Конспекты лекций по математической логике.

1. Теория алгоритмов

<u>1.1</u> *Различные подходы к определению алгоритма:*

1^0. Неформальное понятие алгоритма (последовательность инструкций для выполнения действия).
2^0. Машина с неограниченными регистрами (МНР).
3^0 Машина Тьюринга – Поста (МТ-П).
4^0 Нормальные алгоритмы Маркова (НАМ).

<u>1.1.1</u> *Машина с неограниченными регистрами (МНР).*

R_0	R_1	R_2	.... - регистры
r_0	r_1	r_2	.... - числа

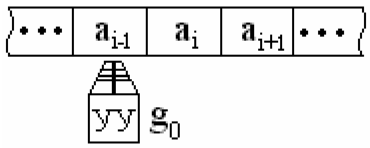
Имеется некое устройство, в котором счетное число ячеек памяти (регистров), в которых хранятся целые числа.

Допустимые команды:
Z(n) - обнуление регистра R_n.
S(n) - увеличение числа в регистре R_n на 1.
T(m,n) - копирует содержимое R_m в регистор R_n.
I(p,q,n) - если содержимое $R_p = R_q$ то выполняется команда с номером *n* , если нет следующая.

Программа для МНР должна быть последовательностью команд Z, S, T, I с определенным порядком, выполняемые последовательно.

<u>*Тезис Черча (Churcha)*</u>: Первое и второе определение алгоритма эквивалентны между собой. Любой неформальный алгоритм может быть представлен в программе для МНР.

<u>1.1.2</u> *Машина Тьюринга - Поста.*



Имеется устройство просматривающее бесконечную ленту, где есть ячейки содержащие элементы алфавита: $A = \{a_0, a_1, a_3, ..., a_n\}$, где Λ - пустой символ (пустое слово), который может принадлежать и не принадлежать A. Также существует управляющая головка (устройство) (УУ)/(УГ), которая в начальный момент расположена в определенном месте, в состоянии g_0. Также существуют внутренние состояния машины: $Q = \{g_0, g_1, ..., g_n\}$

<u>Слово в данном алфавите</u> - любая конечная упорядоченная последовательность букв данного алфавита, притом длина слова это количество букв в нем (у пустого слова длина 0).

Допустимые команды:

1) $a_i g_j \to a_{i^1} g_{j^1} \mu$,где $\mu = \left\{\begin{matrix} R\ (вправо) \\ L\ (влево) \\ \Lambda\ (ничего) \end{matrix}\right\}$.

2) $a_i g_j \to stop$ (остановка программы).

<u>Последовательность команд называется программой</u>, если в этой последовательности не встречается команд с одинаковыми левыми частями. Машина останавливается если она не находит команды с левой частью подобной текущей.

<u>1.1.3</u> *Нормальные алгоритмы Маркова.*

Тип машины перерабатывающий слова, в которой существует некий алфавит $A = \{a_0, a_1, a_3, ..., a_n\}$, для которого W - множество всех слов.

Допустимые команды: (Для машин этого типа важна последовательность команд.)

$$u_i \to \varepsilon_i u_{i^1} \text{ где } \begin{cases} u_i \ \& \ u_{i^1} \in W \\ \varepsilon_i = \begin{cases} \bullet \ (\textit{остановка}) \\ \Lambda \ (\textit{ничего}) \end{cases} \end{cases}$$

Пример: $A = \{a, б, о\}$ $U = баобаб$

Программа: $ба \to аб$

$U(баобаб) \to U'(абобаб) \to U''(абоабб).$

1.1.4 *Реализация функции натурального переменного.* $N = \{0,1,2,...\}$

$f : N \to N$ но мы допускаем не всюду определенную функцию.

$МНР\left|\begin{matrix}\textit{прогр.}\\\textit{релиз.}\end{matrix}\right| f$: то это означает, что $\boxed{n}\boxed{0}$……… $\Rightarrow f_{прогр} \Rightarrow$ $\boxed{N}\boxed{?}$??????…

притом $f(n) = N$, если f не определена, то и программа не должна ничего выдавать.

$МТ - П\left|\begin{matrix}\textit{прогр.}\\\textit{релиз.}\end{matrix}\right| f$: $\boxed{1}\boxed{1}\boxed{...}\boxed{1}\boxed{1}$ $= \overline{n} \Rightarrow f_{прогр} \Rightarrow \overline{N} =$ $\boxed{1}\boxed{1}\boxed{...}\boxed{1}\boxed{1}$

притом $f(n) = N$, если f не определена, то и программа не должна ничего выдавать.

($A = \{\Lambda, 1\}$, а числа представляются в виде $\overline{n} = \underbrace{11...11}_{n+1\ раз}$, например $\overline{0} = 1$; $\overline{3} = 1111$.)

1.2 *Эквивалентность трех подходов к понятию алгоритм.*

1.2.1 *Теорема об эквивалентности понятия вычислимой функции.*

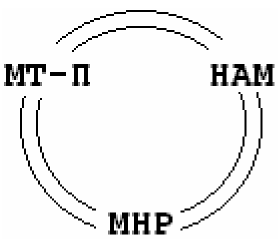
$f : N \to N$ вычислима: ($0 \in N$)

1) Если существует программа МНР, которая вычисляет эту функцию.
2) Если существует программа МТ-П, которая вычисляет эту функцию.
3) Если существует программа НАМ, которая вычисляет эту функцию.

Использование НАМ: $f = 2n$ $\qquad A = \{\Lambda, 1, \alpha, \beta\}$

$$\begin{cases} \alpha 1 \to 1\beta \\ \beta 1 \to 11\beta \\ \beta\Lambda \to 1 \bullet \Lambda \\ \Lambda \to \alpha \end{cases} \qquad \Lambda 1111\Lambda \xrightarrow{4} \alpha 1111\Lambda \xrightarrow{1} 1\beta 111 \xrightarrow{2} 111\beta 11 \xrightarrow{2} \xrightarrow{2} 11111\beta 1 \xrightarrow{2} 1111111\beta \xrightarrow{3} 1111111$$

Теор.: Классы функций вычислимых на МТ-П, с помощью НАМ и с помощью МНР совпадают.



Пусть $\exists\, f(n)$ которая вычисляется на МТ-П, вычислим её на НАМ.

МТ-П: $\left.\begin{matrix} A_T = \{\Lambda, 1, ...\} \\ Q = \{q_0, q_1, ..., q_n\} \end{matrix}\right\} u \quad \exists P_{МТ-П}$

НАМ: $A_M = A_T \cup \{q_0, q_1, ..., q_n\}$

Команда МТП: $a_i q_j \to a_{i^1} q_{j^1} \mu$ преобразуется по правилам:

$$\left.\begin{matrix} \mu = \Lambda & a_v q_j a_i \to a_v q_{j^1} a_{i^1} \\ \mu = L & a_v q_j a_i \to q_{j^1} a_v a_{i^1} \\ \mu = R & a_v q_j a_i \to a_v a_{i^1} q_{j^1} \end{matrix}\right\} \ a_v \textit{ пробегает все } a \in A_T$$

$+ \Lambda \to q_0$

Команда МТП: $a_i q_j \to stop \quad \Rightarrow \quad a_v q_j a_i \to \bullet a_v a_i \} \forall a \in A_T$

2. Булевы функции.

2.1 Основные определения

2.1.1 Декартово произведение

$A \times B \overset{def.}{=} \{(a,b),\, a \in B,\, b \in B\}$ - мн-во всевозможных упорядоченных пар элементов из А и В.

Пример: $A = \{0,1,2\} \quad B = \{1,3\} \quad A \times B \neq B \times A$

$A \times B = \{(0,1),(0,3),(1,1),(1,3),(2,1),(2,3)\} \quad |A| = n \quad |B| = m \quad A \times B = C \quad |C| = mn$

$A^2 = A \times A;\ \Re^2 \overset{def}{=} \Re \times \Re = \{(r_i, r_j);\ \forall r_i, r_j \in \Re\}$

2.1.2 Декартова степень произвольного множества.

Опр: $A^n = \{(a_1, a_2, ..., a_n);\ a_j \in A\}$ - множество всевозможных упорядоченных наборов длины n , элементов множества А. $\quad |A^n| = |A|^n$

2.1.3 Определение булевой функции от n переменных.

Любое отображение $\varphi : E^n \to E$ - называется булевой функцией от n переменных, притом множество $E = \{1\,(истина), 0\,(ложь)\}$

$(x_1, x_2, ..., x_n) \in E^n \quad \varphi((x_1, x_2, ..., x_n)) \to \begin{cases} 0 \in E \\ 1 \in E \end{cases}$

2.1.4 Примеры булевой функции.

1) $x \operatorname{V} y =$ логическая сумма (дизъюнкция).

x	y	рез:
0	0	0
0	1	1
1	0	1
1	1	1

2) $x \bullet y = x \Lambda y = xy = x \,\&\, y =$ логическое умножение (конъюнкция).

x	y	рез:
0	0	0
0	1	0
1	0	0
1	1	1

3) $x \oplus y =$ сложение по модулю два.

x	y	рез:
0	0	0
0	1	1
1	0	1
1	1	0

4) $x \to y =$ логическое следствие (импликация).

x	y	рез:
0	0	1
0	1	1
1	0	0
1	1	1

5) $\neg x = \bar{x} =$ отрицание.

x	рез:
0	1
1	0

2.1.5 Основные булевы тождества.

1) $(x_1 \operatorname{V} x_2) \operatorname{V} x_3 = x_1 \operatorname{V} (x_2 \operatorname{V} x_3)$ (ассоциативность)
2) $x_1 \operatorname{V} x_2 = x_2 \operatorname{V} x_1$ (коммутативность)
3) $x_1 \operatorname{V} 0 = 0 \operatorname{V} x_1 = x_1$ (свойство нуля)
4) $1 \operatorname{V} x_1 = x_1 \operatorname{V} 1 = 1$ (закон поглощения для 1)
5) $(x_1 x_2) x_3 = x_1 (x_2 x_3)$ (ассоциативность)
6) $x_1 x_2 = x_2 x_1$ (коммутативность)
7) $x_1 0 = 0 x_1 = 0$ (свойство нуля по умножению)
8) $x_1 1 = 1 x_1 = x_1$ (свойство нейтральности 1 по умножению)
9) $x_1 (x_2 \operatorname{V} x_3) = x_1 x_2 \operatorname{V} x_1 x_3$ (дистрибутивность)
10) $x_1 \operatorname{V} x_2 x_3 = (x_1 \operatorname{V} x_3)(x_1 \operatorname{V} x_2)$ (дистрибутивность 2)
11) $x_1 \operatorname{V} x_1 x_2 = x_1$ (закон поглощения)
12) $\overline{x_1 \operatorname{V} x_2} = \bar{x}_1 \bar{x}_2$ (Законы

13) $\overline{x_1 x_2} = \bar{x}_1 \vee \bar{x}_2$ де Моргана)
14) $\neg(\neg x_1) = x_1$ (закон снятия двойного отрицания)
15) $x_1 \vee \bar{x}_1 = 1$ (tertium non datur – третьего не дано)
16) $(x_1 \oplus x_2) \oplus x_3 = x_1 \oplus (x_2 \oplus x_3)$ (ассоциативность)
17) $x_1 \oplus x_2 = x_2 \oplus x_1$
18) $x_1 \oplus 0 = 0 \oplus x_1 = x_1$
19) $x_1 \oplus 1 = 1 \oplus x_1 = \bar{x}_1$
20) $x_1 \oplus x_1 = 0$
21) $x_1 \vee x_1 = x_1$ (Свойства
22) $x_1 x_1 = x_1$ идемпотентности)

2.2 Дизъюнктивные нормальные формы.

2.2.1 Основные определения.

$A = \{x_1, x_2, ..., x_n\}$ - конечный алфавит из переменных.

Рассмотрим слово: $x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} ... x_{i_S}^{\varepsilon_S}$ $\quad 1 < i_1 < i_2 ... < i_s \le n$

Экспоненциальные обозначения: $x_i^0 = \bar{x}_i \quad x_i^1 = x_i \quad \varepsilon_i = \begin{cases} 0 \\ 1 \end{cases}$

$x_1^0 x_3^1 x_4^0 = \bar{x}_1 x_3 \bar{x}_4$ - элемент конъюнкции.

S – длина элемента конъюнкции.

ДНФ – дизъюнкция нескольких различных элементарных конъюнкций.

$$f(x_1, x_2, ..., x_n) = u_1 \vee u_2 \vee ... \vee u_k = ДНФ \quad дл(ДНФ) \overset{def}{=} \sum_{i=1}^{k} дл(u_i)$$

Любая булева функция может быть представлена как ДНФ

2.2.2 Теорема о совершенной ДНФ.

Любая булева функция $f(x_1, x_2, ..., x_n)$ тождественно не равная 0 может быть разложена в ДНФ следующего вида:

(1) $\quad f(x_1, x_2, ..., x_n) = \sum\limits_{f(\delta_1, \delta_2, ..., \delta_n)} x_1^{\delta_1} x_2^{\delta_2} ... x_n^{\delta_n}$

Опр: Носитель булевой функции $f(x_1, x_2, ..., x_n) = 1$

$T_f \overset{def}{=} \{(x_1, x_2, ..., x_n) \in E^n;\ f(x_1, x_2, ..., x_n) = 1\}.$

Лемма: $f(x_1, x_2, ..., x_n) = q \quad (x_1, x_2, ..., x_n) \Leftrightarrow T_f = T_q$

1) $\Rightarrow$ это элементарно $f = q \Rightarrow T_f = T_q$

2) $\Leftarrow T_f = T_q$ возьмем набор $(x_1^*, x_2^*, ..., x_n^*)$

а) $f(x_1^*, x_2^*, ..., x_n^*) = 1 \Rightarrow (x_1^*, x_2^*, ..., x_n^*) \in T_f = T_q \Rightarrow$
$\Rightarrow q(x_1^*, x_2^*, ..., x_n^*) = 1 \Rightarrow f = q$ *на наборе* $(x_1^*, x_2^*, ..., x_n^*)$

б) $f(x_1^*, x_2^*, ..., x_n^*) = 0 \Rightarrow (x_1^*, x_2^*, ..., x_n^*) \notin T_f = T_q$ *– если бы она* $\in T_q$, *то ссыл на* $(a) \Rightarrow$
$\Rightarrow (x_1^*, x_2^*, ..., x_n^*) \notin T_q \Rightarrow q(x_1^*, x_2^*, ..., x_n^*) = 0 \Rightarrow f = q$ *на наборе* $(x_1^*, x_2^*, ..., x_n^*)$

Доказательство: $(1) \overset{def}{\equiv} q$, будем доказывать, что $T_q = T_f$.

1) Докажем, что $T_f \subseteq T_q$. Возьмем $(x_1^*, x_2^*, ..., x_n^*) \in T_f \Rightarrow f(...) = 1 \Rightarrow$ он попадает в число суммируемых наборов и по нему будет проводиться сумирование.

$$q(x_1^*, x_2^*, ..., x_n^*) \equiv ... \vee x_1^{x_1^*}, x_2^{x_2^*}, ..., x_n^{x_n^*} \vee ... \Rightarrow$$

$$\Rightarrow q(x_1^*, x_2^*, ..., x_n^*) \equiv ... \vee \underbrace{x_1^{*x_1^*}, x_2^{*x_2^*}, ..., x_n^{*x_n^*}}_{=1} \vee ... \Rightarrow q = 1$$

2) Докажем, что $T_q \subset T_f$. Возьмем другой набор из T_q

$$(t_1, t_2, ..., t_n) \Rightarrow q(t_1, t_2, ..., t_n) = 1 \Rightarrow \exists\ \text{слог}\ t_1^{\delta_1} t_2^{\delta_2} ... t_n^{\delta_n} = 1 \Rightarrow t_1 = \delta_1, ... \Rightarrow$$

$$\Rightarrow t_1^{t_1} t_2^{t_2} ... t_n^{t_n} = 1 \Rightarrow f(t_1, t_2, ..., t_n) = 1 \Rightarrow T_f \subset T_q$$

Следовательно $T_q \subset T_f \ \& T_f \subset T_q \Rightarrow T_q = T_f$

2.2.3 Некоторые другие виды ДНФ.

Опр: $u_1 V u_2 V .... V u_s$ - называется *минимальной ДНФ*, если она имеет $S = \min(s_i ... s_n)$ - наименьшую возможную длину из всех ДНФ данной функции.

Опр: $u_1 V u_2 V .... V u_s$ - называется *тупиковой ДНФ*, если из неё нельзя выбросить ни одного слагаемого с сохранением булевой функции.

(Легко понять, что любая минимальная ДНФ является тупиковой, а обратное не верно.)

Опр: *К-мерной гранью* называется такое подмножество E^n, которая является носителем некоторой элементарной конъюнкции длины: n-k.

Опр: Предположим дана функция $f(E^n)$ и есть $T_f = T$. Грань называется *отмеченной*, если она целиком содержится в носителе *T*.

Опр: *Максимальная грань* – это такая грань, которая не содержится ни в какой грани более высокой размерности.

Предложение: Любую отмеченную грань можно вложить в максимальную грань.

Предложение: $T_{f \vee q} = T_f \cup T_q \quad f = u_1 \vee u_2 \vee ... \vee u_n \Rightarrow T_f = T_{u_1} \cup T_{u_2} \cup ... \cup T_{u_n}$

(Носитель любой функции можно разложить в объединение нескольких граней разной размерностей)

Предложение: Носитель любой функции разлагается в объединение всех своих максимальных граней. $T_f = Q_1 \cup Q_2 \cup ... \cup Q_t$

Опр: *Элементарная конъюнкция называется минимальной*, если её носитель является максимальной гранью. Следовательно всякая булева функция разлагается в дизъюнкцию всех своих элементарных конъюнкций.

Опр: *Сокращенная ДНФ* – разложение данной булевой функции в соответствующие ДНФ, которые соответствуют объединению её максимальных граней.

Теор: *Минимальная ДНФ* может быть получена из сокращенной отбрасыванием некоторого количества слагаемых, возможно пустого.

3 Логические Исчисления.

3.1 Исчисления высказывания (ИВ).

3.1.1 Определения.

$$ИВ = \{L\ (язык\ ИВ),\ Ax\ (аксиомы\ ИВ),\ \mathrm{Re}\,g\ (правила\ вывода\ ИВ)\}$$

$$L = \{A\ (алфовит), V\ (слова),\ F\ (формулы)\}$$

$$A = \left\{ \underbrace{A, B, C, ..., Z, A_1, B_1, C_1, ..., Z_1, ..., A_n, B_n, C_n, ..., Z_n}_{символы\quad переменных} \right\} \cup \left\{ \overbrace{\underbrace{\vee, \&, \neg}_{логич\quad связи}, \underbrace{(,)}_{скобки}}^{спец\quad символы} \right\}$$

Опр: V – *словом в алфавите А*, называется любая конечная упорядоченная последовательность его букв.

Опр: *Формативная последовательность слов* – конечная последовательность слов и высказываний $u_1, u_2, ..., u_n$, если они имеют формат вида:

$$v_k = \begin{cases} v_i - символ\ переменной \\ v_i = (u_i \vee u_j),\ где\ u_{i,j} - подслова\ i, j < k \\ v_i = (u_i \,\&\, u_j),\ где\ u_{i,j} - подслова\ i, j < k \\ v_i = (\neg u_i),\ где\ u_{i,j} - подслова\ i, j < k \\ v_i = (u_i \to u_j),\ где\ u_{i,j} - подслова\ i, j < k \end{cases}$$

Опр: F – *формулой ИВ*, называется любое слово, входящее в какую-нибудь формативную последовательность.

Пример: $(\neg(\neg(A_{1999} \to A))) = F$

$u_1 = A_{1999}$
$u_2 = A$
$u_3 = (A_{1999} \to A)$
$u_4 = (\neg(A_{1999} \to A))$
$u_5 = (\neg(\neg(A_{1999} \to A)))$

Опр: *Аксиомы* – специально выделенное подмножество формул. $Ax \subseteq F$

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

Reg – правила вывода ИВ (некоторые правила преобразования первого слова в другое).
a – символ переменной $a \in A$
ψ - произвольное слово ИВ (формула)

Отображение $S_{\psi}^{a}: V \to V \quad (F \to F \text{ если } \psi \in A)$ действует так, что на место каждого вхождения символа a, пишется слово ψ.

Пример: $a = B; \psi = AB \Rightarrow S_{\psi}^{a}(A\underbrace{B}\underbrace{B}AC) \to (A\underbrace{AB}\underbrace{AB}AC)$

<u>*Правило modus ponens*</u>: $V^2 \to V \qquad m.p(\varphi, (\varphi \to x)) = x$

<u>3.1.2</u> Формальный вывод.(простейшая модель доказательства теоремы)

Опр: Последовательность формул ИВ, называется формальным выводом, если каждая формула этой последовательности имеет следующий вид:

$$u_k = \begin{cases} \in Ax\ (аксиома) \\ S_{\psi}^{a}(u_i),\ i < k \\ m.p(u_i, u_j),\ i, j < k \end{cases}$$

Опр: Выводимый формулой (теоремой) ИВ называется любая формула входящая в какой-нибудь формальный вывод. $\mapsto \varphi$ - выводимая формула ИВ.

Пример: $\mapsto (A \to A)$

1)	$(A \to (B \to A))$	$\in Ax(1)$
2)	$(A \to (B \to C)) \to ((A \to B) \to (A \to C)))$	$\in Ax(2)$
3)	$(A \to (B \to A)) \to ((A \to B) \to (A \to A)))$	$= S_{A}^{C}((2))$
4)	$((A \to B) \to (A \to A))$	$= m.p((1),(3))$
5)	$((A \to (B \to A)) \to (A \to A))$	$= S_{(B \to A)}^{B}((4))$
6)	$(A \to B)$	$= m.p((1),(5))$

Правило одновременной подстановки.

<u>Замечание</u>: Если формула φ выводима, то выводима и $S_{\psi}^{a}(\varphi)$

Возьмем формативную последовательность вывода φ $u_1, u_2, ..., u_n$ и добавим в неё $u_{n+1} = S_{\psi}^{a}(\varphi)$, получившаяся последовательность является формальным выводом.

(Если выводима $\mapsto \varphi$ то если $\mapsto (\varphi \to \psi)$, то выводима $\mapsto \psi$)

Теор: Если выводимая формула φ, то $S_{\psi_1, \psi_2, ..., \psi_n}^{a_1, a_2, ..., a_n}(\varphi)$ $(a_1, a_2, ..., a_n$ - различные символы переменных) выводима

Выберем $b_1, b_2, ..., b_n$ - символы переменных которые различны между собой и не входят не в одну из формул $\varphi, \psi_1, \psi_2, ..., \psi_n$, сделаем подстановку $S_{b_1}^{a_1}(\varphi)$ и последовательно применим $S_{b_n}^{a_n} ....S_{b_2}^{a_2} S_{b_1}^{a_1}(\varphi)$ и в новом слове делаем последовательную подстановку:

$S_{\psi_n}^{b_n} ....S_{\psi_2}^{b_2} S_{\psi_1}^{b_1}\left[S_{b_n}^{a_n} ....S_{b_2}^{a_2} S_{b_1}^{a_1}(\varphi)\right] = S_{\psi_1 \psi_2 ... \psi_n}^{a_1 a_2 ... a_n}(\varphi)$, где $u_1, ..., (u_n = \varphi), S_{b_1}^{a_1}, ..., S_{\psi_n}^{b_n}, ...$ - является формальным выводом.

<u>3.1.3</u> Формальный вывод из гипотез.

Опр: Формальным выводом из гипотез $\psi_1, \psi_2, ..., \psi_n$ (формулы), называется такая последовательность слов $u_1, u_2, ..., u_N$, каждая из которых удовлетворяет условию:

$$u_k = \begin{cases} -\textit{выводима}\ (\mapsto u_k) \\ =\psi_l,\ l = 1,2,\dots,n. \\ = m.p(u_i, u_j), \quad i, j < k \end{cases}$$

$\psi_1, \psi_2, \dots, \psi_n \mapsto \varphi$ если формулу φ можно включить в некоторый формальный вывод из гипотез $\psi_1, \psi_2, \dots, \psi_n$.

<u>*Лемма:*</u> $\psi_1, \psi_2, \dots, \psi_n \mapsto \varphi$; $\psi_1, \psi_2, \dots, \psi_n \mapsto (\varphi \to \psi)$: то тогда $\psi_1, \psi_2, \dots, \psi_n \mapsto \psi$

Напишем список:

$$\begin{array}{ll} & W_1\dots \\ u_1 & W_2\dots \\ \vdots & \vdots \\ u_N = \varphi & W_S = (\varphi \to \psi) \\ & \psi_0 = \psi \end{array} \qquad \begin{array}{l} \psi = m.p(\varphi, (\varphi \to \psi)) = \\ = m.p(u_N, W_S) \end{array}$$

<u>*Лемма*</u>: $\psi_1, \psi_2, \dots, \psi_n \mapsto (\omega \to \varphi); \psi_1, \psi_2, \dots, \psi_n \mapsto (\omega \to (\varphi \to \psi)) \Rightarrow \psi_1, \psi_2, \dots, \psi_n \mapsto (\omega \to \psi)$

$$\text{Док:} \begin{array}{lll} u_1 & W_1 & S^{A,B,C}_{\omega,\varphi,\psi}(Ax2) = (\omega \to (\varphi \to \psi)) \to \dots = \overline{A} \\ \vdots & \vdots & m.p(W_s, A) = ((\omega \to \varphi) \to (\omega \to \varphi)) = \overline{B} \\ u_N = (\omega \to \varphi) & W_S = (\omega \to (\varphi \to \psi)) & m.p(u_N, B) = (\omega \to \psi) \end{array}$$

<u>3.1.4</u> Теорема Дедукции.

Если из

$$\begin{array}{l} \varphi_1, \varphi_2, \dots, \varphi_n \mapsto \psi \quad \textit{то, тогда} \\ \varphi_1, \varphi_2, \dots, \mapsto (\varphi_n \to \psi) \\ \qquad \dots\dots\dots\dots \\ \mapsto (\varphi_1 \to (\varphi_2 \to (\dots\varphi_{n-1} \mapsto (\varphi_n \mapsto \psi)\dots) \end{array} \qquad \left.\begin{array}{l} u_1 \\ \vdots \\ u_N = \psi \end{array}\right\}, \textit{где}\ \psi = \begin{cases} 1) \mapsto \psi \\ 2a)\ \psi = \varphi_i,\ i < n \\ 2б)\ \psi = \varphi_n \end{cases}$$

1) и 2а) $(A \to (B \to A))$, где $A = \psi \quad B = \varphi_n \quad (\psi \to (\varphi_n \to \psi))$ по правилу m.p. $(\varphi_n \to \psi)$, ч.т.д.

2б) $\varphi = \varphi_n$, $(A \to A)$ - уже выводили $\Rightarrow \mapsto (\varphi_n \to \varphi_n)$, ч.т.д.

Базис индукции: N=1 ψ - формальный вывод из длинного списка $\mapsto \psi$

$\mapsto \psi = \varphi_i$ (только что доказано), осуществим переход по индукции:

$\mapsto \psi \quad \psi = \varphi_i \quad \psi = m.p. \quad u_1, \dots, u_i = \varphi \dots u_j = (\varphi \to \psi) \dots u_N = \psi$

$\varphi_1, \varphi_2, \dots, \varphi_{n-1} \mapsto (\varphi_n \to \varphi)$ по индукции

$\varphi_1, \varphi_2, \dots, \varphi_{n-1} \mapsto (\varphi_n \to (\varphi \to \psi))$ и по лемме 2

$\varphi_1, \varphi_2, \dots, \varphi_{n-1} \mapsto (\varphi_n \to \psi)$

Пример: $(A \to (B \to C)), A, B, \quad \mapsto C$

$$\begin{array}{lll} 1) & (A \to (B \to C)) & \\ 2) & A & \\ 3) & B & \\ 4) & (B \to C) & = m.p(1,2) \\ 5) & C & = m.p(4,3) \end{array} \qquad \begin{array}{l} (A \to (B \to C)), B \mapsto (A \to B) \\ \text{по теореме дедукции } (A \to (B \to C)) \mapsto (B \to (A \to C)) \\ \mapsto ((A \to (B \to C)) \to (B \to (A \to C))) \end{array}$$

<u>3.2</u> Критерий выводимости в ИВ.

3.2.1 Формулировка теоремы.

$\mapsto \varphi \Leftrightarrow \varphi \equiv 1$ - тавтология

при любой интерпретации алфавита (символов переменных)

$\mapsto \varphi \Leftrightarrow \Psi(\varphi) \equiv 1$

3.2.2 Понятие интерпретации.

$$\underbrace{(A \to (B \to A))}_{слово} \mapsto \underbrace{(x_1 \to (x_2 \to x_3))}_{булева\ \ функция}$$

символ переменной $\mapsto \{x_1, x_2, ..., x_n\}$ переменную поставим в соответствие.

$A \mapsto x_1 (= \omega_1^1(x_1))$, где $\omega_3^2(x_1, x_2, x_3) = x_2$ - проекция на x_2.

$\Psi : A \to \omega_n^i(x_1, ..., x_n)$

$u_1 \mapsto \Psi(u_1)$

$u_2 \mapsto \Psi(u_2)$

$\dots\dots\dots$

$u_n \mapsto \Psi(u_n)$

; u_1 - только символ переменных, т.к. это заглавное слово формативной последовательности вида:

$$u_n = \begin{cases} \text{символ переменной} \\ = (u_i \to u_j), i, j < n \\ = (u_i \vee u_j), i, j < n \\ = (\neg u_i), i < n \\ = (u_i \& u_j), i, j < n \end{cases}$$

Где:

$$\Psi(u_i \to u_j) \overset{def}{=} \Psi(u_i) \to \Psi(u_j) \qquad ; \Psi(u_i \vee u_j) \overset{def}{=} \Psi(u_i) \vee \Psi(u_j)$$

$$\Psi(u_i \& u_j) \overset{def}{=} \Psi(u_i) \& \Psi(u_j) \qquad ; \Psi(\neg u_i) \overset{def}{=} \overline{\Psi(u_i)}$$

3.2.3 Доказательство теоремы.

$$\left.\begin{matrix} \varphi_1 \\ \varphi_2 \\ \dots \\ \varphi_N \end{matrix}\right\} \text{формальный вывод } \varphi \qquad \varphi_k = \begin{cases} \in Ax \\ = S_\psi^a(\varphi_i), i < k \\ = m.p.(\varphi_i, \varphi_j), i, j < k \end{cases}$$

$\varphi_k \in Ax, \Psi(\varphi_k) \equiv 1, k < N$

$\varphi_N = S_\psi^a(\varphi_i), \Psi(\varphi_i) \equiv 1 \Rightarrow \Psi(S_\psi^a(\varphi_i) \equiv 1)$

$\varphi_N = m.p.(\varphi_i, \varphi_j), i, j < N$

продолжение см. (1)

(1)

$\varphi_i \mapsto \Psi(\varphi_i) \equiv 1$

$\varphi_j \mapsto \Psi(\varphi_j) \equiv 1 \qquad \varphi_j = (\varphi_i \to \varphi_N)$

$\varphi_N \mapsto \Psi(\varphi_N) \overset{?}{\equiv} 1$

$\Psi(\varphi_i \to \varphi_N) \equiv 1, \Psi(\varphi_i) \equiv 1$

$\Psi(\varphi_i \to \varphi_N) \overset{def}{=} \Psi(\varphi_i) \to \Psi(\varphi_N) \equiv 1 \Rightarrow \Psi(\varphi_N) \equiv 1$

$\Psi(\varphi_N)(x_1^*, ..., x_n^*) = 0$

$\Psi(\varphi_i)(x_1^*, ..., x_n^*) \to 0 = 1$

$$\left.\begin{matrix} \Psi(\varphi_i)(x_1^*, ..., x_n^*) = 1 \\ \Psi(\varphi_i)(x_1^*, ..., x_n^*) = 0 \end{matrix}\right\} - \text{пришли к противоречию}$$

ч.т.д.

3.3 Непротиворечивость ИВ.

3.3.1 Определение.

1) ИВ *противоречиво*, если формула A выводима в нем. $A \in$ *алфавиту*.
2) $\forall \varphi \in F :\mapsto \varphi$ ($\forall$ формула выводима в ИВ) $\Rightarrow$ ИВ *противоречиво*.
3) $\exists \varphi \in F ::\mapsto \varphi, \mapsto (\neg \varphi) \Rightarrow$ ИВ *противоречиво*.

ИВ *непротиворечиво*, если оно не является противоречивым.

Теорема: ИВ является непротиворечивым исчислением по отношению к любому из трех определений.

Док-во: (1) Если $\mapsto A$, то соответствующая ей булева функция будет тождественно равна 1. $\Psi(A) \equiv 1 \quad \Psi : A \mapsto \omega_i(x_1, x_2, ..., x_n) \quad f(x_1) \equiv x_1 \quad при\ x_1 = 0\ f(0) = 0 \neq 1 \Rightarrow противоречие$

(2) Если любая формула выводима, то выводима и A, что соответствует пункту 1.
(3) Пусть $\mapsto \varphi$ и $\mapsto (\neg\varphi)$ $\Psi(\varphi) = \Psi(x_1, x_2, ..., x_n) \equiv 1$ - булева функция

$$\Psi((\neg\varphi)) \overset{def}{=} \overline{\Psi(\varphi)} = \overline{\Psi(x_1, x_2, ..., x_n)} \equiv 0, \quad но\ \Psi((\neg\varphi)) \equiv 1,\ т.к. \mapsto (\neg\varphi)$$ - противоречие.

3.4 Формальные исчисления.

Алфавит – конечное или счетное множество символов, возможно, разбитых на группы. Алфавит должен быть упорядоченным множеством.
Слово – конечная упорядоченная последовательность символов алфавита, в т.ч. пустое слово.
V – множество всех слов.

Вычислимая функция от нескольких натуральных переменных $f(x_1, x_2, ..., x_n)$
(f – может быть не всюду определенной)
f – называется _вычислимой_, если $\exists$ такая машина Тьюринга, которая её вычисляет.

$M \subseteq N$ - _разрешимое_ множество, если характеристическая функция
$X_M(x) \overset{def}{=} \begin{cases} 1, & x \in M \\ 0, & x \notin M \end{cases}$ - является вычислимой.
Множество $M \subseteq N$ называется перечислимым, если $\exists$ такая вычислимая функция $f(x_1) : f(N) = M$
M - разрешимо $\Leftrightarrow$ M и $N \backslash M$ перечислимы.
M – перечислимо $\Leftrightarrow$ M – область определения некоторой вычислимой функции.
Множество всех формул F – некоторое разрешимое подмножество V.
T – счетное множество, если $\exists$ его биективное отображение на V.
$|T| = K_0$ - обозначение счетного множества. (K_0 - алеф-нуль)

Если $\exists$ и зафиксировано биективное и вычислимое отображение $f : L \xrightarrow{1-1} N$ (вычис.), то L – _ансамбль_.
V – ансамбль (слова лексикографически упорядочены и занумерованы)

Определение: В произвольном формальном исчислении: $Ax \subseteq F$ - множество всех аксиом – разрешимое подмножество множества всех формул.

$$\frac{\varphi}{S_\psi^a(\varphi)} \qquad \frac{\varphi^\varphi \to \psi}{\psi} \qquad ;F^2 \to F \qquad S_\psi^a : F \to F$$

Правило вывода:
$r(\varphi_1, \varphi_2, ..., \varphi_n) = \psi, \quad F^n \to F$,при $n \le N$ разрешимо. Для ИВ N=2.
Пример:
$L : A = \{a_j\}; \quad V; \quad F = V \qquad Ax = \{\Lambda\}$ (пустое слово) , $|Ax| = 1$
$\operatorname{Re} g = \{r_1\},\ r_1(u) = uaa$

$$1: \begin{cases} \Lambda \\ aa \\ aaaa \end{cases} \quad 2: \begin{cases} \Lambda \\ \Lambda \\ \Lambda \end{cases} \quad 3: \begin{cases} \Lambda \\ aaaa \\ \end{cases}$$

1 и 2 – формальные выводы.
3 – не является формальным выводом.

4 Предикаты и кванторы.

4.1 Определение предиката.

$P=\{1055>1999\}$

$P(x)=\{x>1999\}$ - высказывание, содержащее переменную.

$x\in N$ - предметная область предиката.

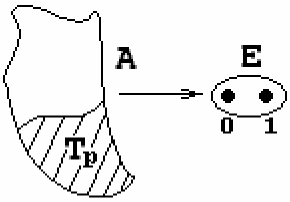
$x_1,x_2\in N \quad P(x_1)=1 \quad P(x_2)=0 \quad P:N\to E=\{0,1\}$

Пусть А – множество объектов произвольной природы (*предметная область предиката*).

n-местный предикат – произвольное отображение $P:A^n\to E$

$P(x_1,...,x_n)\in E,\ \ x_i\in A\ \ \forall i$

Множество истинности данного предиката $P:T_p=\{(x_1,...,x_n)\in A^n:P(x_1,...,x_n)=1\}$



$P=X_A(x)$ -
- характеристическая функция от x на множестве A - совпадает с предикатами

$P(x)\vee Q(x,y)=R_1(x,y) \qquad P(x)Q(x,y)=R_2 \qquad P\to Q=R_3$

$T_{PVQ}=T_P\cup T_Q \qquad T_{P\&Q}=T_P\cap T_Q$

$\varphi(P,Q)=R_4(x,y)$

4.2 Понятие квантора.

$\sum_{S=1}^{n}a_k=\sum_{S=1}^{n}a_S$ k – связанная переменная
n – свободная переменная

$\int_0^t f(x)dx=\int_0^t f(s)ds$ t – свободная, x – связанная.

$\int_a^b F(x,y)dx$, a,b,y – свободные переменные, x – связанная.

$P(x)="x>1999", \quad x\in N$

$(\exists x)P(x)=1$

$(\forall x)P(x)=0$

$Q(m,n)="m\ делит\ n", \quad A=N\setminus\{0\}$

$(\forall m)Q(m,n)=R(n) \quad (\exists m)Q(m,n)=T(n)\equiv 1$

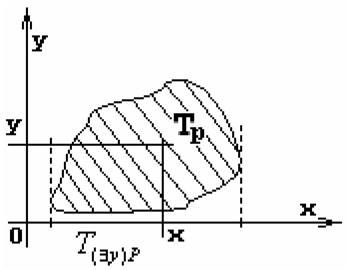
$(\forall n)Q(m,n)=S(m) \quad (\exists n)Q(m,n)=T(m)\equiv 1$

$S(m)=\begin{cases}1, & m=1\\ 0, & m\neq 1\end{cases}$

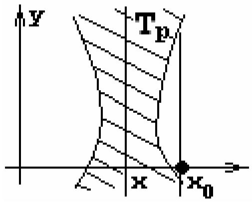
$(\forall x)R(y,z)\equiv R(y,z)$

$(\exists x)R(y,z)\equiv R(y,z)$

4.3 Геометрическая интерпретация навешивания кванторов.



$(\exists y)P(x,y)$
$x,y \in R$
$x \in T_{(\exists y)P} \Leftrightarrow (\exists y)P(x,y)=1 \Leftrightarrow$
$\Leftrightarrow (\exists y)(x,y) \in T_P$
$T_{(\exists x)P(x,y)}$ - ортогональная проекция на ось x



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

Пронесение отрицания через кванторы

$\overline{(\forall x)P(x,y)} = (\exists x)\overline{P(x,y)}$
$\overline{(\forall y)P(x,y)} = (\exists y)\overline{P(x,y)}$
$\overline{(\exists x)P(x,y)} = (\forall x)\overline{P(x,y)}$
$\overline{(\exists y)P(x,y)} = (\forall y)\overline{P(x,y)}$

$Q(x,y) \overset{def}{=} \overline{P(x,y)}$
$\overline{(\forall x)Q(x,y)} = (\exists x)\overline{Q(x,y)}$
$(\forall x)Q(x,y) = ((\forall x)\overline{P(x,y)}) = \overline{\overline{(\exists x)\overline{Q(x,y)}}} = (\overline{(\exists x)P(x,y)})$

Геометрическое 'доказательство':
$*: x_0 \in T_{\overline{(\forall y)P}} = R \setminus T_{(\forall y)P} \quad A \setminus T_P = T_{\overline{P}}$; x_0 не обладает свойством, что прямая $x = x_0$ целиком лежит в T_P
$(x_0,y_0) \notin T_P \quad \exists y_0 \in R; \quad (x_0,y_0) \in R^2 \setminus T_P$
$(x_0,y_0) \in T_{\overline{P}}, \quad \exists y_0 \in R: \quad (x_0,y_0) \in T_{\overline{P}}$
$(\exists y)\overline{P(x,y)} = 1 \qquad x_0 \in T_{(\exists y)\overline{P}}$ ч.т.д.

$(\exists y)P(x,y) \quad y \subset A, \quad y_1, y_2, \ldots.$
$(\exists y)P(x,y) = P(x,y_1) \vee P(x,y_2) \vee \ldots$
$(\forall y)P(x,y) = P(x,y_1) \,\&\, P(x,y_2) \,\&\, \ldots$

$\neg(\forall x)(P(x,y) \vee (\exists y)\overline{Q(x,y)}) =$
$= \{(\exists y)(P(x,y) \vee \overline{Q(x,y)})\} =$
$= \neg(\forall x)(P(x,y) \vee (\exists z)\overline{Q(x,z)}) =$
$= \neg(\forall x)((\exists z)P(x,y) \vee (\exists z)\overline{Q(x,z)}) =$
$= \neg(\forall x)(\exists z)(P(x,y) \vee \overline{Q(x,z)}) =$
$= (\exists x)(\forall z)(\overline{P(x,y) \vee \overline{Q(x,z)}}) =$
$= (\exists x)(\forall z)(\underbrace{\overline{P(x,y)} \vee Q(x,z)}_{\text{предикат от } (x,y,z) \text{ зав от } y}).$