удаление,7)

13. $\neg\forall x\, A(x)$ ($\neg$-введение,8)

14. $\exists x \neg A(x) \rightarrow \neg \forall x\, A(x)$ (теорема дедукции,7,12)

15. $\neg \forall x\, A(x) \leftrightarrow \exists x \neg A(x)$ ($\leftrightarrow$ - введение, 6,13).

2) $\forall x\,(P(x)\rightarrow Q(x)) \vdash \forall x\, P(x) \rightarrow \forall x\, Q(x)$:

$\forall x\,(P(x)\rightarrow Q(x)), \forall x\, P(x) \vdash P(x)\rightarrow Q(x)$ (удаление$\forall$)

$\forall x\,(P(x)\rightarrow Q(x)), \forall x\, P(x) \vdash P(x)$ (удаление$\forall$)

$\forall x\,(P(x)\rightarrow Q(x)), \forall x\, P(x) \vdash Q(x)$ (удаление$\rightarrow$)

$\forall x\,(P(x)\rightarrow Q(x)) \vdash \forall x\, P(x) \rightarrow Q(x)$ (введение$\rightarrow$)

$\forall x\,(P(x)\rightarrow Q(x)) \vdash \forall x\, P(x) \rightarrow \forall x\, Q(x)$ (введение$\forall$)

Формула вида $Q_1 x_1 \ldots Q_n x_n A$, где A бескванторная формула, а Q_i есть $\forall$ или $\exists$, называется *предваренной* (или *пренексной*) *нормальной формой*.

ТЕОРЕМА 9. У всякой формулы исчисления предикатов есть эквивалентная ей предваренная нормальная форма.

ТЕОРЕМА (*Геделя о полноте исчисления предикатов*). $\vdash E \Leftrightarrow \models E$**.**

(Без доказательства).

Следствие. Исчисление предикатов непротиворечиво.

Упражнение

1. Обосновать допустимость *производных правил вывода исчисления предикатов.*

2.Доказать следующую теорему: Какова бы ни была формула E и нуль-местная предикатная буква P, всегда $\vdash E \sim (P\&F_1)\vee(\neg P\&F_2)$, где F_i есть P или $\neg$P, или некоторая формула, не содержащая P (i=1,2).

3. Доказать *основные тавтологии исчисления предикатов с кванторами.*

4. Найти ошибку в выводе:

$P(x),\ Q(x) \vdash \exists x(Q(x) \,\&\, P(x))$

$P(x), \exists x\, Q(x) \vdash \exists x(Q(x) \,\&\, P(x))$

$\exists x\, P(x), \exists x\, Q(x) \vdash \exists x(Q(x) \,\&\, P(x))$

$\exists x\, P(x) \,\&\, \exists x\, Q(x) \vdash \exists x(Q(x) \,\&\, P(x))$

$\vdash \exists x\, P(x) \,\&\, \exists x\, Q(x) \rightarrow \exists x(Q(x) \,\&\, P(x))$

5. Доказать, что следующие теоремы имеют место, если A(x,x) является результатом подстановки ‘x’ вместо свободных вхождений ‘y’ в A(x,y), причем ‘x’ свободно для ‘y’ в A(x,y) :

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

6. Какое из утверждений верно: $A(x) \vdash \forall x\, A(x)$ или $\vdash A(x) \Rightarrow \forall x\, A(x)$?

7. Доказать теорему 9.

8. Привести к предваренной форме формулу:

$(\neg \exists x\, P(x) \vee \forall x\, Q(x)) \,\&\, (R \to \forall x\, S(x))$

9. Являются ли выводимыми следующие формулы:

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

(b) $(\forall x\, P(x) \to P(y)) \to (\forall x P(x) \to \forall y P(y))$, где P – одноместная предикатная буква;

(c) $A(x) \to \exists x\, A(x)$;

(d) $(A(x) \to \exists x\, A(x)) \to (\forall x\, A(x) \to (A(x) \to \exists x\, A(x)))$;

(e) $\forall x\, A(x) \to (A(x) \to \exists x\, A(x))$;

(f) $(\forall x\, A(x) \to A(y)) \to (\forall x A(x) \to \forall y A(y))$;

(i) $(A(y) \to \exists x\, A(x)) \to (\exists y A(y) \to \exists x\, A(x)))$.

10. Доказать при условии, что переменная x не входит свободно в формулы списка Γ : (a) Если $\Gamma \vdash A(x) \sim B(x)$, то $\Gamma \vdash \forall x\, A(x) \sim \forall x B(x)$.

(b) Если $\Gamma \vdash A(x) \sim B(x)$, то $\Gamma \vdash \exists x\, A(x) \sim \exists x\, B(x)$.

11. Обосновать правильность вывода: $\forall x\, (P(x) \sim \exists z\, R(x,w,z)) \vdash$

$P(x) \vee \forall x \exists y\, (P(x) \to Q(y)) \sim P(x) \vee \forall x \exists y (\exists z\, R(x,w,z) \to Q(y))$.

12. Доказать УТВЕРЖДЕНИЕ об эквивалентности конгруентных формул.

13. Доказать, что если множества формул $T_0, T_1, T_2, \ldots$ непротиворечивы и $T_i \subseteq T_{i+1}$ $(i=0,1,\ldots)$, то $\bigcup T_i$ - непротиворечивое множество формул.

14. Пусть множество $\Gamma \cup \{\exists x\, A(x)\}$ непротиворечиво. Доказать, что если переменная ‘y’ не входит в Γ и $\exists x\, A(x)$, то множество $\Gamma \cup \{\exists x\, A(x), A(y)\}$ непротиворечиво.

15. Пусть множество формул Γ полно и непротиворечиво. Доказать, что для любых замкнутых (не содержащих свободных переменных) формул A и B верно: a) $\Gamma \vdash A\&B \Leftrightarrow \Gamma \vdash A$ и $\Gamma \vdash B$;

b) $\Gamma \vdash A \vee B \Leftrightarrow \Gamma \vdash A$ или $\Gamma \vdash B$;

c) $\Gamma \vdash \neg A \Leftrightarrow$ не$(\Gamma \vdash A)$;

d) $\Gamma \vdash A \to B \Leftrightarrow$ не$(\Gamma \vdash A)$ или $\Gamma \vdash B$.

16. Добавим в алфавит исчисления предикатов функциональные символы $f^{(n)}(x_1,\ldots,x_n)$ $(n \geq 0)$ и определим новые выражения – термы: (1) $x_1, x_2, \ldots$-термы; (2) если $t_1,\ldots,t_n$ – термы и $f^{(n)}(x_1,\ldots,x_n)$ $(n \geq 0)$ – функциональный символ, то $f^{(n)}(t_1,\ldots,t_n)$ - функциональный терм.

Интерпретациями функциональных символов являются отображения (соответствующей местности) на заданной предметной области $D \neq \varnothing$.

Найти значения функционального терма $t = f(f(x))$ на области $D=\{1,2\}$ и построить истинностную таблицу формулы $P(f(x)) \to \exists x \neg P(f(f(x)))$.

17. Какие из термов: (a) f(x,y), (b) g(w,y), (c) g(z, f(x,y)), (d) g(y, f(h,x)) свободны для ‘x’ в формуле ‘$\forall w\,(P(x,y) \vee \exists z\, Q(y,z) \to R(w))$’?

18. Пусть x – произвольная переменная и A(x) – произвольная формула, t – терм, свободный для x в формуле A(x). Доказать, что

(a) $\models \forall x\, A(x) \to A(t)$, (b) $\models A(t) \to \exists x\, A(x)$.

19. Пусть формулы Γ не содержат свободно переменной x и терм t свободен для x в формуле A(x). Доказать, что $\Gamma \vdash A(x) \Rightarrow \Gamma \vdash A(t)$.

2.3 Формальная арифметика

Опишем теперь одну формальную систему, предназначенную для формализации элементарной теории чисел.

А л ф а в и т: (1) символы алфавита исчисления предикатов: предикатные буквы, предметные переменные, логические связки и кванторы;

(2) предикатная константа : $=$;

(3) функциональные константы : $'$, $+$, $\bullet$;

(4) предметная константа : 0 ;

(5) вспомогательные символы : (,).

Т е р м ы : (1) a , b, c , …- предметные переменные ;

(2) 0 – предметная константа ;

(3) если t, s – термы, то t', $t + s$, $t \bullet s$ – термы.

Ф о р м у л ы: (1) $t = s$, где t, s – термы, - элементарные формулы;

(2) если A, B – формулы, то $A\&B$, $A \vee B$, $\neg A$, $A \to B$, $A \leftrightarrow B$, $\forall x\, A(x)$, $\exists x\, A(x)$ – формулы.

А к с и о м ы и п р а в и л а в ы в о д а:

(1) аксиомы исчисления предикатов 1-12 и правило вывода modus ponens;

(2) нелогические аксиомы [1]**:**

13° (*Аксиома индукции*) $(A(0)\& \forall a\,(A(a) \to A(a'))) \to \forall a\, A(a)$, где A(a) - произвольная формула;

14°. $a' = b' \to a = b$;

15°. $\neg (a' = 0)$;

16°. $a = b \to (a = c \to b = c)$;

17°. $a = b \to a' = b'$;

18°. $a + 0 = a$;

19°. $a + b' = (a + b)'$;

20°. $a \bullet 0 = 0$;

21°. $a \bullet b' = a \bullet b + a$.

ТЕОРЕМА 1. $\vdash a = a$.

Д о к а з а т е л ь с т в о:

---

[1] Аксиомы Пеано

1. a=b→(a=c→b=c) (аксиома 16)
2. 0=0→(0=0→0=0) (аксиома 1a)
3. (a=b→(a=c→b=c))→((0=0→(0=0→0=0))→(a=b→(a=c→b=c)) (аксиома 1a)
4. (0=0→(0=0→0=0))→(a=b→(a=c→b=c)) (modus ponens)
5. (0=0→(0=0→0=0))→∀c (a=b→(a=c→b=c)) (введение ∀)
6. (0=0→(0=0→0=0))→∀b∀c (a=b→(a=c→b=c)) (введение ∀)
7. (0=0→(0=0→0=0))→∀a∀b∀c (a=b→(a=c→b=c)) (введение ∀)
8. ∀a∀b∀c (a=b→(a=c→b=c)) (modus ponens)
9. ∀a∀b∀c (a=b→(a=c→b=c))→ ∀b∀c (a+0=b→(a+0=c→b=c)) (удаление ∀)
10. ∀b∀c (a+0=b→(a+0=c→b=c)) (modus ponens)
11. ∀b∀c (a+0=b→(a+0=c→b=c))→ ∀c (a+0=a→(a+0=c→a=c)) (удаление ∀)
12. ∀c (a+0=a→(a+0=c→a=c)) (modus ponens)
13 ∀c (a+0=a→(a+0=c→a=c))→(a+0=a→(a+0=a→a=a)) (удаление ∀)
14. a+0=a→(a+0=a→a=a) (modus ponens)
15. a+0=a (аксиома 18)
16. a=a (2 раза modus ponens).

ТЕОРЕМА 2. |– a=b → b=a.

ТЕОРЕМА 3. |– a=b&b=c → a=c.

ТЕОРЕМА 4. |– a=b → a+c=b+c.

Д о к а з а т е л ь с т в о использует аксиому индукции.

Докажем |– A(0) (где A(0) ≡ a=b→a+0=b+0).

1. a=b (допущение)
2. a+0=a (аксиома 18)
3. b+0=b (аксиома 18)
4. ? =a+0→(?=b+0→a+0=b+0) (аксиома 16)
5. a+0=a → a=a+0 (теорема 2)
6. a=a+0 (modus ponens,2,5)

(? есть a)

7. a=b+0 → a+0=b+0 (modus ponens 6,4)
8. ??=a → (??=b+0→a=b+0) (аксиома 16)
9. a=b → b=a (теорема 2)
10. b=a (modus ponens 1,9)

(?? есть b)

11. b=b+0 → a = b+0 (modus ponens 10,8)
12. b+0 = b → b = b+0 (теорема 2)
13. b = b+0 (modus ponens 3,12)
14. a = b+0 (modus ponens 13,11)
15. a+0 = b+0 (modus ponens 14,7)
16. a = b→a+0 = b+0 (теорема дедукции 1,15) (т.е. |–A(0))
17. A(c) (допущение) (докажем |–A(c′))
18. a = b (допущение)
19. a+c = b+c (modus ponens 18,17)
20. a+c′ = (a+c)′ (аксиома 19)
21. b+c′ = (b+c)′
22. a+c = b+c → (a+c)′ = (b+c)′ (аксиома 17)
23. (a+c)′ = (b+c)′ (modus ponens 19,22)
24. a+c′ = (a+c)′ & (a+c)′ = (b+c)′ → a+c′ = (b+c)′ (теорема 3)
25. a+c′ = (a+c)′ & (a+c)′ = (b+c)′ (введение & 20,23)
26. a+c′ = (b+c)′ (modus ponens 24,25)

27. $b+c' = (b+c)' \to (b+c)' = b+c'$ (теорема 2)
28. $(b+c)' = b+c'$ (modus ponens 21,27)
29. $a+c' = (b+c)' \,\&\, (b+c)' = b+c'$ (введение & 26,28)
30. $a+c' = (b+c)' \,\&(b+c)' = b+c' \to a+c'=b+c'$ (теорема 3)
31. $a+c' = b+c'$ (modus ponens 29,30)
32. $a=b \to a+c' = b+c'$ (теорема дедукции 18,31) (т.е. $\vdash A(c')$)
33. $A(c) \to A(c')$ (теорема дедукции 17,32)
34. $\forall c\,(A(c)\to A(c'))$ (введение $\forall$,33)
35. $A(0)\&\forall c\,(A(c)\to A(c'))$ (введение & 16,34)
36. $A(0)\&\forall c\,(A(c)\to A(c'))\to\forall c\,A(c)$ (аксиома 13)
37. $\forall c\,A(c)$ (modus ponens 35,36)
38. $A(c)$ (удаление $\forall$,37).

ТЕОРЕМА 5. $\vdash a=b \to a\bullet c=b\bullet c$

ТЕОРЕМА ГЕДЕЛЯ (О неполноте формальной арифметики).

Если $\forall A_{13}$[2],..., $\forall A_{21} \vdash \Phi$, то $\forall A_{13}$,..., $\forall A_{21} \models \Phi$. Обратное неверно.
(Без доказательства)

Теорема Геделя о неполноте применима к любой рекурсивно аксиоматизируемой системе, в которой представимы все разрешимые предложения. В частности, это верно для более сильных систем, чем арифметика Пеано. Тем самым нельзя избавиться от неполноты арифметики добавлением новых аксиом.[2]

Упражнение

1. Доказать теоремы 2, 3, 5.
2. Доказать справедливость законов коммутативности, ассоциативности и дистрибутивности для операций “+” и “•”.
3. Определяя отношение “$x < y$” формулой $\exists z\,(z \neq 0 \,\&\, x + z = y)$, доказать следующие свойства :

$x < y \to (y < z \to x < z)$; $x \le x$; $x < x'$; $0 \le x$;
$x < y \to \neg(y < x)$; $x < y \leftrightarrow x' \le y$;
$x < y \to x + z < y + z$; $x \le y \leftrightarrow x < y'$;
$z \neq 0 \to x + z > x$; $x \le y \to (y \le z \to x \le z)$;
$x = y \vee x < y \vee y < x$. $x \le y \,\&\, y \le x \to x = y$;
$x \neq 0 \to y\bullet x \ge y$; $y \neq 0 \to \exists!u\exists!v\,(x = y\bullet u + v \,\&\, v < y)$.

4. Построить нестандартную модель формальной арифметики, добавив в ее алфавит новую предметную константу ‘c’ и присоединив нелогические аксиомы: $c\neq 0$, $c\neq 0'$, … . Доказать непротиворечивость полученной системы при условии, что непротиворечива формальная арифметика Пеано.

РАЗДЕЛ 2. А Л Г О Р И Т М Ы

[2] Замкнутая формула, получающаяся навешиванием кванторов всеобщности на все свободные переменные формулы. [2] См раздел 2, глава 2.

Г л а в а 1

АЛГОРИТМЫ И ВЫЧИСЛИМЫЕ ФУНКЦИИ

А л г о р и т м есть точное предписание, согласно которому по любому входному объекту из данного класса входных объектов можно эффективно получать выходные объекты. Например, алгоритм деления целых (вещественных) чисел "углом" или алгоритм умножения двух квадратных матриц порядка n. Ограничимся *дискретными* предписаниями, входные и выходные данные которых представляют собой конструктивные объекты. Конструктивные объекты можно кодировать словами в некотором алфавите, отсюда свойство *массовости* алгоритма. Получив входное слово, алгоритм через конечное число *элементарных шагов* должен построить выходное слово и закончить работу, или на данном входном слове предписание ведет к бесконечной последовательности элементарных шагов, тогда алгоритм не определен на этом слове. Алгоритм должен обладать свойством *детерминированности*, т.е. каждый элементарный шаг определяется предыдущей ситуацией. Наконец, выполнение вычислений определяется только предписанием (программой) и не зависит от внешних факторов.

Точное (математическое) понятие алгоритма было дано А.Тьюрингом в 1936 году, которое получило название *машины Тьюринга*. А.Тьюринг привел ряд доводов в пользу того, что любые вычислительные процедуры могут быть реализованы на его машине.

ТЕЗИС ЧЕРЧА – ТЬЮРИНГА: *Все интуитивно вычислимые функции*

являются эффективно вычислимыми.

1.1. Машина Тьюринга

М а ш и н а Т ь ю р и н г а снабжена потенциально бесконечной памятью - лентой, разделенной на ячейки, где накапливается информация. В каждый момент количество информации конечно и не имеет верхней грани. На ленте записывается входное слово, черновая работа и выходное слово. Это - слова над внешним алфавитом A**.** У нас алфавит A = {0, 1} предназначен для вычисления арифметических функций $f: N^k \to N$.

Собственно машина, которая осуществляет вычисление, имеет конечное число возможных "состояний" – внутренний алфавит $Q = \{q_0, q_1,...,q_s\}$, и преставляет собой конечный список правил вида: $q_i a \to b \delta q_j$, где i= 1,...,s; j=0,...,s; $\delta \in \{R,L,S\}$; $a,b \in A$; $q_i, q_j \in Q$. В каждой ячейке рабочей части ленты записан один из символов внешнего алфавита. В каждый момент времени t=0,1,... считывается содержимое одной ячейки и, согласно команде $q_i a \to b \delta q_j$,, символ a заменяется символом b и происходит сдвиг на следующую ячейку, соответственно, вправо (R), влево (L), на месте (S), после чего управление передается команде $q_j c \to ...$, где c - символ ячейки, куда сдвинулась головка. Состояние q_0 означает прекращение работы машины.

Машина Тьюринга вычисляет частичную арифметическую функцию $f^{(k)}(x_{1,...,}x_k)$, если машина Тьюринга всякий набор $(a_1, ...,a_k) \in$ Arg f перебатывает в число $b=f^{(k)}(a_1,...,a_k)$. Функция называется вычислимой на машине Тьюринга, если существует вычисляющая ее машина.

Для удобства вычислений договоримся о следующем: 0 будет изображаться |, 1,соответственно, - || и т.д. ; вычисления начинать с левого конца слова, записанного на

ленте машины, и заканчивать в начале заключительного слова, стерев предварительно черновую работу; кортежи изображать наборами | с пробелами - 0.

Примеры вычислений на машине Тьюринга :

1. “x+y”:

$q_1 1 \to 1Rq_1$
$q_1\ 0 \to 1Lq_2$
$q_2\ 1 \to 1Lq_2$
$q_2 0 \to 0Rq_3$
$q_3 1 \to 0Rq_4$
$q_4 1 \to 0Rq_0$

2. “rm(x,3)”:

$q_1 1 \to 0Rq_2$
$q_2 1 \to 0Rq_3$
$q_3\ 1 \to 0Rq_4$
$q_4 1 \to 0Rq_2$
$q_2\ 0 \to 1Sq_0$
$q_3 0 \to 1Lq_2$
$q_4\ 0 \to 1Lq_3$

3. ‘$\chi_{x<y}(x,y)$”:

$q_1\ 1 \to 1Rq_1$
$q_1 0 \to 0Lq_2$
$q_2 1 \to 0Lq_3$
* $q_3 1 \to 1Rq_4$
$q_4 0 \to 0Rq_4$
$q_4\ 1 \to 0Rq_5$
* $q_5 1 \to 1Lq_6$
$q_6 0 \to 0Lq_6$
$q_6 1 \to 1Sq_2$
$q_3 0 \to 0Sq_7$
$q_7 0 \to 0Rq_7$
$q_7 1 \to 0Rq_8$

$$(x=y)\begin{cases} q_8 0 \to 1Lq_{11} \\ q_{11} 0 \to 1Sq_0 \end{cases}$$

$$(x<y)\begin{cases} q_8 1 \to 1Sq_9 \\ q_9 1 \to 0Rq_9 \\ q_9 0 \to 1Sq_0 \end{cases} \qquad (x\geq y)\begin{cases} q_5 0 \to 0Sq_{12} \\ q_{12} 0 \to 0Lq_{12} \\ q_{12} 1 \to 1Sq_{13} \\ q_{13} 1 \to 0Lq_{13} \\ q_{13} 0 \to 0Sq_8 \end{cases}$$

1.2. Частично рекурсивные функции

Второе направление уточнения понятия алгоритма проходило по пути уточнения класса вычислимых объектов (вычислимых функций и разрешимых множеств). Рассмотрим здесь систему С.Клини - класс рекурсивных функций. Доказано, что вычислимая на машине Тьюринга функция является рекурсивной и, наоборот, для всякой рекурсивной функции найдется вычисляющая ее машина Тьюринга. Это говорит об эквивалентности данных определений. В настоящее время известно несколько эквивалентных понятий алгоритма и вычислимости (машины Тьюринга, нормальные алгоритмы Маркова, продукции Поста, Эрбран-Геделевское исчисление равенств, частично рекурсивные функции С.Клини и др.) .

1.2.1. Класс примитивно рекурсивных функций

Начнем с определения простейшего класса рекурсивных функций – класса примитивно рекурсивных функций, строящегося из базисных функций с помощью вычислимых операторов.

Базисные примитивно рекурсивные функции: O(x)=0 ; S(x)=x+1 (функция следования); $I_i^n(x_1,...,x_n)$(i=1,…,n) (проектирующие функции).

Вычислимые операторы:

1) Оператор суперпозиции C[g,g_1,…,g_m] = f:

$$g^{(m)}(g_1^{(n)}(x_1,\dots x_n),\dots,g_m^{(n)}(x_1,\dots,x_n)) = f(x_1,\dots,x_n).$$

$(x_1,\ldots,x_n)$|- $g_1^{(n)}(x_1,\ldots x_n) = y_1,\ldots, g_m^{(n)}(x_1,\ldots,x_n) = y_m$ |-$(y_1,\ldots,y_m)$|- $g(y_1,\ldots,y_m) = f(x_1,\ldots,x_n)$, останов.

2) Оператор примитивной рекурсии $R(g^n,h^{n+2}) = f^{n+1}$:

$$\begin{cases} f^{(n+1)}(0,x_1,\ldots,x_n) = g^{(n)}(x_1,\ldots x_n) \\ f^{(n+1)}(y+1,x_1,\ldots,x_n) = h^{(n+2)}(y,x_1,\ldots x_n, f(y,x_1,\ldots,x_n)) \end{cases}$$

(рекурсия ведется только по одному аргументу и функция на каждом шаге вычисляется через себя же на предыдущем шаге).

Вычислим функцию f на кортеже (x,y,z): (0,y,z) |- (y,z) |- g(y,z)=w_0, останов, если x=0 (где w_0=f(0,y,z)), а если x≠0, то (1,y,z) |-(o,y,z,w_0) |- h(0,y,z,w_0) = w_1, останов, если x=1 (где w_1=f(1,y,z)) и т.д.

В частности, для одноместной функции f(y) = $\begin{cases} f(0) = a \\ f(y+1) = h(y, f(y)) \end{cases}$.

Примеры примитивно рекурсивных функций (прф):

1^0. Неправильная суперпозиция задает ПРФ.

Покажем это на примере: g (g_1(x), g_2(x,z), g_3(y,z)) = f(x,y,z).

Сведем эту суперпозицию к правильной: f(x,y,z) = g(g_1(x), g_2(x,z),g_3(y,z))= g(g_1(x),g_2(x,z),g_3(y,z))=g($g_1(I_1^3(x,y,z))$,$g_2(I_1^3(x,y,z), I_3^3(x,y,z))$,$g_3(I_2^3(x,y,z), I_3^3(x,y,z))$)

=g($\tilde{q}_1$(x,y,z), $\tilde{q}_2$(x,y,z), $\tilde{q}_3$(x,y,z)).

2^0. Введение (удаление) фиктивных переменных сохраняет примитивную рекурсивность функций. Покажем на примере:

Пусть f(x,y) – ПРФ и g(x,y,z) = f(x,y). Тогда g(x,y,z) = f(x,y) = $f(I_1^3(x,y,z), I_2^3(x,y,z))$ - имеет примитивно рекурсивное описание.

3^0. f (x,y) = x+y

$$= \begin{cases} f(0,y) = 0 + y = y = I_1^1(y) \\ f(x+1,y) = (x+1) + y = (x+y) + 1 = f(x,y) + 1 = s(f(x,y)) = sI_3^3(x,y,f(x,y)) \end{cases};$$

4^0. Усеченная разность $x \dot{-} y = \begin{cases} x - y, & \text{если } x \geq y \\ 0 & \text{- в противном случае} \end{cases}$

Свойства усеченной разности:

(1) $x \dot{-} y = S(x) \dot{-} S(y)$

(2) $x + (y \dot{-} x) = y + (x \dot{-} y)$

(3) $x \dot{-} (y+z) = (x \dot{-} y) \dot{-} z$

(4) $(x \dot{-} y) \dot{-} z = (x \dot{-} z) \dot{-} y$

Докажем свойство (3): Индукция по y :

Базис y =0: $x \dot{-} (0+z) = x \dot{-} z = (x \dot{-} 0) \dot{-} z$.

Индукционный шаг: $x \dot{-} (y+z) = (x \dot{-} y) \dot{-} z$ (индукционное допущение).

Докажем равенство : $x \dot{-} (y'+z) = (x \dot{-} y') \dot{-} z$ ('y' - фиксировано).

Индукция по x (внутри индукционного шага по y):

Базис: $x = 0$: $0 \dot{-} (y'+z) = (0 \dot{-} y') \dot{-} 0$.

Индукционное допущение по x: $x \dot{-} (y'+z) = (x \dot{-} y') \dot{-} z$ (x ,y – фиксированы).

Докажем для x': $x' \dot{-} (y'+z) = x' \dot{-} S(y+z) =$ (по свойству 1) $x \dot{-} (y+z) =$ (по индукционному допущению по y) $(x \dot{-} y) \dot{-} z$;

$(x' \dot{-} y') \dot{-} z =$ (по свойству 1) $(x \dot{-} y) \dot{-} z$. Таким образом, для всех x, $x \dot{-} (y'+z) = (x \dot{-} y') \dot{-} z$, откуда для всех y :

$x \dot{-} (y+z) = (x \dot{-} y) \dot{-} z$, ч.т.д.

Рассмотрим частный случай усеченной разности:

$J(x)=x \dot{-} 1 = \begin{cases} x-1, & \text{если } x \geq 1 \\ 0, & \text{если } x < 1 \end{cases}$. Докажем ее примитивную рекурсивность:

$$\begin{cases} J(0) = 0 \dot{-} 1 = 0 \\ J(x+1) = (x+1) \dot{-} 1 = (x+1) \dot{-} 1 = x = I_1^2(x, J(x)) \end{cases}.$$

Примитивно рекурсивное описание функции $x \dot{-} y$:

$x \dot{-} 0 = x = I_1^1(x)$

$x \dot{-} y' = x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1 = J(x \dot{-} y)$, далее из примера 2^0.

5^0. Модуль разности $|x - y|$ - ПРФ (см. упражнение).

7^0. $sg(x)= \begin{cases} 1, x > 0 \\ 0, x = 0 \end{cases}$, $\overline{sg}(x) = 1 \dot{-} x$ - ПРФ (см. упражнение)

8^0. Остаток от деления 'x' на 'y', т.е. rm (x,y) – ПРФ :

$$\begin{cases} rm(0, y) = 0 \\ rm(x+1, y) = \begin{cases} 0, \text{ если } y \dot{-} rm(x, y) = 1 \\ rm(x, y) + 1, \text{ если } y \dot{-} rm(x, y) \neq 1 \end{cases} \end{cases}$$

$= S(rm(x,y))\, sg\, |y - S(rm(x,y))|$.

9^0. $\tau(x)$ – число делителей числа x - ПРФ (см упражнение).

Оператор минимизации (μ - оператор) : $\mu[g] = f$

$f(x_1,\ldots,x_n) = \mu z\, (g(x_1,\ldots,x_n,z) = 0)$:

$(x_1,\ldots,x_n) \vdash g(x_1,\ldots,x_n,0)$ $\begin{cases} = 0, останов \\ \neq 0 - g(x_1,...,x_n,1) \begin{cases} = 0 \\ \neq 0 - g(x_1,...,x_n,2) \_ u \_ m.д. \end{cases} \end{cases}$

Эта процедура может быть бесконечна, тогда появляются точки разрыва, т.е. μ - оператор может порождать не всюду определенные функции.

О г р а н и ч е н н ы й μ - о п е р а т о р : $f(x_1,\ldots,x_n) = \mu z \le a\ (g(x_1,\ldots,x_n,z)=0)$.
Заметим, что если на интервале [0, a] для всех z $g(x_1,\ldots,x_n,z) \neq 0$, то в точке $(x_1,...,x_n)$ функция $f(x_1,\ldots,x_n)$ может быть доопределена (в отличие от случая задания функции посредством произвольного μ - оператора, где в этом случае может быть нарушена однозначность функции).
10^0. Ограниченный μ - оператор определяет примитивно рекурсивные функции. Докажем на примере функции $f(x) = \mu z \le a\ (g(x,z) = 0)$:

$g(x;0) \neq 0$
$g(x,0)g(x;1) \neq 0$
•••
$g(x,0)g(x,1)...g(x,i) = 0$
•••
$g(x,0)g(x,1)... g(x,a)$

Тогда $f(x) = \mu z \le a\ (g(x,z) = 0) = \sum_{j=0}^{a} sg \prod_{i=0}^{j} g(x;i)$.

Множество (отношение, предикат) называют *примитивно рекурсивным, если такова его характеристическая функция.*
11^0. Свойство ‘быть простым числом’ представимо предикатом $Pr(x) \equiv (\tau(x) = 2) \equiv (|\tau(x) - 2| = 0)$, т.ч. $\chi_{Pr}(x) = sg\ |\tau(x) - 2|$, т.е. Pr (x) – ПРП.

Последовательность простых чисел: $P_0 = 2, P_1 = 3, P_2 = 5, P_3 = 7, ...$

12^0. $\pi(x)$ - число простых чисел, предшествующих x, –ПРФ (см. упражнение).

13^0. Функция $P_n = P(n)$ - (n+1)- е простое число - ПРФ:

$P_{n+1} = \mu z \le 2^{2^{(n+1)}}\ (\pi(z) = n+2) = \mu z \le 2^{2^{(n+1)}}\ (|\pi(z) - (n+2)| = 0)$.

Покажем, что $P_{n+1} < 2^{2^{(n+1)}}$:

$P_0 \le 2^{2^0} = 2$

$P_1 \le 2^{2^1} = 4$

•••

$P_n \le 2^{2^n}$.

Докажем, что $P_{n+1} \le 2^{2^{n+1}}$, перемножая вышестоящие неравенства:

$P_0 P_1 \ldots\ldots P_n \le 2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^n} \Big|$

$P_0 P_1 \ldots\ldots P_n + 1 \le 2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^n} + 1$

$= 2^{2^0+\ldots+2^n} + 1 = 2^{1+\ldots+2^n} + 1 = 2^{\frac{1(2^n-1)}{2-1}} + 1 = 2^{2^n} + 1 \le 2^{2^{n+1}}$,т.ч. $P_0P_1...P_n+1 < 2^{2^{(n+1)}}$.

Т.к. для всех j = 1,...,n P_j не делит $P_0P_1...P_n+1$, представление $P_0P_1...P_n+1$ в виде произведения степеней простых чисел начинается с некоторого P_k, где $k \ge n+1$, так что $P_{n+1} \le P_k^{\alpha_k} \ldots = P_0P_1...P_n+1 \le 2^{2^{n+1}}$, т.е. $P_{n+1} \le 2^{2^{n+1}}$.

14⁰. Пусть $n = P_0^{\alpha_0} \cdot \ldots \cdot P_k^{\alpha_k} \cdot \ldots \cdot P_m^{\alpha_m}$, то $\alpha_k = \exp(n,x)$ – ПРФ.

Для доказательства воспользуемся ограниченным μ-оператором:

$\alpha_k = \exp(n,k) = \mu\, z \le n\, (\overline{sg}\,(rm\,(n, P_k^{z+1})) = 0)$.

15⁰. x = y, x ≤ y - ПРО (см. упражнение).

16⁰. Конечное множество - ПРМ. Покажем это на примере множества A={a,b}. Его характеристическая функция $\chi_A(x) = \begin{cases} 0, \text{если } x = a \vee x = b \\ 1, \text{если } \neg(x = a \vee x = b) \end{cases}$

Таким образом, $\chi_A(x) = sg(|x - a| \cdot |x - b|)$ - ПРФ.

ТЕОРЕМА. Класс примитивно рекурсивных множеств (отношений) замкнут относительно операций ∩,∪, — (дополнение). Т.е. если A,B - ПРМ, то A∩B, A∪B, A - ПРМ.

Доказательство проведем для ∪: {A∪B - ПРМ↔$\chi_{A\cup B}$ - ПРФ)

1 A,B - ПРФ

2 χ_A, χ_B - ПРФ (по определению ПРМ)

3. $x \in A\cup B \leftrightarrow x \in A \vee x \in B \leftrightarrow \chi_A(x) = 0 \vee \chi_B(x) = 0 \leftrightarrow \chi_A(x)\chi_B(x) = 0$,
т.е. $\chi_{A\cup B}(x) = \chi_A(x) \cdot \chi_B(x)$ – ПРФ.

ТЕОРЕМА. Класс ПРП замкнут относительно &, ∨, ¬.

Доказательство проведем для &: P(x), Q(x) - ПРП, т.е. χ_P, χ_Q - ПРФ. Тогда $\chi_{P\&Q} = sg(\chi_P + \chi_Q)$ - ПРФ.

17⁰. Примитивную рекурсивность функции - константы $C_q^n(x_1,\ldots,x_n) = q$ можно доказать индукцией по n (см. упражнение).

ТЕОРЕМА. Класс ПРП замкнут относительно ограниченных кванторов.

Доказательство. P(x) - ПРП, докажем ПРП ∃x≤a P(x):

$$\begin{cases} P(0) = P(C_0^1(x)) \\ P(1) = P(C_1^1(x)) \\ \ldots \\ P(a) = P(C_a^1(x)) \end{cases}$$

∃x≤a P(x) ~ P (0) ∨...∨ P (a), что доказывает примитивную рекурсивность ограниченного квантора ∃. (Аналогично для ограниченного квантора ∀).

Возвратная рекурсия

Функция $f(x_1,\ldots,x_n,y)$ получается из функций g^n, h^{n+s+1}, $\alpha_1,\ldots,\alpha_j$

возвратной рекурсией, если она определена схемой:

$$\begin{cases} f(x_1,\ldots,x_n,0) = g(x_1,\ldots,x_n) \\ f(x_1,\ldots,x_n,y+1) = h(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,\alpha_1(y+1)),\ldots,f(x_1,\ldots,x_n,\alpha_j(y+1))). \end{cases}$$

где функции $\alpha_i(y+1) \le y$ $(i=1,\ldots,j)$ задают один из предыдущих шагов.

ТЕОРЕМА. Возвратная рекурсия сводится к примитивной рекурсии, т.е. функция, заданная возвратной рекурсией - примитивно рекурсивна.

Д о к а з а т е л ь с т в о. Введём вспомогательную функцию

$F(x_1,\ldots,x_n,y) = \prod_{i=0}^{y} P_i^{f(x_1,\ldots,x_n,i)}$. Покажем, что $F(x_1,\ldots,x_n,y)$ – ПРФ,

откуда $f(x_1,\ldots,x_n,y) = \exp(F(x_1,\ldots,x_n,y),y)$ также ПРФ.

$$\begin{cases} F(x_1,\ldots,x_n,0) = P_0^{f(x_1,\ldots,x_n,0)} = P_0^{g(x_1,\ldots,x_n)} = G(x_1,\ldots,x_n) \\ F(x_1,\ldots,x_n,y+1) = \prod_{i=0}^{y+1} P_i^{f(x_1,\ldots,x_n,i)} = F(x_1,\ldots,x_n,y) P_{y+1}^{f(x_1,\ldots,x_n,y+1)} = \end{cases}$$

$$F(x_1,\ldots,x_n,y) P_{y+1}^{h(x_1,\ldots,x_n,y,\exp(F(x_1,\ldots,x_n,y),\alpha_1(y+1)),\ldots,\exp(F(x_1,\ldots,x_n,y),\alpha_j(y+1)))} =$$

$=H(x_1,\ldots,x_n,F(x_1,\ldots,x_n,y))$. Таким образом, $F(x_1,\ldots,x_n,y)$ – ПРФ, ч.т.д.

Пример функции, задаваемой возвратной рекурсией - числа Фибоначчи :

$F(0)=1$, $F(1)=1$, $F(n+2)=F(n)+F(n+1)$.

Упражнение

1. Построить машины Тьюринга, вычисляющие функции: $2\bullet x$, $|x - y|$, $sg\, x$, $\max(x,y)$, $\min(x,y)$, $x \dot{-} y$, $[x/2]$, $[\sqrt{x}]$, $[x/y]$, $x \bullet y$.
2. Построить машины Тьюринга, вычисляющие простейшие ПРФ: O, S, I^n, и машины, моделирующие операторы : суперпозиции, примитивной рекурсии, ограниченный μ- оператор.
3. Построить машины Тьюринга, разрешающие отношения: $x = y$, $x \ge y$, $x + 2 \le y$, ‘x – четное’, ‘3 делит x’, ‘$x = y \pmod 4$’, ‘$x \dot{-} 3 = y$’.
4. Доказать, тотальность (всюду определенность) ПРФ.
5. Доказать примитивную рекурсивность функций из примеров 5^0, 6^0, 7^0, 9^0, 10^0, 12^0,14^0, 16^0,17^0 , 19^0.
6. Доказать, что функции f и g – ПРФ, если функции h_1, h_2 – ПРФ:

$$\begin{cases} f(0) = a, g(0) = b, \\ f(x+1) = h_1(x, f(x), g(x)), \\ g(x+1) = h_2(x, f(x), g(x)). \end{cases}$$

7. Доказать ПРФ: d (x,y)(нод) и k (x,y)(нок).
8. Доказать ПРФ long(x) – номер наибольшего простого делителя числа x.
9. Доказать, что график ПРФ есть ПРМ.
10. Доказать, что сумма делителей числа ‘x’ есть ПРФ.
11. Доказать, что число простых делителей числа ‘x’ есть ПРФ.
12 .Доказать, что множество значений возрастающей функции есть ПРМ.
13. Доказать, что всякая ПРФ может быть получена из функций S(x), q (x) = x $\dot{-}$ $[\sqrt{x}]^2$ с помощью операций суперпозиции, итерации[3] и сложения двух функций (*теорема Робинсона*).

14.
$$g(x_1,\ldots,x_n) = \begin{cases} \varphi_1(x_1,\ldots,x_n), \text{ если } f_1(x_1,\ldots,x_n) = 0, \\ \bullet\bullet\bullet \\ \varphi_s(x_1,\ldots,x_n), \text{ если } f_s(x_1,\ldots,x_n) = 0, \end{cases}$$

где $\varphi_{1,\ldots,}\ \varphi_s, f_1,\ldots,f_s$ – ПРФ и одно и только одно из условий $f_i = 0$ (i=1,…,s) имеет место. Доказать, что g – ПРФ.
15. Доказать, что функция f (x), получающаяся с помощью оператора примитивной рекурсии из числа ‘a’ и функции ‘g(x,y)’, может быть получена с помощью операторов итерации[1)] и суперпозиции из ‘a’ и функций g, O, S, I^n и c, l, r[2)].
16. Класс функций, строящихся из простейших функций O,S, I^n с помощью операторов суперпозиции, примитивной рекурсии и ‘тотального’ μ-оператора, называют *общерекурсивными (или рекурсивными) функциями*.
Доказать, что существует в точности $\aleph_0$ рекурсивных функций;
17. Приведем пример общерекурсивной функции A(x), не являющейся, примитивно рекурсивной, *функции Аккермана* :

$$B(0,y) = 2+y,$$
$$B(x+1,0) = sg(x),$$
$$B(x+1,y+1) = B(x,B(x+1,y)),$$

где A(x) = B(x,x). (Доказательство см. в [3]).

---

1 f(0)=0, f(x+1)=g(f(x))
2 канторовские функции [см следующую тему]

Канторовская нумерация

Канторовская нумерация есть нумерация пар и n - ок натуральных чисел. Расположим упорядоченные пары натуральных чисел в порядке возрастания суммы их членов, а в группах с одинаковой суммой - по возрастанию первого члена:

(0,0)<(0,1)<(1,0)<...<(0,x+y)<...<(x,y)<...<(x+y,0)<...

S=0 S=1 S=x+y

Число членов в группе с суммой S равно S+1. Обозначим через c(x,y) канторовский номер пары (x,y), который равен числу пар, предшествующих паре (x,y). Таким образом, c(0,0)=0, c(0,1)=1, c(1,0)=2,...,

c(x,y)=1+2+...+(x+y)+x=(1+x+y)(x+y)/2+x=C^2_{x+y+1}+x.

Покажем, что отображение c:NxN→N взаимно однозначно «на». Однозначность c(x,y) очевидна, т.к. (x,y) = (a,b) ↔ x = a & y = b, откуда c(x,y) = c(a,b). Доказательство обратной однозначности функции c(x,y) проведем средствами формальной арифметики, определяя отношение x>a формулой ∃r (r>0&x=a+r). Докажем импликацию: c(x,y) = c(a,b)→(x,y)=(a,b):

1. c(x,y)=c(a,b) (допущение)
2. $C^2_{x+y+1} + x = C^2_{a+b+1} + a$
3. (x,y) ≠ (a,b) (допущение противного)
4. ¬(x = a & y = b)
5. x ≠ a ∨ y ≠ b (по закону де Моргана)

6а. x ≠ a (допущение) 6б. y ≠ b (допущение)

7а. x > a ∨ x < a 7б. y < b ∨ y > b

8а′. x>a (допущение) 8а″. x<a (допущение) 8б. x≠a(допущение противного)

9а′. ∃r (r>0&x=a+r)

10′а′. r>0&x=a+r (допущение) •••

11′а′. r>0 (удаление &) (далее, как на ветке (а),

12′а′. x=a+r (удаление &) получаем противоречие)

13′а′. $C^2_{a+r+y+1} + a + r = C^2_{a+b+1} + a$ 9б. x = a (введ.¬, удал.¬)

14′а′. $C^2_c + a + r = C^2_{a+b+1} + a$ &c=a+r+y+1 10б. $C^2_{a+y+1} + a = C^2_{a+b+1} + a$

15′а′. $C^2_c + r = C^2_{a+b+1}$ 11б. $C^2_y = C^2_b$

16′а′. $C^2_c < C^2_{a+b+1}$ 12б. y=b

17′а′. $C^2_c + r < C^2_c + c = C^2_c + C^1_c = C^2_{c+1}$ 13б. противоречие

18′а′. $C^2_{a+b+1} < C^2_{c+1}$

19′а′. a+r+y+1<a+b+1 (из 16′а′ и свойств C^2_x)

20′а′. y+r < b (из 19′а′)

21′а′. ∃s (s>0&b= y+r+s)

22″а′. s>0&b=y+r+s (допущение)

23″а′. s>0 (удаление &)

24″a′. b=y+r+s (удаление &)

25″a′. $C^2_{a+b+1} = C^2_{a+r+y+s+1} = C^2_{c+s}$ & s>0

26″ a′. $C^2_{c+1} < C^2_{c+s}$ &s>0 (из 18′a′ и 25″a′), т.е. противоречие

27′a′. противоречие (удал.∃,21′a′) •••

28 a′ противоречие (удал.∃,9a′) 28a″. противоречие (получено как на a′)

29a. противоречие (удал.∨,7a)

30. противоречие (удаление∨, 5)

31.(x,y) = (a,b) (введение ¬ ,3, удал.¬)

32 c(x,y) = c(a,b) → (x,y) = (a,b) (введ.→,1,31).

Покажем, что c(x,y) есть отображение «на», т.е. ∀n∈N ∃(x,y) n = c(x,y).
Доказательство проведем индукцией по n.

Базис: n=0 → c(0,0)=0, n=1 → c(0,1)=1.

Индукционный шаг: n = c(x,y) = $C^2_{x+y+1} + x$ (индукционное допущение)

$$n+1 = C^2_{x+y+1} + x + 1 = C^2_{(x+1)+(y+1)+1} + (x+1) = c(x+1, y-1),$$

если y>0.

$$n+1 = C^2_{x+1} + x + 1 = C^2_{x+2} = C^2_{0+(x+1)+1} + 0 = c(0, x+1),$$ если y=0,

так как (x,0) < (0,x+1) и c(x,0) = n, то n+1 = c(0,x+1).

Обратные канторовские функции l(n), r(n): c(l(n),r(n)) = n и l(n) ≤ n, r(n) ≤ n. Как следует из их описания в [3], обратные канторовские функции l(c(x,y)), r(c(x,y)) примитивно рекурсивны.

Определим по индукции *канторовские функции для произвольной n-ки*:
$c^{n+1}(x_1,...,x_{n+1}) = c(c^n(x_1,...,x_n),x_{n+1})$. Если $c^n(x_1,...,x_n) = z$, то
$x_n = r(z)$, $x_{n-1} = rl(z)$, $x_{n-2} = rll(z)$, . . . , $x_2 = r\underbrace{l....l}_{n-2}(z)$, $x_1 = \underbrace{l....l}_{n-1}(z)$,
которые, очевидно, также примитивно рекурсивны.

Упражнение

1.Пусть $\pi(x,y)=2^x(2y+1)-1$. Покажите, что π - вычислимая биекция из N^2 в N и что обратные функции π_1, π_2 такие, что $\pi(\pi_1(z),\pi_2(z))=z$, вычислимы.

2. Нумерацию n-ок можно задать как $\tau(a_1,\ldots,a_n) = 2^a\, 2^{a+a+1}\, 2^{a+\ldots+a+n-1}$?

1.2.2. Рекурсивно перечислимые множества и предикаты

Класс функций, построенных из базисных функций o(x), s(x), $J_i^n(x_1,...,x_n)$ (i=1,…,n) с помощью операторов C, R, μ, называется классом *частично рекурсивных функций* (ЧРФ). Если ограничиться тотальным μ - оператором (порождающим тотальные функции), то получим класс всюду определенных ЧРФ или *общерекурсивных функций* (ОРФ).

ТЕЗИС ЧЕРЧА-КЛИНИ: *Любая интуитивно вычислимая функция является частично рекурсивной функцией.*

Подобно тому, как с примитивно рекурсивными функциями были соотнесены примитивно рекурсивные множества (отношения и предикаты), так и с частично рекурсивными (общерекурсивными) функциями соотносятся рекурсивно перечислимые (рекурсивные) множества (отношения и предикаты).

Множество (отношение, предикат) называют **рекурсивно перечислимым,** ***если найдется ПРФ g такая, что соответственно***

$x \in A \leftrightarrow \exists y\,(g(x,y)=0)$ $(P(x) \leftrightarrow \exists y\,(g(x,y)=0))$

УТВЕРЖДЕНИЕ 1. Всякое примитивно рекурсивное множество (предикат) является рекурсивно перечислимым. Обратное не верно.

Д о к а з а т е л ь с т в о по определению.

ТЕОРЕМА. (1) Класс рекурсивно перечислимых множеств замкнут отно -сительно операций $\cap, \cup$.

(2) Класс рекурсивно перечислимых предикатов замкнут относительно операций $\&, \vee, \exists$.

Д о к а з а т е л ь с т в о. Докажем некоторые из утверждений.

(1) Пусть A,B – рекурсивно перечислимые множества, докажем для $A \cap B$:

$x \in A \cap B \leftrightarrow x \in A \,\&\, x \in B \leftrightarrow \exists\, y\,(g(x,y)=0) \,\&\, \exists\, y\,(f(x,y)=0)$ (где f,g – ПРФ) $\leftrightarrow$

$\leftrightarrow \exists\, y\,(g(x,y)=0 \,\&\, \exists\, y\,(f(x,y)=0)) \leftrightarrow \exists\, y\, \exists\, z\,(g(x,y)=0 \,\&\, f(x,z)=0) \leftrightarrow$

$\leftrightarrow \exists\, n\,(n=c(y,z) \,\&\, g(x,l(n))=0 \,\&\, f(x,r(n))=0) \leftrightarrow \exists\, n\,(g(x,l(n))+f(x,r(n))=0) \leftrightarrow$

$\leftrightarrow \exists\, n\,(\Phi(x,n)=0)$, где Ф – ПРФ, как суперпозиция ПРФ.

(2) Пусть P(x,y) – РПП, докажем для $\exists\, y\, P(x,y)$: $P(x,y) \leftrightarrow \exists\, z\,(f(x,y,z)=0)$,

$\exists y\, P(x,y) \leftrightarrow \exists y \exists z\,(f(x,y,z)=0) \leftrightarrow \exists n\,(n=c(y,z) \,\&\, f(x,l(n),r(n))=0) \leftrightarrow \exists n\, \Phi(x,n)=0)$,

где Ф – ПРФ, как суперпозиция ПРФ.

УТВЕРЖДЕНИЕ 2**.** Если f – ПРФ, то Val f (множество значений функции f) – РПМ.

УТВЕРЖДЕНИЕ 3. Если f – ПРФ и f – монотонно возрастает, то Val f – ПРМ.

Доказательство проведем для случая, когда Val f бесконечно. Допустим, что $\neg\exists\, x{\le}y\ (y = f(x))$. Тогда $\forall\, x\ (x > y \vee y \neq f(x))$, т.е.

$\forall\, x\ (y = f(x) \rightarrow x > y)$. Ввиду того, что функция f монотонно возрастает:

$x > y \rightarrow f(x) > f(y)$, или $x > y = f(x) > f(y) = ff(x)$. Отсюда $x > y = f(x) > ff(x) > > fff(x)$ и т.д., так что на конечном интервале [0,y] располагается бесконечно много натуральных чисел, что составляет противоречие. Следовательно, $y \in \mathrm{Val}\ f \leftrightarrow \exists\, x \le y\ (y = f(x))$, т.е. Val f – ПРМ.

ТЕОРЕМА (*Н. и д. условие рекурсивной перечислимости множеств*).

$A \neq \varnothing$, то A – РПМ $\leftrightarrow \exists$ f – ПРФ ($A = \mathrm{Val}\ f$).

Доказательство. 1. $\varnothing \neq A$ и A – РПМ (допущение)

2. $b \in A$ (допущение)
3. $x \in A \leftrightarrow \exists\, y\ (g(x,y)=0)$, где g – ПРФ.
4. $x \in A \rightarrow \exists y\ (g(x,y)=0)$
5. $x \in A$ (допущение)
6. $\exists y\ (g(x,y)=0)$ ($\rightarrow$ удаление)
7. $g(x,y)$ (допущение)
8. найдем $z = \mu y\ (g(x,y)=0)$
9. и по паре (x,z) вычисляем $c(x,z)=t$.

Положим $f(t) = l(t)\ \overline{sg}\ g(l(t),r(t))+b\ sg\ g(l(t),r(t))$. Тогда очевидно $A = \mathrm{Val}\ f$.

Обратно, если $A=\mathrm{Val}\ f$, где f – ПРФ, то, по утверждению 2, A – РПМ.

ТЕОРЕМА (*Поста*)**.** Если множества A, $\overline{A}$ – РПМ, то A (тогда и $\overline{A}$) -рекурсивное множество.

Доказательство. Множества A, $\overline{A}$ – РПМ, поэтому существуют ПРФ f, g, такие, что $x \in A \leftrightarrow \exists y(g(x,y)=0)$, $x \in \overline{A} \leftrightarrow \exists y\ (f(x,y)=0)$. Функция $h(x) = \mu\, y\ (f(x,y)\cdot g(x,y)=0)$ – ОРФ, т.к. $f(x,y)g(x,y)=0$ определено для любого x. Тогда, очевидно, $\chi_A(x) = sg\ f(x,h(x))$ – ОРФ, следовательно, A – рекурсивное множество. Обратное также верно.

Упражнение

1. Доказать, что каждое бесконечное рекурсивно перечислимое множество перечислимо некоторой общерекурсивной 1-1 – функцией.
2. Доказать, что множество, перечислимое строго возрастающей общерекурсивной функцией, рекурсивно.
3. Доказать, что если два множества A и B отличаются конечным числом элементов и одно из них рекурсивно перечислимо (рекурсивно), то таково же и другое множество.
4. Доказать, что всякое рекурсивно перечислимое множество содержит бесконечное рекурсивное подмножество.
5. Пусть f – тотальная вычислимая функция, A – рекурсивное множество, а B – РПМ Показать, что множество $f^{-1}(A)$ рекурсивно и что множества f(A), f(B) и $f^{-1}(B)$ - РПМ, но не обязательно рекурсивны. Что еще можно сказать об этих множествах, если f есть биекция?

1.2.3. Порожденные множества

Алгеброй называют непустое множество $A\neq\varnothing$ с определенными на нем частичными операциями $F^{(m)}: A^m\to A$.

Непустое подмножество множества A, замкнутое относительно операций алгебры A, называется *подалгеброй алгебры A*.

УТВЕРЖДЕНИЕ. Пусть $\varnothing\neq V\subset A$ и $\{A_i;\ i\in I\}$ – семейство подалгебр алгебры A, содержащих подмножество V. Тогда $\bigcap_{i\in I} A_i$ есть наименьшая подалгебра алгебры A, содержащая подмножество V, обозначим ее через <V>.

Д о к а з а т е л ь с т в о (см. упражнение).

ТЕОРЕМА. <V> = T, где T – множество всех значений термов в A.

Д о к а з а т е л ь с т в о (см. упражнение).

ТЕОРЕМА. Множество <V>, порожденное РПМ ‘V’ с помощью конечной системы ПРФ $\{F_i;\ i=1,\ldots,n\}$, будет РПМ.

Д о к а з а т е л ь с т в о.

1. Пусть V – РПМ, тогда существует ПРФ ‘v’ такая, что V = Val v.
2. <V> = $\{t(a_1,\ldots,a_m);\ a_1,\ldots,a_m\in V\}$, или, учитывая 1,
   <V> = $\{t(v(b_1),\ldots v(b_m));\ b_1,\ldots,b_m\in N\}$.
3. Закодируем v - термы: код терма v(b) есть 3^b;

   код $F_i(t_1,\ldots,t_{m_i})$ есть $2^i\cdot p_1^{C_1}\ldots p_{m_i}^{Cm_i}$,

   где $c_1,\ldots,c_{m_i}$ соответственно коды термов $t_1,\ldots,t_{m_i}$.

Очевидно, что не каждое натуральное число является кодом v-терма, но декодирование однозначно.

4. Строим функцию f таким образом, что f(n) есть значение v-терма с кодом n, если n - код v-терма, в противном случае f(n) есть значение какого-то v-терма:

$$\begin{cases} f(0)=v(0) \\ f(n+1)=\begin{cases} F_1(f(\exp(n+1,1)),\ldots,f(\exp(n+1),m_1)), \text{ если } \exp(n+1,0)=1 \\ \ldots \\ F_1(f(\exp(n+1,1)),\ldots,f(\exp(n+1),m_s)), \text{ если } \exp(n+1,0)=s \\ v(\exp(n+1,1)) \text{ – для остальных } n \end{cases} \end{cases}$$

или

$$\begin{cases} f(0)=v(0) \\ f(n+1)=G(n, f(\exp(n+1,1)),\ldots,f(\exp(n+1,t))), \text{ где } t=\max\{m_1,\ldots,m_s\}, \end{cases}$$

где $G(n,x_1,\ldots,x_t) =$

$$v(\exp(n+1,1))\cdot \operatorname{sg}\prod_{i=1}^{s}\left|\exp(n+1,0)-i\right| + \sum_{i=1}^{s} F_i(x_1,\ldots,x_{m_i})\overline{sg}\left|\exp(n+1,0)-i\right|$$

Функция f(x) задана возвратной рекурсией, следовательно, f – ПРФ.

5. Индукцией по n докажем, что $f(n)\in$<V> для всех n.

Базис: n=0 или n=1: $f(0) = f(1) = v(0)\in$<V>.

Индукционный шаг: Допустим, что $f(m)\in$<V> для всех $m \le n$ и докажем для f(n+1):

(1) (n+1) – код v-терма $F_i(t_1,\ldots,t_{m_i})$:

$n+1 = 2^i\cdot p_1^{A_1}\ldots p_{m_i}^{Am_i}$, где $A_1,\ldots,A_{m_i}$ – коды термов $t_1,\ldots,t_{m_i}$;

из 4: $f(n+1) = F_i(f(A_1),\ldots,f(A_{m_i}))$.

Так как $A_j \le n$ (j=1,…,m_i), то $f(A_j) = t_j$, так что $f(n+1) = F_i(t_1,\ldots,t_{m_i}) \in <V>$.

(2) (n+1) – не является кодом v-терма:
$exp(n+1,i) = A_i \le n$; из 4: $f(n+1) = F_i(f(A_1),\ldots,f(A_{m_i}))$ (i=1,..,s) или $f(n+1)=v(A_1)$.

Т.к. $A_j \le n$, то $f(A_j) = t_j$ (где t_j – терм, не обязательно с кодом A_j),
тогда $f(n+1) = F_i(t_1,\ldots,t_{m_i}) \in <V>$ или $f(n+1) = v(A_1) \in <V>$.

Таким образом, для всех n, $f(n) \in <V>$, т.е. Val f $\subset$ <V>. Обратное включение следует из построения функции f. Т.к. <V>=Val f, где f – ПРФ, тогда по утверждению 2, <V> - РПМ.

1.2.4. Функции на n - ках

Множество A n-ок натуральных чисел называется *примитивно рекурсивным* (*рекурсивным, рекурсивно перечислимым*), если таковым является множество C(A) номеров n-ок из A. Например, A – ПРМ, если явля ется ПРФ его характеристическая функция: $\chi_{C(A)}(z) = \chi_A(c_{n1}(z),\ldots,c_{nn}(z))$
или $\chi_{C(A)}(c(x_1,\ldots,x_n)) = \chi_A(x_1,\ldots,x_n)$. Доказанные прежде утверждения о множествах переносятся на множества n-ок.

ТЕОРЕМА (*О параметризации*). A – множество n – ок, $A \neq \varnothing$, то A – РПМ т. и т. т .,когда $\exists f_1,\ldots,f_n$ – ПРФ $\forall(x_1,\ldots,x_n) \in A$ $\exists t ((x_1,\ldots,x_n)=(f_1(t),\ldots,f_n(t))$.

Д о к а з а т е л ь с т в о. (1) Пусть $A \neq \varnothing$ – РПМ, тогда, по определению, C(A) – РПМ и по утверждению 2 C(A) = Val f, где f – ПРФ.
Тогда $\forall(x_1,\ldots,x_n) \in A$ $\exists t$ $C(x_1,\ldots,x_n)=f(t)$ и $x_i = C_{ni}(f(t)) = f_i(t)$, где f_i – ПРФ как суперпозиция ПРФ.
(2) Пусть $\exists f_1,\ldots,f_n$ – ПРФ $((x_1,\ldots,x_n) \in A \leftrightarrow \exists t (x_1,\ldots,x_n)=(f_1(t),\ldots,f_n(t)))$, тогда $C(x_1,\ldots,x_n)=C(f_1(t),\ldots,f_n(t))=f(t)$, т.е. f – ПРФ.
Таким образом, C(A)=Val f, т.е. C(A) - РПМ, следовательно, A – РПМ.

ТЕОРЕМА (*О графике ЧРФ*). f - ЧРФ $\leftrightarrow$ график f – РПМ .
(без доказательства)

Следствие 1. Область определения ЧРФ есть РПМ.

Следствие 2. *Множество значений ЧРФ есть РПМ.*

Следствие 3. Множество решений уравнения $f(x_1,\ldots,x_n)=0$, где f – ЧРФ, есть рекурсивно перечислимое множество (РПМ).
Д о к а з а т е л ь с т в о. $\alpha(x) = \mu t (x + t=0)$ – ЧРФ, определенная только для x=0. Тогда $\{(x_1,\ldots,x_n); f(x_1,\ldots,x_n) = 0\} = Arg\ \alpha(f(x_1,\ldots,x_n))$ – РПМ.

ТЕОРЕМА. Если $F^{(n)}$ – тотальная функция, график которой – РПМ, то $F^{(n)}$ – общерекурсивная функция (ОРФ).
Д о к а з а т е л ь с т в о. График $F = \{(x_1,\ldots,x_n,y);\ y = F(x_1,\ldots,x_n)\}$ - РПМ, то по теореме о параметризации существуют ПРФ $f_1,\ldots,f_n$, f_{n+1} такие, что $(x_1,\ldots,x_n,y) \in$ гр F $\leftrightarrow \exists$ t $((x_1,\ldots,x_n,y) = (f_1(t),\ldots,f_n(t),f_{n+1}(t)))$.
Так как $F(x_1,\ldots,x_n)=f_{n+1}(\mu t (|x_1-f_1(t)|+\ldots+|x_n-f_n(t)|) = 0)$, то F – ОРФ.

С функцией $F(\tau_1,\ldots,\tau_m)=\tau$, где $\tau_i = (x_{i1},\ldots,x_{in})$ (i=1,…,m), $\tau = (y_1,\ldots,y_n)$ связаны *координатные функции*: $y_j = f_j(x_{11},\ldots,x_{1n},\ldots, x_{m1},\ldots,x_{mn})$ (j=1,…,n)
и *представляющая функция:* $f(a_1,\ldots,a_n)=a$, где $a_i=C(\tau_i)$ (i=1,..,m), $a=C(\tau)$.

Функция $F(\tau_1,\ldots,\tau_m)=\tau$ называется ЧРФ (ОРФ, ПРФ), если такова её представляющая функция $f(a_1,\ldots,a_n) = a$.

УТВЕРЖДЕНИЕ. Функция $F(\tau_1,\ldots,\tau_m)=\tau$ - ЧРФ (ОРФ, ПРФ) т. и. т. т., когда таковы её координатные функции (представляющая функция).

Упражнение

1. Доказать, что:

a) функция, получающаяся с помощью оператора суперпозиции, из функций с рекурсивно перечислимым графиком, имеет рекурсивно перечислимый график;

b) функция, построенная посредством оператора примитивной рекурсии из функций с рекурсивно перечислимым графиком, имеет рекурсивно перечислимый график;

c) функция, полученная с помощью μ - оператора, примененного к функции с рекурсивно перечислимым графиком, имеет рекурсивно перечислимый график;

d) частично рекурсивная функция имеет рекурсивно перечислимый график.

2. Доказать следствия 1 – 3 из параграфа 1.2.4.

3. Доказать рекурсивную перечислимость предиката $\exists x_1 \ldots \exists x_n\, P(x_1,\ldots,x_n)$, где $P(x_1,\ldots,x_n)$ – ПРП.

4. Об'ясните различие предикатов $\exists x\, P_e(a,x)$ (машина Тьюринга остановится на аргументе 'a') и $\exists x < t\, P_e(a,x)$ (машина Тьюринга остановится на аргументе 'a ' меньше, чем за t шагов'))?

5. Доказать, что пересечение подалгебр алгебры A, содержащих непустое подмножество $V \subset A$, есть наименьшая из этих подалгебр.

6. Доказать теорему о множестве значений термов алгебры [из1.2.3].

1.2.5. Рекурсия 2-ой ступени

Допустим, что мы хотим задать функцию F(x,y) рекурсией не по одному, а сразу по двум аргументам. Тогда надо предварительно упорядочить пары натуральных чисел (x,y), скажем следующим образом:

$(0,0)<(0,1)<\ldots<(1,0)<(1,1)<\ldots<(2,0)<(2,1)<\ldots$,

т.е. $(x_1,y_1)<(x_2,y_2)$, если $x_1<x_2$ или если $x_1=x_2$, то $y_1<y_2$.

Функция F(x,y) задана *рекурсией 2-ой ступени* через тотальные функции $G(x_0,\ldots,x_m)$, $H(x_0,\ldots,x_k)$, $f_i(x)\le x$, $g_j(x)\le x$ $(i=1,\ldots,m;\ j=1,\ldots,k)$, если для всех значений n, x:

$$\begin{cases} F(0,x) = h(x), \\ F(n+1,0) = H(n, F(g_1(n),F(g_2(n),0)), F(n,0),F(g_3(n),0),\ldots,F(g_{kk}(n),0)), \\ F(n+1,x+1)=G(n+1,F(f_1(n),F(n+1,x)),F(f_2(n),F(f_3(n),x+1)),F(f_4(n),x+1),\ldots, \\ \qquad F(f_m(n),x+1)) \end{cases} \qquad (*)$$

ТЕОРЕМА (*О рекурсии 2-й ступени*). Функция F(x, y), заданная рекурсией 2-й ступени относительно ПРФ G, H, h, f_i $(i=1,\ldots,m)$, g_j $(j=1,\ldots,k)$, есть ОРФ.

Д о к а з а т е л ь с т в о. Не теряя общности, рассмотрим случай m=4, k=3.

1). Как следует из построения, функция F всюду определенная.

Если график F – РПМ, то по теореме F(x, y) – ОРФ.

2). Из первого равенства (*) имеем: $(a, x, h(x)) \in$ графику F.

3). Из второго равенства (*) имеем :

$(g_2(n),0,u),(g_1(n),u, v),(n,0,p),(g_3(n),0,q) \in$ гр F $\rightarrow (n+1,0,H(n, v, p, q)) \in$ гр F.

Для удобства переобозначим координаты троек:

$(x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3),(x_4,y_4,z_4) \in$ гр F $\rightarrow (x_3+1,y_3,H(x_3,z_2,z_3,z_4)) \in$ гр F, где

$z_1=y_2$

$x_1=g_2(x_3)$ $y_1=y_3=y_4=0$ (**)
$x_2=g_1(x_3)$
$x_4=g_3(x_3)$
Определим на N^3 операцию B:
$B((x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3),(x_4,y_4,z_4)) = (x_3+1,y_3,H(x_3,z_2,z_3,z_4))$, если условия (**) выполнены, $B((x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3),(x_4,y_4,z_4)) = (0,0,h(0))$–иначе.

4). Из третьего равенства (*) имеем:
$(n+1,x,u),(f_1(n),u,v),(f_3(n),x+1,p),(f_2(n),p,q),(f_4(n),x+1,w)\in$гр $F\rightarrow$
$(n+1,x+1,G(n+1,x,v,q,w))\in$гр F.
Снова переобозначим тройки:
$(x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3),(x_4,y_4,z_4),(x_5,y_5,z_5)\in$гр $F \rightarrow (x_1+1,y_1+1,G(x_1+1,y_1,z_2,z_4,z_5))\in$гр F , где
$x_2 = f_1(x \bullet\underline{1})$ $y_1 = y_5 = y_1+1$
$x_3 = f_3(x \bullet\underline{1})$ $y_2 = z_1$ (***)
$x_4 = f_2(x \bullet\underline{1})$ $y_4 = z_3$ $x_5 = f_4(x \bullet\underline{1})$

Определим на N^3 операцию A:
$A((x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3),(x_4,y_4,z_4),(x_5,y_5,z_5)) = (x_1,y_1,G(x_1,y_2,z_2,z_4,z_5))$,
если условия (***) выполнены, $A((x_1,y_1,z_1),(x_2,y_2,z_2),(x_3,y_3,z_3),(x_4,y_4,z_4),(x_5,y_5,z_5)) = (0,0,h(0))$ – иначе.

5). A, B – ПРФ, т.к. их координатные функции – ПРФ.

6). $M_0=\{(0,x,h(x))\}=\{(0(x), I_1^1(x), h(x))\}$ – РПМ (по теореме о параметризации).

7). $M^* = <M_0>_{A,B}$ – РПМ (по теореме о порожденной совокупности).

8). $M_0 \subset$ гр F и гр F – подалгебра относительно операций A,B, т.ч.
гр $F \supset M^*$ (т.к. M^* - наименьшая подалгебра).

9). Покажем, что гр $F\subset M^*$: $(n, x, F(n, x))\in$гр F, индукцией по n, x докажем, что $(n, x, F(n, x))\in M^*$.
Базис: n=0 : $(0,x,h(x))\in$гр F & $(0,x,h(x))\in M_0\subset M^*$.
Индукционное допущение: для $r\le n$, $s\le x$, $(r, s, F(r, s))\in$гр F & $(r, s, F(r, s))\in M^*$.

а). Покажем, что $(n+1,0,F(n+1,0))\in M^*$:
$(g_2(n),0,u), (g_1(n), u, v), (n,0,p), (g_3(n),0,q)\in M^*$ (по индукционному допущ.)
$B((g_2(n),0,u), (g_1(n), u, v), (n,0,p), (g_3(n),0,q))=(n+1,0,H(n, u, v, p))\in M^*$ (ввиду замкнутости множества M* относительно операции B).

б). $(n+1,x,u,), (f_1(n),u,v), (f_3(n),x+1,p), (f_2(n),p,q), (f_4(n),x+1,w)\in M^*$
(по индукционному допущению).
$A((n+1,x,u),(f_1(n),u,v),(f_3(n),x+1,p),(f_2(n),p,q),(f_4(n),x+1,w))=$
$=(n+1,x+1,G(n+1,x,v,q,w))\in M^*$ (ввиду замкнутости , множества M* относительно операции A).

Таким образом, гр $F \subset M^*$, т.е. гр $F = M^*$.

10). Поскольку F – тотальная функция, график которой – РПМ, то F – ОРФ.

1.2.6. Универсальная функция

Функция $F(x_0,x_1,\ldots,x_n)$ называется *универсальной для семейства δ n-местных функций*, если выполнены два условия:
1) для каждого фиксированного i : $F(i,x_1,\ldots,x_n) = f(x_1,\ldots,x_n)$, $\exists f\in\delta$

2) для каждой функции $f(x_1,\ldots,x_n)\in\delta$ существует i такое, что
$F(i,x_1,\ldots,x_n) = f(x_1,\ldots,x_n)$.

ТЕОРЕМА. Класс n-местных рекурсивных (примитивно рекурсивных) функций не имеет рекурсивной (примитивно рекурсивной) универсальной функции (n=1,2,…).

Доказательство. Пусть $F(x_0,x_1,\ldots,x_n)$ – универсальная функция для класса δ^n всюду определенных n-местных функций. Положим $F(x_1,x_1,x_2,\ldots,x_n)+1 = g(x_1,\ldots,x_n)$.
Если $g \in \delta^n$, то $\exists i\ F(i,x_1,\ldots,x_n) = g(x_1,\ldots,x_n)$ для всех значений $x_1,\ldots,x_n$.
В частности, $F(i, i,\ldots,i) = g(i, i,\ldots,i) = F(i, i,\ldots,i)+1$. Полученное противоречие доказывает теорему.

ТЕОРЕМА. Класс одноместных ПРФ имеет общерекурсивную универ -сальную функцию.

Доказательство. 1). По теореме Робинсона, все одноместные ПРФ можно получить из элементарных функций s(x), $q(x)(=x\bullet[\sqrt{x}])$ с помощью операторов +, •, J[1].

2). Так что одноместные ПРФ являются значениями термов над алфавитом {s,q, +, •, I}. Введем следующую нумерацию ν термов (следовательно, и одноместных ПРФ): $\nu(1)=1$, $\nu(q)=3$; $\nu(t_1+t_2)=2^1\cdot3^a\cdot5^b$, где a, b – коды термов t_1, t_2, соответственно; $\nu(t_1*t_2)=2^2\cdot3^a\cdot5^b$, где a, b – коды термов t_1, t_2, соответственно; $\nu(I(t))= 2^3\cdot3^a$, где a – код терма t.

3). Обозначим $f_n(x)=F(n, x)$, где $f_n(x)$ – терм с кодом n. Для натуральных чисел n, являющихся кодами подходящих термов, имеем:

$$F(n,x)=\begin{cases} f_a(x)+f_b(x), & \text{если } n = 2^1\cdot3^a\cdot5^b;\\ f_a(f_b(x)), & \text{если } n = 2^2\cdot3^a\cdot5^b;\\ f_a(f_n(x)), & \text{если } n = 2^3\cdot3^a,\ x=0;\\ q(x), & \text{если } n = 3;\\ s(x), & \text{если } n = 1.\end{cases}$$

или, вводя обозначение $\exp(n,i)=(n)_i$,

$$F(n,x)=\begin{cases} F((n)_1,x)+F((n)_2,x), & \text{если } (n)_0=1;\\ F((n)_1,F((n)_2,x)), & \text{если } (n)_0=2;\\ F((n)_1,F(n,x-1)), & \text{если } (n)_0=3,\ x>0;\\ 0, & \text{если } (n)_0=3,\ x=0;\\ Q(n,x) & \text{– для остальных n, x,}\end{cases}$$

где $Q(n,x)=s(x)\,\overline{sg}\,|n-1|+q(x)\cdot\overline{sg}\,|n-3|$.

4). Доопределим функцию F(n,x) до всюду определенной функции D(n,x):

$D(0,x)=0$;

$$D(n+1,0)=\begin{cases} D(f_1(n),0)+D(f_2(n),0), & \text{если } (n+1)_0=1;\\ D(f_1(n),D(f_2(n),0)), & \text{если } (n+1)_0=2;\\ 0 & \text{– для остальных n;}\end{cases}$$

$$D(n+1,x+1)=\begin{cases} D(f_1(n),x+1)+D(f_2(n),x+1), & \text{если } (n+1)_0=1;\\ D(f_1(n),D(f_2(n),x+1)), & \text{если } (n+1)_0=2;\\ D(f_1(n),D(n,x+1)), & \text{если } (n+1)_0=3;\\ Q(n+1,x+1) & \text{– для остальных n;}\end{cases}$$

где $f_i(n)=(n+1)_i$ (i=1,2),
или

$$\begin{cases} D(0,x) = 0;\end{cases}$$

---

[1] g(0)=0,
g(n+1)=J(g(n))

$\begin{cases} D(n+1,0) = H(n, D(f_1(n),D(f_2(n),0)),D(f_1(n),0),D(f_2(n),0); \\ D(n+1,x+1) = G(n+1,x,D(f_1(n),D(n,x+1)),D(f_1(n),D(f_2(n),x+1)),D(f_1(n),x+1),D(f_2(n),x+1), \end{cases}$

где $G(m,x,y,z,u,v) = (u+v)\ \overline{sg}\,|(m)_0 - 1| + z\ \overline{sg}\,|(m)_0 - 2| + y\ \overline{sg}\,|(m)_0 - 3| +$

$Q(m,x)\cdot sg(|(m)_0 - 1|\cdot|(m)_0 - 2|\cdot|(m)_0 - 3|),$

$H(m, y, z, u)=(z+u)\ \overline{sg}\,|(m)_0 - 1| + y\cdot \overline{sg}\,|(m)_0 - 2|,\ f_i(x) \le x\ (i=1,2).$

Таким образом, функция $D(n, x)$ задана рекурсией 2-ой ступени, т.е. ОРФ.

5). Индукцией по n докажем, что $D(n, x) = f_n(x)$, если n – код терма, $D(n, x) = g(x)$ – одноместная ПРФ – для остальных n.

Базис: $n=0,1,2,3$: $D(0,x) = D(2,x) = 0$; $D(1,x) = s(x)$; $D(3,x) = q(x)$.

Индукционный шаг: Допустим, что утверждение верно для n и докажем для n+1: (1) n+1 – код терма. Тогда описания функций $D(n+1,x)$, $F(n+1,x)$ совпадают с точностью до замены $D(f_i(n),x)$ на $F(f_i(n),x)$. Последние совпадают по индукционному допущению, т.к. $f_i(n) \le n$ $(i=1,2)$. Откуда $D(n+1,x) = F(n+1,x)$. Таким образом, для всех n $D(n, x) = F(n, x)$, если n – код терма. (2) n+1 – не является кодом терма. Тогда $D(n+1,x)$ получается примитивной рекурсией из функций $D(f_1(n),x)$, $D(f_2(n),x)$. Последние ПРФ по индукционному допущению, т.к. $f_i(n) \le n$ $(i=1,2)$. Следовательно, $D(n+1,x)$ получается возвратной рекурсией, т.е. $D(n,x)$ есть ПРФ.

Таким образом, для всех n $D(n, x)$ – ПРФ, обладающая свойствами:

1) для фиксированного n $D(n, x)$ есть одноместная ПРФ;

2) для каждой одноместной ПРФ f: $\exists n\ D(n,x) = f(x) = f_n(x)$.

Это означает, что $D(n,x)$ – универсальная функция для класса одноместных ПРФ.

Следствие 1. Существуют ОРФ, не являющиеся ПРФ.

Д о к а з а т е л ь с т в о. $D(x,x)$ - ОРФ, не является ПРФ, в противном случае $D(x,x) + 1 = g(x)$ – ПРФ, следовательно, $\exists i\ D(i,x) = g(x) = D(x,x)+1$ для всех значений x. В частности, $D(i,i) = D(i,i) +1$, что есть противоречие.

Следствие 2. Для каждого $n=1,2,\ldots$ класс δ^n n-местных ПРФ имеет общерекурсивную универсальную функцию.

Д о к а з а т е л ь с т в о. Покажем, что универсальная функция этого класса $D^{(n+1)}(x_0,x_1,\ldots,x_n) = D(x_0,c(x_1,\ldots,x_n))$?

(1) При фиксированном значении $x_0 = c$:
$D(c,z)\in\delta^1$, т.е. $D(c,c(x_1,\ldots,x_n)) = D^{(n+1)}(c,x_1,\ldots,x_n)\in\delta^n$.

(2) Для любой $g(x_1,\ldots,x_n)\in\delta^n$, ее представляющая функция
$f(x)=g(c_{n1}(x),\ldots,c_{nn}(x))\in\delta^1$. Тогда $\exists i\ (f(x) = D(i,x))$ или
$g(x_1,\ldots,x_n)=g(c_{n1}(x),\ldots,c_{nn}(x))=f(x)=D(i,x)=D(i,c(x_1,\ldots,x_n))=D^{n+1}(i,x_1,\ldots,x_n)$.

Следствие 3. Существуют рекурсивные множества, не являющиеся РПМ.

Например, множество A с характеристической функцией $\chi_A(x)= \overline{sg}\ D(x,x)$.

1.2.7. Универсальные частично рекурсивные функции

ТЕОРЕМА (*Клини о нормальной форме*). Каждая ЧРФ $f(x_1,\ldots,x_n)$ предста вима в форме $f(x_1,\ldots,x_n) \cong^{4)} U(\mu t\ F^{(n+1)}(x_1,\ldots,x_n,t)=0)$, где $F^{(n+1)}$ – ПРФ.

Д о к а з а т е л ь с т в о. $f(x_1,\ldots,x_n)$ - ЧРФ, то гр $f(x_1,\ldots,x_n)$ есть РПМ, т.е. $(x_1,\ldots,x_n,y)\in$гр $f(x_1,\ldots,x_n)\leftrightarrow \exists z\ (g(x_1,\ldots,x_n, y, z)=0)$, где g – ПРФ $\leftrightarrow$

---

[4] $\cong$ означает условное равенство, т.е. равенство, обе части которого одновременно определены и совпадают или одновременно не определены.

$\exists t = c(x, y)\ (g(x_1,\ldots,x_n, l(t),r(t)) \ \&\ y=l(t))$.
Откуда $f(x_1,\ldots,x_n) = U(\mu t\ g(x_1,\ldots,x_n,l(t),r(t))=0) = U(\mu t\ (F^{(n+1)}(x_1,\ldots,x_n, t)=0))$, где $F^{(n+1)}$ – ПРФ, как суперпозиция ПРФ.

ТЕОРЕМА (*Об универсальной функции*). Существует ЧРФ $T^{(n+1)}(x_0,x_1,\ldots,x_n)$, универсальная для класса n-местных ЧРФ.

Д о к а з а т е л ь с т в о. $T^{(n+1)}(x_0,x_1,\ldots,x_n) = U(\mu\ t\ D^{(n+2)}(x_0,x_1,\ldots,x_n,)=0))$, где $D^{(n+2)}$ - универсальная функция для класса (n+1)-местных ПРФ.

Покажем, что $T^{(n+1)}(x_0,x_1,\ldots,x_n)$ – универсальная функция для класса n-местных ЧРФ:

(1) При фиксированном значении $x_0=e$:

$T^{(n+1)}(e,x_1,\ldots,x_n)=U(\mu\ t\ (D^{(n+2)}(e,x_1,\ldots,x_n, t)=0))=U(\mu\ t\ (f_e^{(n+1)}(x_1,\ldots,x_n, t)=0))$, где $f_e^{(n+1)}$ – ПРФ. Тогда $\mu\ t\ (f_e^{(n+1)}(x_1,\ldots,x_n, t)=0)$ – ОРФ. Таким образом, $T^{(n+1)}(e,x_1,\ldots,x_n)$ – ОРФ.

(2) Для любой ЧРФ $f^n(x_1,\ldots,x_n)$ по теореме Клини о нормальной форме имеем:

$F^{(n)}(x_1,\ldots,x_n)=U(\mu\ t\ (F^{(n+1)}(x_1,\ldots,x_n, t)=0))$, где $F^{(n+1)}$ – ПРФ. Тогда

$\exists e\ (D^{(n+2)}(e,x_1,\ldots,x_n, t)=F^{(n+1)}(x_1,\ldots,x_n, t))$,

т.е. $f(x_1,\ldots,x_n) = U(\mu\ t\ (D^{(n+2)}(e,x_1,\ldots,x_n, t)=0)) = T^{(n+1)}(e,x_1,\ldots,x_n)$, $\exists e$.

ТЕОРЕМА. Никакая ЧРФ $T^{n+1}(x_0,x_1,\ldots,x_n)$, универсальная для класса n-местных ЧРФ, не имеет общерекурсивных доопределений.

Д о к а з а т е л ь с т в о. 1). Пусть $V(x) = \overline{sg}\ T^{(n+1)}(x, x,\ldots,x)$ – ЧРФ. Допустим, что она имеет общерекурсивное доопределение W(x). Представим $W(x_1)= I_1^n (W(x_1), x_2,\ldots, x_n)$. По определению универсальной функции

$\exists e\ \forall\ x_1, x_2,\ldots, x_n\ \ W(x_1) = T^{(n+1)}(e,x_1,\ldots,x_n)$.В частности, $W(e)=T^{(n+1)}(e, e,\ldots,e)$. Так как $T^{(n+1)}(e, e,\ldots,e)$ определено, то $V(e) = \overline{sg}\ T^{(n+1)}(e, e,\ldots,e)$ определено.

W(x) - продолжение функции V(x), тогда $W(e) = V(e) = \overline{sg}\ T^{(n+1)}(e, e,\ldots,e)$, что противоречит тому, что $W(e) = T^{(n+1)}(e, e,\ldots,e)$.

2). Допустим, что $P(x_0,x_1,\ldots,x_n)$ – общерекурсивное доопределение функции $T^{(n+1)}(x_0,x_1,\ldots,x_n)$. Тогда функция $\overline{sg}\ P(x,\ldots,x)$ была бы общерекурсивным доопределением ЧРФ $V(x) = \overline{sg}\ T^{(n+1)}(x, x,\ldots,x)$, что не верно.

Следствие. Существуют нерекурсивные рекурсивно перечислимые множества.

Д о к а з а т е л ь с т в о. Возьмем частично рекурсивную функцию $V(x) = \overline{sg}\ T^2(x, x)$, не имеющую общерекурсивных доопределений. Из следствия 3 теоремы о графике ЧРФ, множество решений уравнения V(x)=0 является рекурсивно перечислимым множеством. Оно не рекурсивно, в противном случае функция V(x) имела бы общерекурсивное доопределение.

Упражнение.

1.Показать,что множество n-ок рекурсивно (примитивно рекурсивно) т.и т.т., когда его характеристическая функция рекурсивна (примитивно рекурсивна).

2. Доказать, что множество n-ок рекурсивно перечислимо т.и т.т., когда его частичная характеристическая функция частично рекурсивна.

3. Доказать, что если f – ЧРФ, то $M=\{(x_1,\ldots,x_n);\ \ \exists y\ f(x_1,\ldots,x_n,y)=0\}$ - РПМ.

4. Пусть $M_1,\ldots,M_k$ – попарно непересекающиеся РПМ n-ок, $f_1,\ldots,f_k$ – ЧРФ.

Доказать, что g – ЧРФ, если

$$g(x_1,...,x_n)=\begin{cases} f_1(x_1,...,x_n), \_ если \_ (x_1,...,x_n)\in M_1, \\ ... \\ f_k(x_1,...,x_n), \_ если \_ (x_1,...,x_n)\in M_k, \\ не \_ определена \_ в \_ остальных \_ случаях. \end{cases}$$

5. Пусть $f(x_1,\ldots,x_n)$ – частичная функция. Функция f – ЧРФ т.и т.т., когда предикат $f(x_1,\ldots,x_n) = y$ - РПП.

6. Пусть $k_n(e,\mathbf{x},t)$, $j_n(e,\mathbf{x},t)$ – соответственно, конфигурация и состояние машины Тьюринга после t шагов и $\sigma_n(e,\mathbf{x},t) = c(k_n(e,\mathbf{x},t), j_n(e,\mathbf{x},t))$ (n – длина кортежа аргументов). Показать, что функции σ_n, k_n, j_n - вычислимы, следовательно, по *Тезису Черча - Клини,* являются ЧРФ

7.Доказать, что предикат ‘$\varphi_e(\mathbf{x})$ – всюду определенная функция’ (проблема остановки) не разрешим.

8. Доказать, что множество {x; φ_x - тотальна } не является РПМ.

9. Какие из следующих множеств являются рекурсивными? Какие РПМ?

a) {x: x есть полный квадрат}, b) {x: φ_x инъективна}, c) {x: в десятичном разложении числа π существует набор последовательно идущих друг за другом семерок, длина которого больше x}.

10. Пусть f – одноместная вычислимая функция, $A \subset \mathrm{Arg}\, f$ и $g = f \mid A$. доказать, что g – вычислима т.и т.т., когда A – РПМ.

11. Пусть f – одноместная функция. Доказать, что f - вычислима т.и т.т., когда $\{2^x 3^{f(x)} : x \in \mathrm{Arg}\,(f)\}$ – РПМ.

Г л а в а 2

ПРИЛОЖЕНИЯ ТЕОРИИ АЛГОРИТМОВ

2.1. Теоремы о рекурсии и неполноте

Важнейшими задачами для формальной аксиоматической системы является установление ее неразрешимости (разрешимости) и неполноты (полноты), которые решаются вложением формальной системы в формальную арифметику Ar с помощью процедуры геделизации.

Геделевской нумерацией (геделизацией) множества слов Ω в алфавите A называют взаимно однозначное отображение $\gamma : \Omega \to N$, для которого существует алгоритм, вычисляющий по слову $\alpha \in \Omega$ его номер $\gamma(\alpha)$, и наоборот, по натуральному числу $n \in N$ выдающий слово α, если
$n = \gamma(\alpha)$, и число 0, - если n не является кодом никакого слова из Ω.

Объекты формальной системы, а также программы машины Тьюринга, или рекурсивные описания функций есть слова в конечных алфавитах и поэтому геделизуемы, что позволяет изучать их свойства в рамках формальной арифметики Ar .

Приведем пример одной геделевской нумерации машин Тьюринга. Командам машины Тьюринга: $q_j a_i \to a_r S q_r$, $q_j a_i \to a_r R q_r$, $q_j a_i \to a_r L q_r$ присвоим соответственно г.н.: $2^j 3^i 5^r 7^s$, $2^j 3^i 5^r 7^s 11$, $2^j 3^i 5^r 7^s 13$. Тогда, если
$c_1, c_2, \ldots, c_k$ - геделевские номера всех команд машины Тьюринга, то ее код
(г.н.) есть число $z = 2^{C_1} \ldots P_k^{C_K}$. Характерным свойством г.н. является то, что его всегда можно вычислить и обратно – по любому натуральному числу z
можно установить, является z г.н. некоторой программы машины Тьюринга , и если – да, то восстановить саму программу. Через $\{z\}(x_1,\ldots,x_n)$ будем обозначать функцию, вычислимую на машине P_z (с г.н.z).

Известна теорема об эквивалентности классов функций, вычислимых на машине Тьюринга, и ЧРФ, так что все полученные результаты о вычислимых функциях распространяются на обе теории. Отметим одну их важную особенность, а именно, инвариантность по отношению к геделевской нумерации, что означает независимость данных теорий от конкретного вида выбранной геделевской нумерации. Это свойство г.н. позволяет доказать такие принципы программирования, как теоремы об универсальной функции и неподвижной точке и s-m-n-теорему.

Пусть машина P_z вычисляет функцию $\{z\}(x,y) = \varphi(x,y)$. При фиксированном значении $x = a$, функция $\varphi(a,y)$ также вычислима и ее г.н.
может быть эффективно найден по z и x.

ТЕОРЕМА (*s-m-n-теорема*). Существует ПРФ $S_n^m(z, x_1, \ldots, x_m)$ такая, что

$$\{S_n^m(z, x_1, \ldots, x_m)\}(y_1, \ldots, y_n) \cong \{z\}(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

Д о к а з а т е л ь с т в о. (Рассмотрим случай $m = n = 1$).

Для каждого x эффективно строится программа Q_x, преобразующая аргумент ‘y’ в пару (x,y). Искомая функция $S_1^1(z,x)$ дает номер w машины, которая : на аргументе y порождает программу Q_x и применяет ее к аргументу ‘y’, а затем к паре (x,y) применяет программу машины z , так что $\{S_1^1(z,x)\}(y) \cong \{z\}(x,y)$. В силу эффективного характера г.н. номер w строится эффективно по z и x, поэтому $S_1^1(z,x)$ является рекурсивной и даже ПРФ.

Из s-m-n-теоремы как следствие можно получить теорему о неподвижной точке.

Следствие. (*Теорема о неподвижной точке*). Пусть $\varphi(z,x_1,\ldots,x_n)$ – вычислимая функция. Тогда существует машина e такая, что для любых $(x_1,\ldots,x_n)$: $\{e\}(x_1,\ldots,x_n) \cong \varphi(e,x_1,\ldots,x_n)$.

Д о к а з а т е л ь с т в о проведем для случая n = 1. Очевидно, что функция $\varphi(S_1^1(z,x),x)$ по прежнему вычислима на некоторой машине P_r. Положим $e = S_1^1(r,r)$, тогда $\{e\}(x) = \{S_1^1(r,r)\}(x) \cong \{r\}(r,r) \cong \varphi(S_1^1(r,r),x) = \varphi(e,x)$, ч.т.д.

Поскольку язык Ar беден, расширим его до Ar^+, вводя функциональные символы для каждой примитивно рекурсивной функции. Аксиоматика Ar^+ кроме аксиом Ar (аксиом равенства и аксиом Пеано) содержит определяющие аксиомы для примитивно рекурсивных описаний. Так что каждая примитивно рекурсивная функция представима в Ar^+ подходящим термом. По существу же Ar и Ar^+ эквивалентны, т.к. термы Ar^+ выразимы в Ar.

ЛЕММА 1**.** (*О нумерической выразимости ПРФ в Ar^+*). Для любого набора натуральных чисел $k_1, \ldots, k_n$, если $f(k_1, \ldots, k_n) = (\neq^5) g(k_1, \ldots, k_n)$, то $Ar^+ \vdash t(\mathbf{k_1, \ldots, k_n}) = (\neq^{1)}) r(\mathbf{k_1, \ldots, k_n})$, где t, r - термы , представляющие функции f, g, соответственно; $\mathbf{k}_i$ - терм, представляющий натуральное число k_i (i=1,...,n) в Ar^+**.**

ТЕОРЕМА (*О неподвижной точке*). Пусть A(x) - формула Ar^+, где x - свободная переменная. Тогда найдется формула B такая, что $Ar^+ \vdash B \leftrightarrow A([B])$, где [B] - терм, представляющий число $\gamma(B)$ в Ar^+.

Д о к а з а т е л ь с т в о. Пусть $y = \gamma(C(x))$ (x-свободная переменная). Рассмотрим прф $SUB(y, z) = \gamma(C(z))$, где Sub (y , z) - представляющий терм в Ar^+. Для $A^* = Sub(x, x))$ и $B = A^*([A^*])$ имеем $\gamma(B) =$ $SUB(\gamma(A^*), \gamma(A^*))$, и по лемме 1: $Ar^+ \vdash [B] = Sub([A^*], [A^*])$. Из вышесказанного имеем

$$Ar^+ \vdash B \leftrightarrow A^*([A^*]) \leftrightarrow A(Sub([A^*], [A^*])) \leftrightarrow A([B]).$$

Следствие. Для всюду определенной функции f найдется натуральное число n , такое, что $\varphi_{f(n)} = \varphi_n$.

С помощью геделевской нумерации выводимость в Ar^+ можно изучать средствами самой Ar^+. Рассмотрим примитивно рекурсивный предикат PRF(y,x): « y есть г.н. вывода в Ar^+ формулы с г.н. x » и рекурсивно перечислимый предикат $PR(x) \equiv \exists y\, PRF(y,x)$: « x есть г.н. формулы, выводимой в Ar^+ ». Соответственно, Prf (y,x), $Pr(x) \equiv \exists y\, Prf(y,x)$ - представляющие их в Ar^+ формулы.

По теореме о неподвижной точке, существует формула ν, утверждающая свою собственную невыводимость: $Ar^+ \vdash \nu \equiv \neg Pr([\nu])$.

ЛЕММА 2**.** Если теория Ar^+ непротиворечива, то не ($Ar^+ \vdash \nu$).

Д о к а з а т е л ь с т в о.

1. Ar^+ - непротиворечива (допущение)
2. $Ar^+ \vdash \nu$ (допущение противного)

---

[5] $t \neq r$ есть сокращение формулы $\neg(t=r)$.

3. $\exists y\, PRF(y,\gamma(\nu))$ (из п.2)
4. $Ar^+ \vdash \exists y\ Prf(y, [\nu])$
5′. $Ar^+ \vdash Prf(p, [\nu])$ (допущение)
6′. $Ar^+ \vdash Pr([\nu])$ ($\exists$-введение)
7′. $Ar^+ \vdash \nu \equiv \neg Pr([\nu])$ (теорема о неподвижной точке)
8′. $Ar^+ \vdash \neg\nu$ (по правилам вывода)
9. $Ar^+ \vdash \neg\nu$ ($\exists$-удаление)
10. не $(Ar^+ \vdash \nu)$ ($\neg$ - введение)
11. Ar^+ - непротиворечива $\rightarrow$ не $(Ar^+ \vdash \nu)$ ($\rightarrow$ - введение)

Теория[1)] T в языке Ar^+ называется *ω- непротиворечивой*, если не существует такой формулы A (y) с единственной свободной переменной, что (1) $T \vdash \exists y\ A(y)$ и (2) $T \vdash \neg A(m)$ для любого натурального m.

УТВЕРЖДЕНИЕ**.** Если теория T ω - непротиворечива, то T непротиворечива

ЛЕММА 3**.** Если теория Ar^+ ω - непротиворечива, то не $(Ar^+ \vdash \neg\nu)$.

Д о к а з а т е л ь с т в о.

1. Ar^+ ω - непротиворечива (допущение)
2. Ar^+ - непротиворечива (из п.1 и утверждения перед леммой)
3. $Ar^+ \vdash \nu \leftrightarrow \neg Pr([\nu])$ (теорема о неподвижной точке)
4. $Ar^+ \vdash \neg\nu$ (допущение противного)
5. $Ar^+ \vdash Pr([\nu])$ (из п. 3, 4 с помощью правил вывода)
6. $Ar^+ \vdash \exists y\ Prf(y, [\nu])$ (по определению формулы $Pr([\nu])$)
7. не $(Ar^+ \vdash \nu)$ (в силу непротиворечивости Ar^+ и п.4)
8. $\neg PRF(m, \gamma(\nu))$ для любого m (из п.7)
9. $Ar^+ \vdash \neg Prf(\mathbf{m}, [\nu])$ для любого m (из п.8 по лемме 1)
10. не $(Ar^+ \vdash \exists y\ Prf(y, [\nu]))$ (из ω-непротиворечивости Ar^+)
11. не $(Ar^+ \vdash \neg\nu)$ ($\neg$ - введение, 4)
12. Ar^+ ω - непротиворечива $\rightarrow$ не $(Ar^+ \vdash \neg\nu)$ ($\rightarrow$ - введение)

Теория T полна, если для любой формулы Ф из T имеет место $T \vdash Ф$ или $T \vdash \neg Ф$.

ТЕОРЕМА ГЕДЕЛЯ О НЕПОЛНОТЕ. Если теория Ar^+ ω - непротиворечива, то формулы ν и $\neg\nu$ не выводимы в Ar^+.

Д о к а з а т е л ь с т в о следует из лемм 2 и 3.

Обозначим через $Th_L(U)$ множество всех предложений языка L, истинных в модели[6] U, а через [T]- множество всех теорем теории T.

Теория T полна относительно модели U, если $[T] = Th_L(U)$.

Через ω обозначим элементарную арифметику, ее называют стандартной моделью Ar^+.

ТЕОРЕМА. Если Ar^+ ω - непротиворечива, то она существенно неполна относительно модели ω.

Д о к а з а т е л ь с т в о. Формула ν истинна в стандартной модели ω, но не выводима в Ar^+, т.е. Ar^+ неполна относительно модели ω. Рассмотрим теорию $T = Ar^+ \cup \{\neg\nu\}$. Теория T непротиворечива, так как в противном случае $Ar^+ \vdash \nu$, что невозможно. Таким образом, $T \vdash \neg Prf(\mathbf{m}, [\nu])$ для любого натурального числа m, и $T \vdash \exists y\ Prf(y,[\nu])$ (т.к. $\neg\nu \leftrightarrow \exists y\ Prf(y, [\nu])$),

---

[1]Математическая теория в содержательном смысле.

т.е. T ω-противоречива.

Покажем, что нельзя доказать непротиворечивость теории только средствами самой этой теории.

Рассмотрим замкнутую формулу $Con \equiv \forall y \neg Prf(y, [0=S(0)])$ (где $Ar^+ \vdash \neg [0=S(0)]$), утверждающую непротиворечивость теории Ar^+.

ВТОРАЯ ТЕОРЕМА ГЕДЕЛЯ. Если теория Ar^+ непротиворечива, то не $(Ar^+ \vdash Con)$.

Сначала докажем вспомогательные утверждения.

УТВЕРЖДЕНИЕ 1. $Ar^+ \vdash Con \to \neg Pr[\nu]$.

Доказательство следует из леммы 2.

УТВЕРЖДЕНИЕ 2. $\neg \exists y\ PRF(y, \gamma(\nu)) \to (Ar^+$ - непротиворечива).

Доказательство. Пусть верно $\neg \exists y\ PRF(y, \gamma(\nu))$.Допустим противное : Ar^+ противоречива. Тогда в Ar^+ выводима любая формула, в частности, и формула ν. Пусть D есть вывод формулы ν в Ar^+, тогда истинно $PRF(\gamma(D), \gamma(\nu))$, следовательно, $\exists y\, PRF(y,\gamma(\nu))$, что противоречит условию.

УТВЕРЖДЕНИЕ 3. $Ar^+ \vdash \neg\exists y\ Prf(y, [\nu]) \to Con$.

УТВЕРЖДЕНИЕ 4. $Ar^+ \vdash \nu \equiv Con$.

Доказательство *второй теоремы Геделя о неполноте* следует из утверждения 4 и леммы 2.

Упражнение

1. Доказать, что из условия леммы 1 не следует, что для свободных переменных $x_1, \ldots, x_n$ имеет место $Ar^+ \vdash t(x_1, \ldots, x_n) = r(x_1, \ldots, x_n)$,
2. Доказать, что если теория T противоречива, то T |–Ф для любой формулы Ф.
3. Доказать утверждения 1-4 из параграфа 2.1.
4. Пусть $\varphi_1(z_1,z_2,x)$ и $\varphi_2(z_1,z_2,x)$ - вычислимые функции. Доказать, что существуют машины e_1 и e_2 такие, что $\{e_i\}(x) \cong \varphi_i(e_1,e_2,x)$ (i=1,2).
5. Применить метод неподвижной точки, чтобы придать смысл рекурсивным программам: $f(x_1,\ldots,x_n) = \tau(f, x_1,\ldots,x_n)$, где τ - выражение некоторого языка программирования L и f – функциональный символ.

2.2. Разрешимость и неразрешимость формальных систем

Аксиоматическая формальная система T *разрешима*, если по любому выражению Ф из T можно эффективно узнать, является Ф теоремой (выводима в T) или нет.

В силу *Тезиса Черча* вопрос о разрешимости исчисления, допускающего геделизацию, сводится к вопросу о рекурсивности множества геделевых номеров теорем теории T.

Приведем необходимые сведения из теории алгоритмов.

Множества $A_0,\ A_1 \subseteq N$ называются *рекурсивно отделимыми***,** если существуют рекурсивно перечислимые множества B_0 и B_1, такие, что $A_0 \subseteq B_0,\ A_1 \subseteq B_1,\ B_0 \cap B_1 = \varnothing,\ B_0 \cup B_1 = N$.

УТВЕРЖДЕНИЕ**.** Если множества A_0, A_1 рекурсивно неотделимы и не пересекаются, то они нерекурсивны.

Напомним, что предикат $T_n(e, x_1,...,x_n, z) \equiv \varphi_e(x_1,...,x_n) = z$.

Возьмем два примитивно рекурсивных предиката :

$W_0(x, y) \equiv T_1(r(x),\ x, y) \wedge \forall z \le y\ \neg T_1(l(x), x, z)$,

$W_1(x, y) \equiv T_1(l(x), x, y) \wedge \forall z \le y\ \neg T_1(r(x), x, z)$.

Определим два рекурсивно перечислимых множества:

$V_0 = \{ x ;\ \exists y\ W_0(x, y) \},\quad V_1 = \{ x ;\ \exists y\ W_1(x, y) \}$.

ТЕОРЕМА. Рекурсивно перечислимые множества V_0, V_1 не пересекаются и являются рекурсивно неотделимыми.

Доказательство. Допустим, что $V_0 \cap V_1 \neq \varnothing$ и $x \in V_0 \cap V_1$.

По определению множеств V_0, V_1, найдутся y_0, y_1, такие, что

$W_0(x, y_0)$, $W_1(x, y_1)$, т.е.

(1) $T_1(r(x), x, y_0) \wedge \forall z \le y\ \neg T_1(l(x), x, z)$

(2) $T_1(l(x), x, y_1) \wedge \forall z \le y\ \neg T_1(r(x), x, z)$.

Отсюда имеем : $y_0 < y_1$ и $y_1 < y_0$, что дает противоречие. Таким образом, $V_0 \cap V_1 = \varnothing$.

Для доказательства второй части утверждения допустим, что существуют рекурсивно перечислимые множества B_0, B_1 такие, что

$V_0 \subseteq B_0$, $V_1 \subseteq B_1$, $B_0 \cap B_1 = \varnothing$. Покажем, что $B_0 \cup B_1 \neq N$. Пусть $B_0 = Val\ \varphi_{m0}$, $B_1 = Val\ \varphi_{m1}$ и

$m = c(m_0, m_1)$. Докажем, что $m \notin B_0$ и $m \notin B_1$.

Допустим, что $m \in B_0$, тогда $m \in Val\ \varphi_{m0}$, т.е. $\exists y\ T_1(m_0, m_1, y)$ или $\exists y\ T_1(l(m), m, y)$. Т.к. $m \in B_0$ и $B_0 \cap B_1 = \varnothing$, то $m \notin B_1$, т.е. $m \notin Val\ \varphi_{m1}$, т.е. $\neg\exists y\ T_1(m_1, m, y)$ или $\neg\exists y\ T_1(r(m), m, y)$. Таким образом, имеем: $\exists y\ (T_1(l(m), m, y) \wedge \forall z \le y\ \neg T_1(r(m), m, z))$, то есть $\exists y\ W_1(m, y)$, следовательно, $m \in B_1$, что однако противоречит тому, что $m \notin B_1$. Таким образом, $m \notin B_0$. Аналогично доказывается, что $m \notin B_1$.

Рекурсивная неотделимость множеств V_0, V_1 доказана.

ТЕОРЕМА. Множества $[Ar^+]^0$ и $[Ar^+]^1$ всех номеров, выводимых и, соответственно, опровержимых предложений Ar^+, рекурсивно неотделимы.

Доказательство. Как в предыдущей теореме, рассмотрим примитивно рекурсивные предикаты $W_0(x, y)$, $W_1(x, y)$. Они представляются в Ar^+ арифметическими формулами, которые мы будем также обозначать как $W_0(x,y)$ и $W_1(x,y)$. Множества V_0, V_1 не пересекаются, т.е. $Ar^+ \vdash \exists y\ W_1(x, y) \to \neg\exists y\ W_0(x, y)$. Обозначим через $B(x) \equiv \exists y\ W_0(x, y)$. Если $m \in V_0$, то существует натуральное число k такое, что $W_0(m, k)$, откуда $Ar^+ \vdash W_0(\mathbf{m}, \mathbf{k})$, т.е. $Ar^+ \vdash \exists y\ W_0(\mathbf{m}, y)$, или $Ar^+ \vdash B(\mathbf{m})$. Значит, $\gamma(B(\mathbf{m})) \in [Ar^+]^0$.

По теореме о дедукции : $m \in V_0 \to \gamma(B(\mathbf{m})) \in [Ar^+]^0$.

Пусть теперь $m \in V_1$, тогда существует натуральное число k такое, что $W_1(m, k)$, откуда $Ar^+ \vdash W_1(\mathbf{m}, \mathbf{k})$, т.е. $Ar^+ \vdash \exists y\, W_1(\mathbf{m}, y)$. Так как $Ar^+ \vdash \exists y\, W_1(x, y) \to \neg\exists y\, W_0(x, y)$, то $Ar^+ \vdash \neg\exists y\, W_0(\mathbf{m}, y)$, т.е.
$Ar^+ \vdash \neg B(\mathbf{m})$ и $B(\mathbf{m}) \in [Ar^+]^1$.
Таким образом, $m \in V_1 \to \gamma(B(\mathbf{m})) \in [Ar^+]^1$.

Допустим противное, - множества $[Ar^+]^0$, $[Ar^+]^1$ рекурсивно отделимы и B_0, B_1 -рекурсивно отделяют множества $[Ar^+]^0$, $[Ar^+]^1$, т.е. B_0, B_1 рекурсивно перечислимые множества и $[Ar^+]^0 \subseteq B_0$,
$[Ar^+]^1 \subseteq B_1$, $B_0 \cap B_1 = \varnothing$, $B_0 \cup B_1 = N$. Определим рекурсивно перечислимые множества $B_i^* = \{m;\ \gamma(B(m)) \in B_i\}$ (i=1,2).
Из предыдущего имеем : $V_i \subseteq B_i^*$ (i=1,2) и $B_0^* \cap B_1^* = \varnothing$, $B_0^* \cup B_1^* = N$. Таким образом, множества V_0, V_1 рекурсивно отделимы, что не верно.

ТЕОРЕМА (*О неразрешимости*). Если T непротиворечивая теория в языке Ar^+, в которой выводимы все нелогические аксиомы Ar^+, тогда T неразрешима.

Доказательство. Очевидно, что $[T]^0 \subseteq [Ar^+]^0$. Ввиду непротиворечивости T, $[T]^0 \cap [Ar^+]^1 = \varnothing$. Если бы теория T была разрешимой, то множество $[T]^0$ было бы рекурсивным, но тогда и множество $N \setminus [T]^0$ было бы рекурсивным. Но тогда множества $[T]^0$ и $N \setminus [T]^0$ отделяют множества $[Ar^+]^0$ и $[Ar^+]^1$, что противоречит рекурсивной неотделимости множеств $[Ar^+]^0$ и $[Ar^+]^1$.

Следствие 1. Если Ar^+ непротиворечивая теория, то Ar^+ - неразрешимая теория.

Следствие 2. Все предыдущие реэультаты распространяются на теории T, обладающие следующими двумя свойствами :

1. Теория T аксиоматизируема и геделизируема.
2. Теория T содержит арифметику Ar^+.

Этими свойствами обладают, в частности, теории Ar, Ar^+, ZF (аксиоматическая теория множеств), так что при условии их непротиворечивости они неполны и неразрешимы, а множества их выводимых и опровержимых предложений рекурсивно неотделимы.

ТЕОРЕМА(О *неразрешимости исчисления предикатов*). Множество теорем исчисления предикатов не рекурсивно.

Доказательство. Язык исчисления предикатов содержится в Ar. Допустим, что множество теорем ИП рекурсивно. Тогда существует общерекурсивная функция f такая, что $f(\gamma(B)) = 0 \leftrightarrow \vdash B$, для произвольной формулы B. Пусть Ar^{--} - произвольный фрагмент Ar, содержащий лишь конечное число нелогических аксиом из Ar, конъюнкцию которых обозначим формулой A. Определим общерекурсивную функцию h :
$h(x) = 0 \leftrightarrow$ “x есть г.н. некоторой формулы B языка Ar и $f(\gamma(A \to B)) = 0$”.
Тогда $h(\gamma(B)) = 0 \leftrightarrow Ar^{--} \vdash B$ и теория Ar^{--} разрешима, что противоречит неразрешимости теории Ar^+.

Упражнение

1. Доказать утверждение из параграфа 2.2.
2. Доказать, что если множества A_0, A_1 – рекурсивно отделимы и $A_0 \cap A_1 = \varnothing$, то A_0, A_1 – не рекурсивны.
3. Доказать следствия 1 и 2 теоремы о неразрешимости для Ar и Ar^+.

Глава 3

СЛОЖНОСТЬ ВЫЧИСЛЕНИЯ

В реальных вычислениях важно не только то, что функция вычислима (имеется вычисляющая ее процедура), но не менее существенно – какова ее сложность вычисления (зависящая от внутренней сложности функции, а также – можно ли найти наилучшую программу для ее вычисления.Эти вопросы относятся к теории сложности вычислений.

Теорема Блюма об ускорении показывает, что существуют вычислимые функции, не имеющие “наилучшей программы”. Но есть класс функций, для которых существует быстро работающая программа, вычисляющая функцию, совпадающую с данной почти всюду.

3.1. Меры сложности

Мерой сложности может быть время вычисления, число шагов машины Тьюринга, длина рабочей ленты машины Тьюринга, использованной в вычислении, и др.

Мерой вычислительной сложности называют семейство функций Φ_e со следующими свойствами :

(1) $Arg(\Phi_e) = Arg(\varphi_e)$,

(2) предикат $\Phi_e(x) \cong y$ разрешим.

Семейство временных функций $t_e(x) = \mu t \{P(x)\downarrow$ за t шагов$\}$ является примером вычислительной сложности.

ЛЕММА. (1) $\mathrm{Arg}\, t_e = \mathrm{Arg}\, \varphi_e$ для всех n, e.

(2) Предикат $t_e(x) = t$ разрешим.

Предикат $P(n)$ *выполняется почти для всех n,* или *почти всюду (п.в.)*, если $P(n)$ выполняется для всех $n \in N$, кроме конечного множества натуральных чисел, т.е. $\exists n_0 \forall n \geq n_0\ P(n)$.

ТЕОРЕМА 1. Пусть g – тотальная вычислимая функция. Существует тотальная вычислимая функция $f = \varphi_e$, принимающая только значения 0 и 1, такая, что $t_e(n) > g(n)$ п.в.

Доказательство. Мы хотим иметь следующее: если $t_i(m) \leq g(m)$ для бесконечно многих m, то f отличается от φ_i хотя бы в одном из этих значений. Определим f рекурсией: пусть $f(0), f(1),\ldots,f(n-1)$ уже определены, тогда если $i_n = \mu i \{ i \leq n \,\&\, i \neq i_0,\ldots,i_{n-1} \,\&\, t_i(n) \leq g(n)\}$ и $\varphi_{i_n}(n) = 0$, то $f(n) = 1$, в противном случае $f(n) = 0$.

Поскольку проверка отношения $t_i(n) \leq g(n) \leftrightarrow \exists y \leq g(n)\ (t_i(n) \cong y)$ эффективна, то функция $f(n)$ рекурсивна. $f(n) \neq \varphi_i(n)$ и $e \neq i_n$, покажем, что если $t_i(m) \leq g(m)$ для бесконечно многих m, то $i = i_n$ для некоторого n,следо- вательно, $i \neq e$. Этого достаточно, чтобы доказать, что $t_e(m) > g(m)$ п.в.

Пусть $t_i(m) \leq g(m)$ п.в.; положим $p = 1 + \max\{k;\ i_k\downarrow \,\&\, i_k < i\}$, $p = 0$ – в противном случае. Возьмем n, такое, что $n \geq i$ и $t_i(n) \leq g(n)$.

Если $i = i_k$ для некоторого $k < n$, то все доказано. Если $i \neq i_k$ для всех $k < n$, то $i \neq i_0,\ldots,i_{n-1}$ и $t_i(n) \leq g(n)$. Таким образом, по определению i_n: $i_n\downarrow$ и $i_n \leq i$. Но поскольку $n \geq p$, то $i_n \geq i$. Следовательно, $i = i_n$.

3.2. Теорема об ускорении

Пусть P и Q - программы для вычисления тотальной функции f, такие, что $k\, t_Q(x) < t_P(x)$ для всех x. Тогда программа Q в k раз быстрее (лучше) программы P.

Теорема об ускорении говорит, что существует функция f, для которой не существует наилучшей программы т.к. любую ее программу можно улучшить, ускорив на любой (вычислимый) множитель.

В теореме о псевдоускорении не требуется найти $\varphi_j(x) = f(x)$ для всех x.

ТЕОРЕМА 2 (*О псевдоускорении*). Пусть r тотальная вычислимая функция. Существует тотальная вычислимая функция f, такая, что по любой данной вычисляющей f программе P_i можно найти такую программу P_j, что:

a) φ_j – тотальная вычислимая функция и $\varphi_j(x) = f(x)$ п.в.,

b) $r(t_j(x)) < t_i(x)$ п.в.

Доказательство. 1) $\varphi_e(u,x) \cong \varphi_{s(e,u)}(x)$ (s-m-n - теорема).

2) $g_u(x) = \varphi_e(u,x)$ (теорема об универсальной функции).

3) Строим f со следующими свойствами :

a) $g_0 = f$,

b) $g_u(x) = g_0(x)$ п.в.,

c) если $f = \varphi_i$, то для g_{i+1} найдется j, такое, что $r(t_j(x)) < t_i(x)$ п.в.

(достаточно взять $j = s(e,i+1)$).

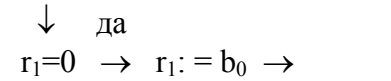
4) Фиксируем u и строим g рекурсией по x:

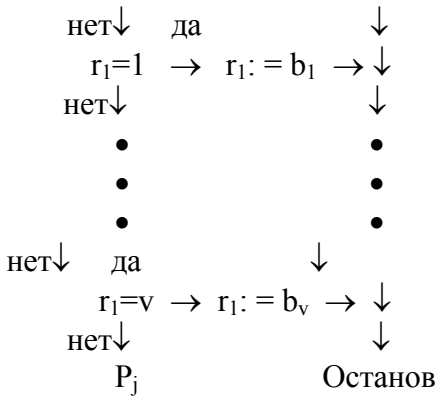
Построим вспомогательные множества $C_{u,x}$ (вычеркнутых индексов):

пусть $g(u,0)$, $g(u,1),\ldots,g(u,x-1)$, $C_{u,0}$, $C_{u,1},\ldots,C_{u,x-1}$ уже определены, тогда
$C_{u,x} = \{i;\ u \le i \le x\ \&\ i \notin \cup C_{u,y}\ \&\ t_i(x) \le r(t_{s(e,i+1)}(x))\}$, если $t_{s(e,i+1)}\downarrow$ для $u \le i < x$;
$C_{u,x} = \varnothing$ для $x \le u$.
Тогда $g(u,x) = 1+\max\{\varphi_i(x);\ i \in C_{u,x}\}$, если $C_{u,x}\downarrow$.
По следствию из второй теоремы рекурсии, $g(u,x) \cong \varphi_e(u,x)$, $\exists e$.
5) Покажем, что $g(u,x) = \varphi_e(u,x)$ удовлетворяет требованиям из п.3:
(1) $g(u,x)$ – тотальная функция: для фиксированного x и $u \ge x$ имеем $C_{u,x} = \varnothing$, т.е. $g(u,x) = 1$;
для $u < x$, покажем, что $g(u,x)\downarrow$: допустим, что $g(x,x), g(x-1,x),\ldots,g(u+1,x)$ определены, тогда $\varphi_{s(e,x)}(x), \varphi_{s(e,x-1)}(x),\ldots, \varphi_{s(e,u+1)}(x)$ определены, следовательно, и $t_{s(e,i+1)}\downarrow$ для $u \le i < x$. Отсюда $C_{u,x}\downarrow$, т.е. $g(u,x)\downarrow$, ч.т.д.
(2) $g_u(x) = g(u,x) = \varphi_e(u,x) = \varphi_{s(e,u)}(x)$ и проверим свойства a)-c):
(a)Для $f = g_0$ функция f тотальна, ч.т.д.
(b) Фиксируем u и покажем, что $g(0,x)$ и $g(u,x)$ отличаются только на конечном множестве точек x. По построению множества $C_{u,x}$ ясно, что для всякого x, $C_{u,x} = C_{0,x} \cap \{u,u+1,\ldots,x-1\}$. Так как все множества $C_{0,x}$ попарно не пересекаются, то существует $v = \max\{x;\ \exists i<u\ i \in C_{0,x}\}$. Для $x > v$, имеем $C_{0,x} \subseteq \{u,u+1,\ldots,x-1\}$, следовательно, $C_{0,x} = C_{u,x}$, т.е. $g(0,x) = g(u,x)$ для $x>v$. Таким образом, $g_0(x) = g_u(x)$ п.в.
(c) Пусть $f = \varphi_i$ & $j = s(e,i+1)$, тогда $\varphi_j = \varphi_{s(e,i+1)} = g_{i+1}$ и $r(t_j(x)) = r(t_{s(e,i+1)}(x)) > t_i(x)$ для всех $x>i$, в противном случае - $x > i\ \&\ i \in C_{0,x}$, и тогда $g(0,x) \ne \varphi_i(x)$, что означает противоречие.

Заметим, что теорема о псевдоускорении эффективна: по данной программе P для f можно эффективно найти другую программу, которая вычисляет f п.в. и п.в. быстрее, чем P.

ТЕОРЕМА 3 (*Об ускорении*). Пусть r тотальная вычислимая функция. Существует тотальная вычислимая функция f, такая, что, для всякой программы P_i, вычисляющей f, существует другая программа P_k для вычисления f, для которой $r(t_k(x)) < t_i(x)$ п.в.
Доказательство. Без потери общности можно считать, что функция r возрастающая.
По теореме 2, существует тотальная вычислимая функция f, где P_i - вычисляющая f программа, и найдется программа P_j, такая, что
a) φ_j – тотальная и $\varphi_j(x) = f(x)$ п.в.;
b) $r(t_j(x) + x) < t_i(x)$ п.в.
Для этого в определении $C_{u,x}$ заменим неравенства $r(x) \le r(t_{s(e,i+1)}(x))$ на $r(x) \le r(t_{s(e,i+1)}(x) + x)$. Покажем, что полученная таким образом функция f удовлетворяет требуемым условиям.
По условию $f = \varphi_i$ и j удовлетворяет условиям a) и b). Изменим программу P_j, чтобы получить программу P_{j^*},такую,что $P_{j^*}(x) = f(x)$ для всех x:
Пусть $\varphi_j(m) = f(m)$ для всех $m> v$ & $f(m) = b_m$ для $m \le v$. Изменим P_j, поместив в начало программы некоторые команды, задающие значения f для $m \le v$, как показано на блок-схеме:





Очевидно, что $P_{j^*}(x) = f(x)$ для всех x, и найдется c, такое, что $t_{j^*}(x) \le t_j(x)+c$ для всех x. Ввиду того, что функция r возрастает: $r(t_{j^*}(x)) \le r(t_j(x)+c) \le r(t_j(x)+x)$ (для всех $x \ge c$) $< t_i(x)$ п.в.
Для $k = j^*$ теорема доказана.

Можно показать, что теорема об ускорении не является эффективной.

Теорема об ускорении является серьезным препятствием определения внутренней сложности функции f, которую нельзя таким образом определить, как сложность вычисляющей ее программы, поскольку для функции f не существует наилучшей программы (или быстрейшего алгоритма).

3.3. Классы сложности. Элементарные функции

Класс сложности тотальной вычислимой функции f определим как $G_b = \{\varphi_e;\ \varphi_e$ – тотальная & $t_e(x) \le b(x)$ п.в.$\}$.

ТЕОРЕМА 4 (*О пробелах*). Пусть r тотальная вычислимая функция, для которой $r(x) \ge x$ для всех x. Тогда существует тотальная вычислимая функция f, такая, что а) $\forall e\ (x \ge e\ \&\ t_e(x)\downarrow\ \&\ t_e(x) \ge f(x) \to t_e(x) > r(f(x))$;

b) $G_f = G_{r\circ f}$.

Доказательство. Определим последовательность чисел $k_0<k_1<\ldots<k_x$ так, что $k_0 = 0$; $k_{i+1} = r(k_i)+1$ $(i < x)$. Рассмотрим непересекающиеся интервалы $[k_i, r(k_i)]$ для $0 < i < x$. Существует $(x+1)$ таких интервалов, значит по крайней мере один из них не содержит ни одного числа $t_e(x)$ для $e < x$, поскольку определено не более чем x таких чисел. Определим $i_x = \mu\, i\ (t_e(x) \notin [k_i, r(k_i)])$ для всех $e < x$, и положим $f(x) = k_i$.

По *Тезису Черча* функция f(x) - вычислимая функция. Предположим, что $x > e\ \&\ t_e(x) \ge f(x)$, тогда $t_e(x) \notin [f(x), r(f(x))]$, следовательно, $t_e(x) \ge r(f(x))$.

Докажем пункт b): Пусть $G_f \subseteq G_{r\circ f}$. Если $g \notin G_{r\circ f} \setminus G_f$, то g вычислима программой P_e с $t_e(x) < r(f(x))$ п.в. Однако $t_e(x) > (f(x))$ п.в. (иначе $g \in G_f$), что противоречит а). Таким образом, $G_f = G_{r\circ f}$.

В терминах временной сложности очень просто может быть охарактеризован класс всех практически вычислимых, функций, получающихся с помощью обычных арифметических операций.

Класс $\mathfrak{I}$ *элементарных функций* является наименьшим классом, таким, что:

(i) функции $x+1$, U_i^n $(1 \le i \le n)$, $x \dot{-} y$, $x+y$, xy входят в $\mathfrak{I}$;

(ii) класс $\mathfrak{I}$ замкнут относительно суперпозиции;

(iii) класс $\Im$ замкнут относительно операций ограниченного суммирования и ограниченного умножения.

Элементарный предикат (множество) имеет элементарную характеристическую функцию.

ЛЕММА. Класс $\Im$ замкнут относительно (1) ограниченного μ - оператора, операций $\neg, \&, \vee$ и ограниченных кванторов $\forall z<y, \exists z<y$.

ТЕОРЕМА 5. Класс $\Im$ замкнут относительно примитивной рекурсии, если определяемая функция элементарно ограничена.

Д о к а з а т е л ь с т в о. Пусть $f(x_1,\ldots,x_n)$, $g(x_1,\ldots,x_n,y,z)$ – ПРФ,

$h(x_1,\ldots,x_n,0) = f(x_1,\ldots,x_n)$

$h(x_1,\ldots,x_n,y+1) = g(x_1,\ldots,x_n,y, h(x_1,\ldots,x_n,y))$

и существует функция b, такая, что $h(x_1,\ldots,x_n,y) \le b(x_1,\ldots,x_n)$ для всех $x_1,\ldots,x_n,y$. Положим $s = 2^{h(x,0)}\ 3^{h(x,1)}\ldots P^{h(x,y)} = \Pi\ P^{h(x,z)} < \Pi\ P^{b(x,z)} = k(x,y)$, где $k(x,y)$ – элементарная функция.

Тогда $h(x,y) =[\mu\ s < k(x,y)\ ((s)_1 = f(x)\ \&\forall z<y((s)_{z+2} = g(x,z,(s)_{z+1})))]_{y+1}$, откуда следует элементарность функции h.

Следствие 1. Предикат $T_n(e,x_1,\ldots,x_n,y)$ нормальной формы Клини элементарен.

Следствие 2. а) Пусть $b(x_1,\ldots,x_n)$ – элементарная функция, $\varphi_{e\,(}x_1,\ldots,x_{n)}$ – тотальная вычислимая функция, такая, что $t_{e\,(}x_1,\ldots,x_{n)} \le b(x_1,\ldots,x_n)$ п.в., тогда $\varphi_{e\,(}x_1,\ldots,x_{n)}$ – элементарная функция.

b) Если $b(x_1,\ldots,x_n)$ – элементарная функция, тогда $G_b \subseteq G$.

Обозначим число $2^{2^{\cdot^{\cdot^{\cdot^{2^z}}}}}$ через $b_k(z)$: $b_0(z) = z$, $b_1(z) = 2^z$, $b_{k+1}(z) = 2^{b\,(z)}$. Очевидно, что $b_k(z)$ возрастающая ПРФ.

ТЕОРЕМА 6. Если $f_(x_1,\ldots,x_n)$ – элементарная функция, то найдется число k, такое, что для всех $x_1,\ldots,x_n$ $f_(x_1,\ldots,x_n) \le b_k(\max(x_1,\ldots,x_n))$.

Следствие. Функция $f(z) = 2^{2^{\cdot^{\cdot^{\cdot^{2^z}}}}}$ - ПРФ, но не элементарная.

Д о к а з а т е л ь с т в о. $f(z) = g(z,z)$, где

$g(z,0) = z$

$g(z,y+1) = 2^{g(z,y)}$, т.е. g – ПРФ.

Так как, с одной стороны, $f(k+1) = b_{k+1}(k+1) < b_k(k+1)$, а с другой - $f(k+1) = =g(k+1,k+1) =$

$=2^{g(k+1,k)} = \ldots = 2^{2^{\cdot^{\cdot^{\cdot^{2^{k+1}}}}}} = b_k(k+1)$ для каждого k, то получено противоречие.

Элементарные функции могут быть вычислены за элементарное время.

ТЕОРЕМА 7. Если функция $f(x_1,\ldots,x_n)$ элементарна, то существует вычисляющая f программа P, такая, что $t_p(x_1,\ldots,x_n)$ – элементарна.

(Без доказательства).

Упражнение

1. Доказать, что нельзя усилить теорему 1 так, чтобы неравенство $t_i(n) > b(n)$ выполнялось для всех n.
2. Доказать, что нельзя усилить теорему 3, заменив условие "$r(t_k(x)) < t_i(x)$ п.в." на "$r(t_k(x)) < t_i(x)$ для всех x ".

СПИСОК ЛИТЕРАТУРЫ

1. *Клини С.К.* Математическая логика. М.: Мир, 1973.
2. *Куратовский К, Мостовский А.* Теория множеств. М.: Мир, 1970.
3. *Мальцев А.И.* Алгоритмы и рекурсивные функции. М.: Наука, 1965.
4. *Мендельсон Э.* Введение в математическую логику. М.: Наука, 1971.
5. *Лавров И.А., Максимова Л.Л.* Задачи по теории множеств, математической логике и теории алгоритмов. М.: Наука, 1975.
6. *Катленд К.* Вычислимость. Введение в теорию рекурсивных функций. Пер. с англ. М.:Мир, 1983.
7. *Барвайс Дж.* (ред.) Справочная книга по математической логике в 4-х т. М.:Наука,1982-1983.
8. *Успенский В.А.,Семенов А.Л.* Теория алгоритмов: Основные открытия и приложения. М.:Наука,1987.
9. *Кудрявцев В.Б.*, *Алешин С.В., Подколзин А.С.* Введение в теорию автоматов. М.:Наука,1982.
10. *Рейуорд-Смит В.Дж.* Теория формальных языков.М.:Радио и связь, 1988.
11. *Манна З.* Теория неподвижной точки. В кн.:Кибернетический сб.Вып.15. М.:Мир,1978, с.38-100.
12. *Абрамов С.А.* Элементы анализа программ. М.:Наука, 1986.

ДОПОЛНИТЕЛЬНЫЙ СПИСОК ЛИТЕРАТУРЫ

1. *Барвайс Дж.* (ред.) Справочная книга по математической логике в 4-х т. М.:Наука,1982-1983.
2. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. М.:Наука,1972.
13. *Клини С.* Введение в метаматематику. М.:Ил,1957.
14. *Ершов Ю.Л.* Теория нумераций. М.:Наука,1977.
15. *Барендрегт Х.* Ламбда – исчисление. М.:Мир,1985.
16. *Козмидиади В.А., Маслов А.Н., Петри Н.В.*(ред.) Сложность вычислений и алгоритмов. Сборник переводов. М.:Мир,1974.
17. *Кудрявцев В.Б.*, *Алешин С.В., Подколзин А.С.* Введение в теорию авто- матов. М.:Наука,1982.
18. *Рейуорд-Смит В.Дж.* Теория формальных языков.М.:Радио и связь,1988.
19. *Манна З.* Теория неподвижной точки. В кн.:Кибернетический сб.Вып.15. М.:Мир,1978, с.38-100.
20. *Абрамов С.А.* Элементы анализа программ. М.:Наука, 1986.