Оглавление

Элементы Теории Алгоритмов

1.1 Понятие алгоритма в интуитивном смысле слова

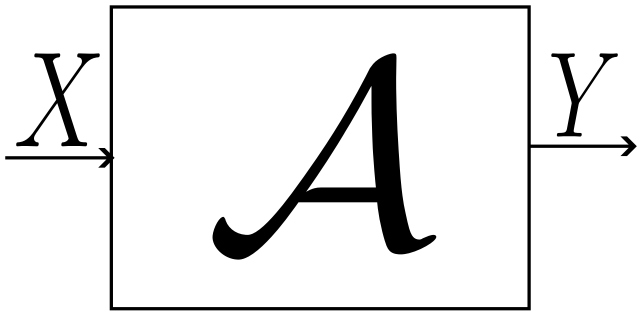


Рис. 1.1: Команда

$\mathcal{A} : X \to Y$

Признаки алгоритма:

- Признак детерминизированности (нет выбора в алгоритме)
- Признак массовости (работает для всех входных данных одного типа , например, квадратных уравнений)
- Признак результативности (ожидается какой-то результат)

Определение 1. алгоритм A применим к элементу x. (То есть останавливается за n шагов)

$$(x \in X)(!A(x))$$

Определение 2. $\neg!A(x)$ - алгоритм A не применим к x.

Определение 3. Конструктивный объект - слово в конечном алфавите.

Определение 4. Вербальная, или словарная, функция - это

$$f : V^* \underset{\bullet}{\to} W^*$$

Вербальная функция (V, W).

Определение 5. Алгоритм можно записать так:

$$\mathcal{A} : V^* \underset{\bullet}{\to} W^*$$

Определение 6. Функция $f : V^* \underset{\bullet}{\to} W^*$ называется вычислимой в интуитивном смысле слова, если существует алгоритм $\mathcal{A}_f : V^* \to W^*$ такой, что

$$(\forall x \in V^*)((!\mathcal{A}_f(x) \iff x \in D(f))\,\&(\mathcal{A}_f(x) = f(x)))$$

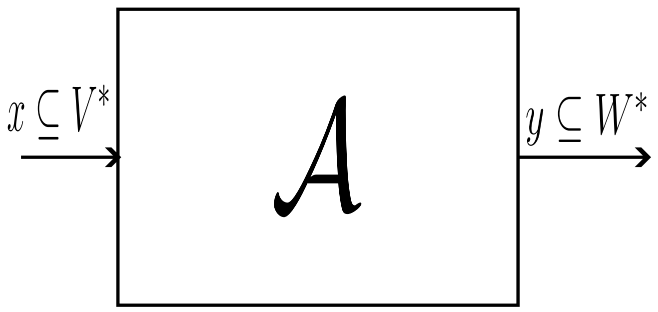


Рис. 1.2: Автомат

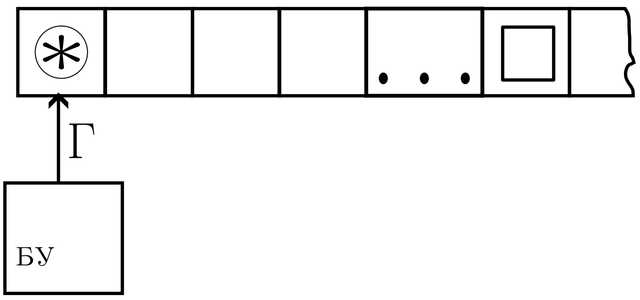


Рис. 1.3: Машина Тьюринга

1.2 Машина Тьюринга.

Команды следующего формата:

$$qa \to rb, \begin{Bmatrix} S \\ L \\ R \end{Bmatrix}; q, r \in Q; a, b \in V \cup \{\circledast, \square\}$$

Заметка. Мы считаем, что у нас не может быть команд с одинаковыми левыми частями.

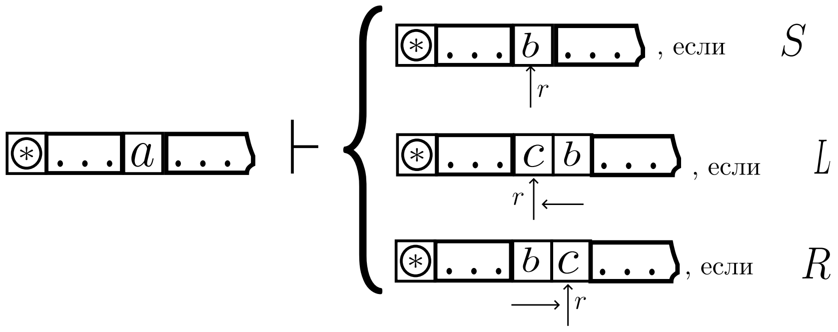
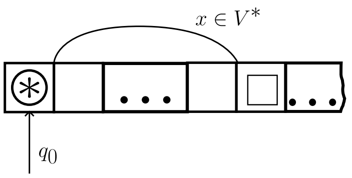
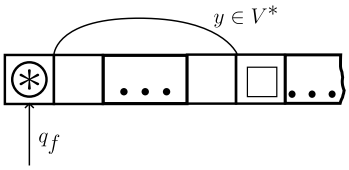


Рис. 1.4: Что к чему

Начальная конфигурация:



Заключительная конфигурация:



Пример программы:

$$
\begin{aligned}
&q_0\circledast \to q_0\circledast, R\\
&q_0a \to q_0a, R\\
&q_0b \to q_0b, R\\
&q_0c \to q_1c, R\\
&q_1a \to q_2a, R\\
&q_1b \to q_0b, R\\
&q_1c \to q_1c, R\\
&q_2a \to q_0a, R\\
&q_2b \to q_3b, R\\
&q_2c \to q_1c, R\\
&q_3\alpha \to q_3\alpha, R \;//\alpha \in \{a, b, c\}\\
&q_3\Box \to q_4\Box, R\\
&q_i\Box \to q_5\Box, L \;//i = 0, 1, 2\\
&q_4\circledast \to q_f1, L\\
&q_5\alpha \to q_5\Box, L\\
&q_5\circledast \to q_5*, R\\
&q_5\Box \to q_f0, L
\end{aligned}
$$

$$
f(x) = \begin{cases} 1, \text{ если } cab \sqsubseteq x \in \{a, b, c\} \\ 0 \text{ иначе} \end{cases}
$$

Определение 7. Машина Тьюринга (МТ):

$$
\mathcal{J} = (V, Q, q_0, q_f, *, \Box, S, L, R, \delta)
$$

Конфигурация МТ:

$$
C = (q, x, ay),
$$

где $q \in Q$, а $x, y \in (V \cup \{*, \Box\})^*, a \in V \cup \{*, \Box\}$

Мы полагаем, что

$$
(q, x, ay) \underset{\mathcal{J}}{\vdash} \begin{cases} (r, x, by), \text{ если } qa \to rb, S \in \delta \\ (r, x', cby), \text{ где } x'c = x, \text{ если} qa \to rb, L \in \delta \\ (r, xb, dy'), \text{ где } y = dy', \text{ если } qa \to rb, R \in \delta \end{cases}
$$

Определение 8. Вывод на множестве конфигураций:

$$K_0, K_1, \ldots, K_n, \text{ где } (\forall i \geq 0)(K_i \vdash K_{i+1}, \text{ если } K_{i+1} \text{ определен в последовательности})$$

$$K \underset{\mathcal{J}}{\vdash^*} K', \text{ если существует вывод } K = K_0 \vdash K_1 \vdash \ldots \vdash K_n = K'$$

Дано:
Начальная конфигурация $C_0 = (q_0, \lambda, \circledast x \Box)$, где $x \in V^*$
Конечная конфигурация $C_f = (q_f, \lambda, \circledast y \Box)$, где $y \in V^*$

Определение 9. Машина Тьюринга применима к слову x, то есть

$$!\mathcal{T}(x) \leftrightharpoons$$
$$\leftrightharpoons C_0 = (q_0, \lambda, \circledast x \Box) \vdash^* C_f = (q_f, \lambda, \circledast y \Box);$$

при этом $y \leftrightharpoons \mathcal{T}(x)$

При этом если не применимо к машине тьюринга данное слово, то

$$\neg!\mathcal{T}(x)$$

Определение 10. Конфигурация машины Тьюринга называется тупиковой, если она не является заключительной и при этом из нее не выводится ни одна конфигурация.

Пример.

$$f(x) = \begin{cases} \#, \text{ если } x = \lambda \\ \lambda, \text{ если } cab \sqsubseteq x \\ x, \text{ если } x \neq \lambda \text{ и } cab \not\sqsubseteq x \end{cases}$$

λ - Пустое слово.

Тогда программа записывается так:

$$\begin{aligned}
&q_0\circledast \to q_0\circledast, R \\
&q_0\Box \to q_f\#, L \\
&q_0a \to q_0'a, R \\
&q_0b \to q_0'b, R \\
&q_0c \to q_1c, R \\
&q_0'a \to q_0'a, R \\
&q_0'b \to q_0'b, R \\
&q_0'c \to q_1c, R \\
&q_1a \to q_2a, R \\
&q_1b \to q_0'b, R \\
&q_1c \to q_1c, R \\
&q_2a \to a_0'a, R \ //caa \\
&q_2b \to q_3b, R \ //cab \\
&q_2c \to q_1c, R \ //cac \\
&q_3\alpha \to q_3\alpha, R \ //\alpha \in \{a, b, c\} \\
&q_3\Box \to q_4\Box, L \\
&q_4\alpha \to q_4\Box, L \\
&q_4\circledast \to q_f\circledast, S \\
&r\Box \to q_5\Box, L \ //r \in \{q_0', q_1, q_2\} \\
&q_5\alpha \to q_5\alpha, L \\
&q_5\circledast \to q_f\circledast, S
\end{aligned}$$

Для ошибочного решения (q_0' не вводится):

$$(a_1, \lambda, \circledast ab\Box) \vdash (q_0, \circledast, ab\Box) \quad \vdash (q_0, \circledast a, b\Box) \vdash (q_0, \circledast ab, \Box) \vdash \underline{(q_f, \circledast a, b\#\Box)}$$

Определение 11. Машина Тьюринга называется детерминированной, если из каждой ее конфигурации непосредственно выводится не более одной конфигурации.

Теорема 1.1. *Машина Тьюринга называется детерминированной тогда и только тогда, когда в ее программе (системе команд) нет двух (более) различных комманд с одинаковыми левыми частями.*

Соглашение. Во всех дальнейших суждениях машина Тьюринга будет считаться детерминированной. ДМТ - детерминированная машина Тьюринга.

Допустим машина Тьюринга с алфавитом V, то мы говорим, что это машина Тьюринга в алфавите V. Но если $V \supset V'$, то мы говорим, что Машина Тьюринга над алфавитом V.

Определение 12. Вербальная функция $f : V^* \underset{\bullet}{\to} V^*$ называется вычисломой по Тьюрингу, если может быть построена МТ $\mathcal{T}_f$ над алфавитом V такая, что

$$(\forall x \in V^*)(!\mathcal{T}(x) \iff x \in D(f) \,\&\, \mathcal{T}_f(x) = f(x))$$

Тезис Тьюринга. Он гласит, что любая вербальная функция, вычислимая в интуитивном смысле слова, вычислима по Тьюрингу.

Общие разделы:

1. Основная модель.
2. Понятие вычислимой функциию. Основная гипотеза.
3. Эквивалентный алгоритм.
4. Теорема сочетания.
5. Универсальный алгоритм.
6. Разрешимые перечислимые множества (языки).
7. Анализ алгоритмически неразрешимых задач.

1.3 Нормальные алгорифмы Маркова

Предположим, что есть

$$V; x, y \in V^*; x \sqsubseteq y \leftrightharpoons (\exists y_1, y_2)(y = y_1 x y_2)$$

причем тройка слов $(y1, x, y2)$ - вхождение слова x в слово y.

Некоторые свойства:

- $(\forall x)(\lambda \sqsubseteq x)$
- $(\forall x)(x \sqsubseteq x)$
- $(\forall x)(\forall y)(\forall z)(x \sqsubseteq y, y \sqsubseteq z \implies x \sqsubseteq z)$

Записывается иногда так: $y_1 * x * y_2$ $(x \notin V)$
Пример: $y = \underbrace{\text{вход}}_{x}\text{ит}$; $*$вход$*$ит - корень
Еще один: $\underbrace{\text{абра}}_{x}\text{када}\underbrace{\text{бра}}_{x}$

Среди всех вхождений x в y выделяется первое, или главное, вхождение, а именно имеющую наименьшую длину левого крыла (самое левое вхождение).

Определение 13. Подстановка:

$$u, v \in V^* \quad \underbrace{u}_{\text{л.ч.}} \to \underbrace{v}_{\text{п.ч.}}; \to \notin V$$

Определение 14. Омега применима, или подходит, если ее левая часть входит в слово x.

$$\omega : u \to v$$

Тогда вхождение:

$$x = x_1 u x_2;\ x_1 * u * x_2 \text{ - 1-е вхождение u в x}$$

Отсюда

$$y \leftrightharpoons \omega x \leftrightharpoons x_1 v x_2$$

Это можно представить так:

$$\begin{array}{rl} x & = \boxed{x_1}\boxed{u}\boxed{x_2} \\ & \qquad\ \downarrow \\ y = \omega x & = \boxed{x_1}\boxed{v}\boxed{x_2} \end{array}$$

Пример. Пусть дана замена:

$$\omega : B \to y$$

Тогда слово Входит превратится в слово уходит. $\omega x =$ уходит

Определение 15. Нормальный алгорифм $\mathcal{A} = (V, S, \mathcal{P})$

Пример.

$$\mathcal{A} : \begin{cases} \#a \to a(1) \\ \#b \to b\# \\ \# \to \cdot aba \\ \ \to \# \end{cases}$$

Рассматриваем систему сверху вниз и ищем первую подходящую формулу. Пусть

$$x = bbab$$

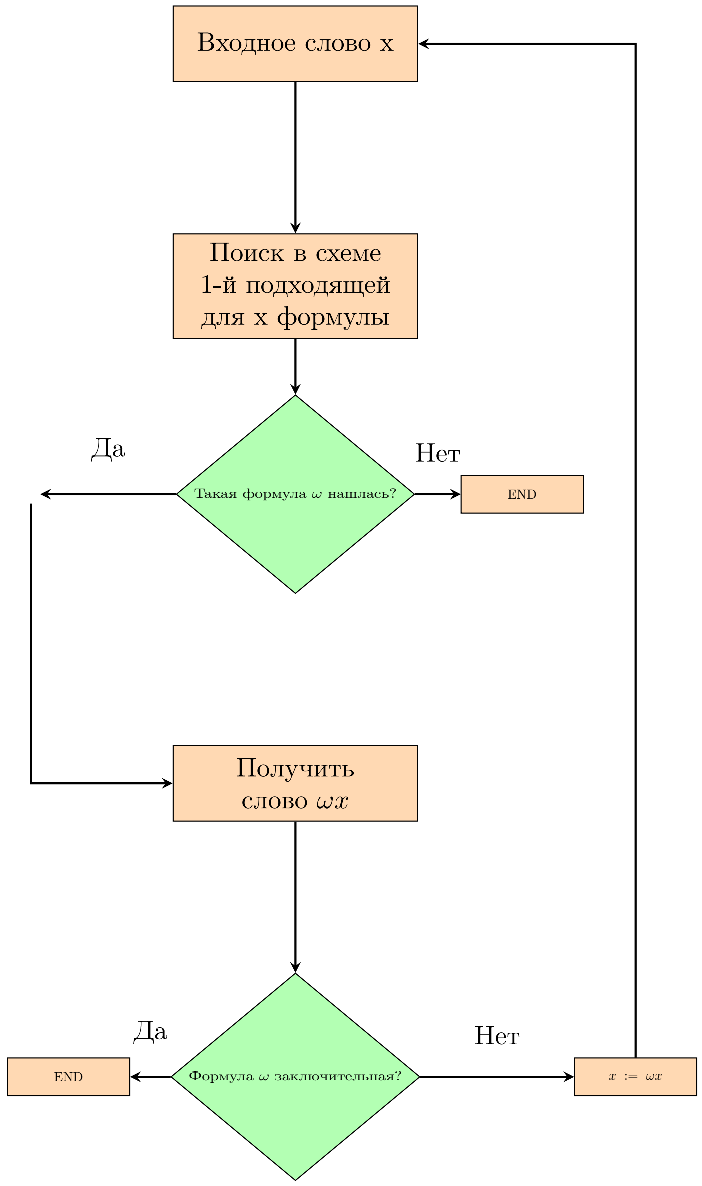
Отсюда получаем:

$$x = bbab \vdash \#bbab \vdash b\#bab \vdash bb\#ab \vdash bba\#b \vdash bbab\# \vdash \cdot bbab\underline{aba}$$

Общий вид:

$$\mathcal{A} : \begin{cases} u_1 \to [\cdot]v_1 \\ u_2 \to [\cdot]v_2 \\ \vdots \\ u_n \to [\cdot]v_n \end{cases}$$

Можно записать это в виде блок-схемы неформально:



Теперь формально опишем его. Распишем 5 разных ситуаций.

1) $\mathcal{A} : x \vdash y \leftrightharpoons$ непосредственно просто переводит слово x в слово y $\leftrightharpoons y = \omega x$, где ω - 1-я в схеме $\mathcal{A}$ формула, которая оказывается простой

2) $\mathcal{A} \vdash \cdot y \leftrightharpoons$ Алгорифм А непосредственно заключительно переводит слово x в слово y $\leftrightharpoons y = \omega x$, где ω - 1-я в схеме $\mathcal{A}$, которая оказывается заключительной

3) $\mathcal{A}x \models y \leftrightharpoons$ Алгорифм А переводит слово x в слово y, когда существует последовательность $x = x_0, x_1, \ldots, x_n = y$, где $(\forall i = \overline{0, n-1})(\mathcal{A} : x_i \vdash x_{i+1})$

4) $\mathcal{A} : x \models \cdot y \leftrightharpoons$ Алгорифм А заключительно переводит слово x в слово y $\leftrightharpoons \mathcal{A} : x \vdash \cdot y \vee (\exists z)(\mathcal{A} : x \models z \vdash \cdot y)$

5) $\sim \mathcal{A}(x) \leftrightharpoons$ в схеме А нет ни одной подходящей формулы для x.

Процесс работы НА $\mathcal{A} = (S, S, P)$ со словом $x \in V^*$: это последовательность слов $x = x_0, x_1, \ldots, x_n, \ldots$ такая, что $(\forall i \geq 0)(\mathcal{A} : x_i \vdash x_{i+1}$ или $\mathcal{A} : x_i \vdash \cdot x_{i+1})$, если x_{i+1} определено в последовательности.

Слово x_{i+1} и каждое слово $x_n n > i + 1$ считается неопределенным, если $\mathcal{A} : x_{i-1} \vdash \cdot x_i$ или $\sim \mathcal{A}(x_i)$

Если процесс работы НА $\mathcal{A}$ со словом конечный, то есть $x = x_0, x_1, \ldots, x_n, n \geq 0$, то $!\mathcal{A}(x)$ и $x_n \leftrightharpoons \mathcal{A}(x)$. В противном случае пишем $\neg!\mathcal{A}(x)$, то есть алгоритм со словом x будет бесконечный, или не останавливается.

Об алфавитах в НА. Пусть НА алгорифм $\mathcal{A} = (V, S, P)$. Тогда мы говорим, что это НА в алфавите V. Пусть $\mathcal{A}_1 = (V_1 \subset V, S_1, P_1)$ - нормальный алгорифм над алфавитом V.

Определение 16. Вербальная функция $f : V^* \underset{\bullet}{\to} V^*$ называется вычислимой по Маркову, если может быть построен нормальный алгорифм $\mathcal{A}_f$ над алфавитом V такой, что

$$(\forall x \in V^*)(!\mathcal{A}_f(x) \Longleftrightarrow x \in D(f))\,\&(\mathcal{A}_f(x) = f(x))$$

Гипотеза НА (Принцип нормализации). Любая вербальная функция, вычислимая в интуитивном смысле слова, вычислима по Маркову.

Примеры НА. Первый пример.

$$\mathcal{J}\alpha : \begin{cases} \to \bullet \end{cases}$$

Получаем вот что: $(\forall x)(\mathcal{J}\alpha(x) = x)$, то есть вычисляет тождественную функцию в любом алфавите.

Второй пример.

$$Null : \begin{cases} \to \end{cases}$$

Для любого слова будет работать бесконечно: $(\forall x)\neg !Null(x)$

Третий пример.

$$Lc : \begin{cases} \to \bullet x_0, \text{ где } x_0 \in V^* \text{ - \underline{фиксированное} слово} \end{cases}$$

Получим: $x \in V^* : x \vdash \bullet x_0 x$, то есть $Lc(x) = x_0 x$

Четвертый пример.

$$Rc : \begin{cases} \#\xi \to \xi\# \\ \# \to \bullet x_0 (x_0 \in V^* \text{ - фиксированное слово }) \\ \to \# \end{cases}$$

$$x \in V^*, x = x(1)x(2)\ldots x(k) \vdash \#x(1)x(2)\ldots x(k) \vdash x(1)\#x(2)\ldots x(k) \models^{k-1} x\# \vdash \bullet x x_0$$

Пятый пример.

$$Double : \begin{cases} \alpha\xi \to \xi\beta\xi\alpha \\ \beta\xi\eta \to \eta\beta\xi \\ \beta \to \\ \alpha \to \bullet \\ \to \alpha \end{cases}$$

Причем $\alpha, \beta \notin V; \xi, \eta \in V$.

Первый тест: $\lambda \vdash \alpha \vdash \bullet\lambda$.

Второй тест: $a \vdash \alpha a \vdash a\beta a\alpha \vdash aa\alpha \vdash \bullet aa$

Третий тест:

$$\begin{aligned} abca &\vdash \alpha abca \vdash a\beta a\alpha bca \vdash a\beta ab\beta b\alpha ca \vdash \\ &\vdash a\beta ab\beta bc\beta c\alpha a \vdash a\beta ab\beta bc\beta ca\beta a\alpha \vdash \\ &\vdash ab\beta a\beta bc\beta ca\beta a\alpha \vdash ab\beta ac\beta b\beta ca\beta a\alpha \vdash \\ &\vdash abc\beta a\beta b\beta ca\beta a\alpha \vdash abc\beta a\beta ba\beta c\beta a\alpha \vdash \\ &\vdash abc\beta aa\beta b\beta c\beta a\alpha \vdash abca\beta a\beta b\beta c\beta a\alpha \models^4 \\ &\models^4 abcaabca\alpha \vdash \bullet abcaabca \end{aligned}$$

Можно строго доказать, что

$$(\forall x \in V^*)(Double(x) = xx = x^2)$$

1.4 Эквивалентность нормальных алгоритмов. Теорема о переводе.

Пусть даны $\mathcal{A}, \mathcal{B} : V^* \underset{\bullet}{\to} V^*$ над алфавитом V.

Определение 17. Алогрифмы $\mathcal{A}, \mathcal{B}$ называются эквивалентными относительно алфавита V, если

$$(\forall x \in V^*)(!\mathcal{A}(x) \Longleftrightarrow !\mathcal{B}(x) \,\&(\mathcal{A}(x) = \mathcal{B}(x)))$$

Это называется условным равенством:

$$\mathcal{A}(x) \simeq \mathcal{B}(x)$$

Рассмотрим такую конструкцию, называемую замыканием НА.

$$\mathcal{A} : \begin{cases} u_1 \to [\bullet]v_1 \\ \vdots \\ u_n \to [\bullet]v_n \end{cases}$$

$$\mathcal{A}^{\bullet} : \begin{cases} \text{Схема } \mathcal{A} \\ \to \bullet \end{cases}$$

То есть

$$(\forall x \in V^*)\mathcal{A}^{\bullet}(x) \simeq \mathcal{A}(x)$$

Рассмотрим преобразования:
$\mathcal{A} : x \models \bullet y$, то есть $\mathcal{A}(x) = y; \mathcal{A}^{\bullet} : x \models y = \mathcal{A}(x)$.
$\mathcal{A} : x \models y$, то есть $y = \mathcal{A}(x); \mathcal{A}^{\bullet} : x \models y \vdash \bullet y = \mathcal{A}(x)$

Заметка. Переход к замыканию НА позволяет без ограничения общности не рассматривать ситуацию естественного обрыва процесса работы.

Если $!\mathcal{A}(x)$, то $x \models \bullet\mathcal{A}(x)$ (система $\mathcal{A}$ замкнутая)

Естественное распространение НА на более широкий алгорифм. $\mathcal{A} = (V, S, P)$ и пусть $V' \supset V$. Тогда $\mathcal{A}' = (V', S, P)$. То есть просто означает, что рассматриваем тот же алгоритм в более широком алфавите. Из этого следует, что

$$(\forall x \in V^*)(\mathcal{A}(x) \simeq \mathcal{A}(x))$$

Формальное распространение НА на более широкий алфавит. $\mathcal{A} = (V, S, P)$ в алфавите V.

$$\mathcal{A}^f : \begin{cases} \eta \to \eta \; //\eta \in V' \setminus V \\ \text{Схема } \mathcal{A} \end{cases}$$

Получаем:

$$(\forall x \in V^*)(\mathcal{A}^f(x) = \mathcal{A}(x)), \text{ но если } x \notin V^*, \text{ то } \neg!\mathcal{A}^f(x)$$

Нам нужно расширить алфавит. Как это делается?
Рассмотрим алфавиты $V = \{a_1, a_2, \dots, a_n\}, V_\alpha = \{\alpha, \beta\}$ и $V \cap V_\alpha = \varnothing$
Тогда считается

$$[a_i \leftrightharpoons \alpha\beta^i\alpha; \quad [\lambda = \lambda; \quad [x = [x(1)x(2)\dots x(k) \leftrightharpoons [x(1)[x(2)\dots[x(k)$$

Пример.

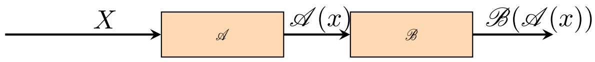
$$[\underbrace{abca}_{V_0} = \underbrace{010}_{a}\underbrace{0110}_{b}\underbrace{0111}_{c}\underbrace{010}_{a}$$

$V_\alpha = \{\alpha, \beta\}$
Чаще всего будет рассматривать такой алфавит: $V_0 = \{0, 1\}$

Теорема 1.2. *(О переводе). Каков бы ни был нормальный алгорифм $\mathcal{A} = (V', S, P)$ над алфавитом $V \subset V'$, может быть построен НА $\mathcal{B}$ в алфавите $V \cup V_\alpha$ так, что $(\forall x \in V^*)(\mathcal{B}(x) \simeq \mathcal{A}(x))$*

1.5 Теорема сочетания

1.5.1 Композиция



Теорема 1.3. *(О композиции). Каковы бы ни были НА* $\mathcal{A}, \mathcal{B}$ *в алфавите* V *может быть построен НА алгорифм* $\mathcal{C}$ *над алфавитом* V *такой, что*

$$(\forall x \in V^*)(\mathcal{C}(x) \simeq \mathcal{B}(\mathcal{A}(x)))$$

Доказательство. Вводится алфавит двойников.

$V = \{a_1, a_2, \dots, a_n\}$ $\overline{V} = \{\overline{a_1}, \overline{a_2}, \dots, \overline{a_n}\}$

Вводятся две буквы α, β такие, что $\alpha, \beta \notin V \cup \overline{V}$

$$\mathcal{C} : \begin{cases} \xi\alpha \to \alpha\xi \ //\xi \in V \\ \alpha\xi \to \alpha\overline{\xi} \\ \overline{\xi}\eta \to \overline{\xi}\overline{\eta} \ //\xi, \eta \in V \\ \overline{\xi}\beta \to \beta\overline{\xi} \\ \beta\overline{\xi} \to \beta\xi \\ \xi\overline{\eta} \to \xi\eta \\ \alpha\beta \to \bullet \\ \overline{\mathcal{B}_\alpha^\beta} \\ \mathcal{A}^\alpha \end{cases}$$

A$^\bullet$	A$^\alpha$
u $\to v$	u$\to v$
u$\to \bullet v$	u$\to \alpha v$

B$^\bullet$	$\overline{\mathcal{B}_\alpha^\beta}$
u$\to v$	$\overline{u} \to \overline{v}$
u $\neq \lambda$	
$\to v$	$\alpha \to \alpha\overline{v}$
u$\to \bullet v$	$\overline{u} \to \beta\overline{v}$
$\to \bullet v$	$\alpha \to \alpha\beta\overline{v}$

Примерно идея доказательства. $x \in V^*$

$$\mathcal{C} : x \models_{(9)}^{!\mathcal{A}^\bullet(x)} y_1\alpha y_2, \text{ где } y_1 y_2 = \mathcal{A}^\bullet(x)$$

Если $\neg!\mathcal{A}^\bullet(x)$, то и $\neg!\mathcal{C}(x)$, заметим. Отсюда

$$y_1\alpha y_2 \models_{(1)} \alpha y_1 y_2 = \alpha y = \alpha y(1)y(2)\dots y(m),$$

где $y_1 y_2 = y$. Далее получаем

$$\alpha y(1)y(2)\dots y(m) \vdash_{(2)} \alpha\overline{y(1)}y(2)\dots y(m) \models_{(3)} \alpha\overline{y(1)y(2)}\dots\overline{y(m)} = \alpha\overline{y}$$

Следующий, третий шаг

$$\alpha\overline{y} \models_{(8)} \alpha\overline{z_1}, \beta\overline{z_2}_z, \text{ где } z_1, z_1 = z = \mathcal{B}^\bullet(y), \text{ если } !\mathcal{B}(y)$$

Заметим, что если $\neg!\mathcal{B}^\bullet(y) \implies \neg!\mathcal{C}(y) \implies \neg!\mathcal{C}(x)$. Получаем

$$\alpha\overline{z_1}\beta\overline{z_2} \models_{(4)} \alpha\beta\overline{z_1 z_2} = \alpha\beta\overline{z} \models_{(5),(6)} \alpha\beta z \vdash \bullet z = \mathcal{B}^\bullet(y) = \mathcal{B}^\bullet(\mathcal{A}^\bullet(x)) = \mathcal{B}(\mathcal{A}(x))$$

□

Пример.

$$\mathcal{A}^{\bullet}: \begin{cases} \#\alpha \to \alpha\# \\ \#\beta \to \beta\# \\ \# \to \bullet aba \\ \to \# \\ \to \bullet \end{cases}$$

$$\mathcal{B}^{\bullet}: \begin{cases} \to \bullet babb \\ \to \bullet \end{cases}$$

Строим систему:

$$\mathcal{A}^{\alpha}: \left[\begin{array}{c} a \to a\# \\ \#b \to b\# \\ \# \to \alpha aba \\ \to \# \\ \to \alpha \end{array} \right.$$

$$\overline{B}^{\beta}_{\alpha}: \left[\begin{array}{c} \alpha \to \alpha\beta\overline{babb} \\ \alpha \to \alpha\beta \end{array} \right.$$

$$\begin{aligned} & x = bab \vdash \#bab \models bab\# \vdash bab\alpha aba \models \alpha bababa \vdash \\ & \vdash \alpha\bar{b}ababa \models \alpha\overline{bababa} \vdash \\ & \vdash \alpha\beta\overline{babbbababa} \vdash \alpha\beta\alpha\beta b\overline{abbbababa} \models \\ & \models \alpha\beta babbbababa \vdash \bullet babbbababa \end{aligned}$$

Отсюда видно:

$$\mathcal{C} \fallingdotseq \mathcal{B} \circ \mathcal{A};$$

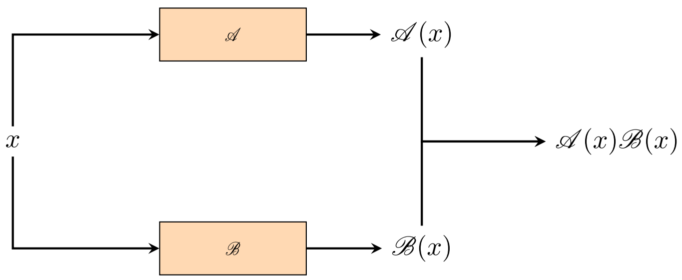
$$\mathcal{B} \circ \mathcal{A}(x) \simeq \mathcal{B}(\mathcal{A}(x));$$

$$\mathcal{A}_n \circ \mathcal{A}_{n-1} \circ \ldots \circ \mathcal{A}_1 \fallingdotseq \mathcal{A}_n \circ (\mathcal{A}_{n-1} \circ \ldots \circ \mathcal{A}_1), n \geq 1;$$

Определение 18. Степень алгорифма:

$$\mathcal{A}^n \fallingdotseq \mathcal{A} \circ \mathcal{A}^{n-1}, n \geq 1, \text{ где } \mathcal{A}^0 \fallingdotseq \mathcal{J}\alpha$$

1.5.2 Объединение



Теорема 1.4. *(Объединения). Каковы бы ни были НА $\mathcal{A}, \mathcal{B}$ в алфавите V, может быть построен НА $\mathcal{A}$ над алфавитом V так, что*

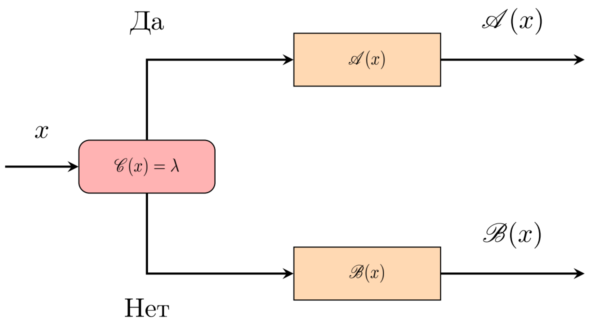
$$(\forall x \in V^*)(\mathcal{C}(x) \simeq \mathcal{A}(x)\mathcal{B}(x))$$

Можно представить это так:

$$\overline{\mathcal{C}(x\$y)} \simeq \mathcal{A}(x)\$\mathcal{B}(y)$$

$$\$ \notin V$$

1.5.3 Разветвление



Записать в виде псевдокода можно так:

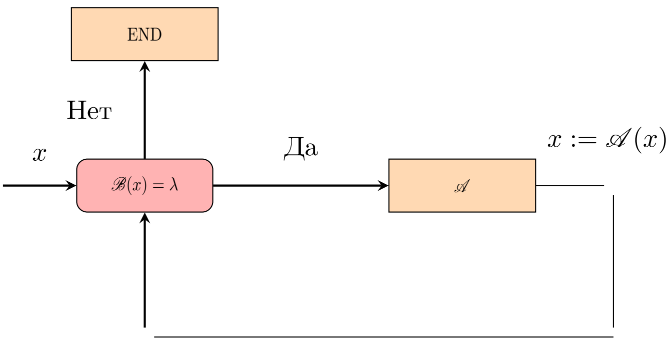
$$if(\mathcal{C}(x) = \lambda)\ \underline{then}\ y := \mathcal{A}(x)\ \underline{else}\ y := \mathcal{B}(x);$$

Теорема 1.5. *(О разветвлении). Каковы бы ни были НА $\mathcal{A}, \mathcal{B}, \mathcal{C}$ в алфавите V, может быть построен НА D над алфавитом V так, что*

$$(\forall x \in V^*)(D(x) = \mathcal{A}(x),\ \textit{если}\ \mathcal{C}(x) = \lambda)\ \textit{и}\ (D(x) = \mathcal{B}(x),\ \textit{если}\ \mathcal{C}(x) \neq \lambda)$$

$D \leftrightharpoons \mathcal{C}(\mathcal{A} \vee \mathcal{B})$

1.5.4 Повторение



В виде псевдокода:

- Для цикла с условием, пока правда:

$$\underline{while}\ \mathcal{B}(x) = \lambda\ \underline{do}\ x := \mathcal{A}(x)\ \underline{end};\ \text{Записывается так: } {}_{\beta}\{\mathcal{A}\}$$

- Для цикла с условием, пока неправда:

$$\underline{while}\ \mathcal{B}(x)! = \lambda\ \underline{do}\ x := \mathcal{A}(x)\ \underline{end};\text{Записывается так: } {}_{\beta}\langle\mathcal{A}\rangle$$

Теорема 1.6. *(Повторения). Каковы бы ни были НА $\mathcal{A}, \mathcal{B}$ в алфавите V, может быть построен НА $\mathcal{C}$ над алфавитом V такой, что $!\mathcal{C}(x) \leftrightharpoons (\mathcal{B}(x) \neq \lambda)$ и тогда $\mathcal{C}(x) = x$ или существует последовательность $x = x_0, x_1, \ldots, x_n$, где $(\forall i = \overline{0, n-1})$ $(\mathcal{B}(x_i) = \lambda)$ и $x_{i+1} = \mathcal{A}(x_i)$; $\mathcal{B}(x_n) \neq \lambda$ и $\mathcal{C}(x) = x_n$*

Примеры использования теоремы сочетания.

1) Проекцирующие НА

   Дано $V, \$ \notin V$. Векторное слово в алфавите $V : x_1\$x_2\$\ldots\$x_n, n \geq 1$, где $(\forall i = \overline{1, n})(x_i \in V^*)$

   Нужен алгоритм, который вычисляет его x_i

   $\prod_i(x_1\$x_2\$\ldots\$x_n) = x_i, \quad i = 1\ldots n$

$$\mathscr{P}_1 : \begin{cases} \$\eta \to \ //\eta \in V \\ \$ \to \\ \to \bullet \end{cases}$$

Результат работы $\mathscr{P}_1(x_1\$x_2\$\ldots\$x_n) = x_1$

$$\mathscr{P}_2 : \begin{cases} \eta \to \# \ //\eta \in V, \# \notin V \\ \# \to \bullet \\ \$ \to \# \end{cases}$$

То есть $\mathscr{P}_2(x_1\$x_2\$\ldots\$x_n) = x_2\$\ldots\$x_n$

Получаем $\prod_i = \mathscr{P}_1 \circ \mathscr{P}_2^{i-1}, \quad 1 \le i \le n$

i = 1: $\mathscr{P}_2^{i-1} = \mathscr{P}_2^0 = \mathcal{J}\alpha$

i = n: $\mathscr{P}_2^{n-1}(x_1\$x_2\$\ldots\$x_n) = x_w; \quad \mathscr{P}_1(x_n) = x_n$

2) НА распознавания равенства слов

$EQ(x\$y) = \lambda \iff x = y; \quad x, y \in V^*, \$ \notin V$

$EQ(x\$y) \simeq Comp(\mathcal{J}\alpha\$\mathcal{I}nv(y))$

$\mathcal{I}nv(y) = y^R$

$$Comp : \begin{cases} \eta\$\eta \to \$ \ //\eta \in V \\ \$ \to \bullet \end{cases}$$

$x^R = (x(1)x(2)\ldots x(k))^R = x(k)\ldots x(2)x(1)$

3) НА определения центра слова

$\mathscr{C}(x) = x_1\$x_2$, где $x_1x_2 = x, \quad ||x_1| - |x_2|| \le 1$, $x \in V^*; \quad \$ \notin V$

$\mathscr{C} = \mathscr{B} \circ {}_{\mathscr{A}}\langle L \circ R \rangle$

$$L : \begin{cases} \alpha\beta \to \bullet\alpha\beta \\ \alpha\xi \to \bullet\xi\alpha \ //\xi \in V, \alpha \notin V \\ \to \alpha \end{cases}$$

$$R : \begin{cases} \gamma\xi \to \xi\gamma \ //\xi \in V; \beta, \gamma \notin V \\ \xi\gamma \to \bullet\beta\xi \\ \xi\beta \to \bullet\beta\xi \\ \to \gamma \end{cases}$$

$$\mathscr{A} : \begin{cases} \alpha\beta\xi \to \alpha\beta \\ \xi\alpha\beta \to \alpha\beta \\ \alpha\beta \to \bullet \\ \to \bullet \end{cases}$$

$$\mathscr{B} : \begin{cases} \alpha\beta \to \bullet\$ \\ \to \bullet\$ \end{cases}$$

Пример 1. $\lambda, \quad \mathscr{B}(\lambda) = \$$

$\mathscr{A}(\lambda) = \lambda \implies$ тело цикла не выполнилось

Пример 2. $x = a \in V$

$\mathscr{A}(a) = a \neq \lambda$

$R : a \vdash \gamma a \vdash a\gamma \vdash \bullet\beta a$

$L : \beta a \vdash \alpha\beta a \vdash \bullet\alpha\beta a$

$\mathscr{A}(\alpha\beta a) = \lambda$

$\mathscr{B}(\alpha\beta a) = \$a$

Пример 3. $x = ab$

$\mathscr{A}(ab) = ab \neq \lambda$

$R : ab \vdash \gamma ab \models^2 ab\gamma \vdash \bullet\alpha\beta b$

$L : \alpha\beta B \vdash \alpha a\beta b \vdash \bullet a\alpha\beta b$

$\mathscr{A}(a\alpha\beta b) = \lambda$

$\mathscr{B}(a\alpha\beta b) = a\$b$

Пример 4. $x = abcde$

$\mathscr{A}(x) = x \neq \lambda$

1 Итерация:

$R : abcde \vdash \gamma abcde \models^5 abcde\gamma \vdash \bullet abcde\beta e$

$L : abcd\beta e \vdash \alpha abcd\beta e \vdash \bullet a\alpha bcd\beta e$

2 Итерация:

$R : a\alpha bcd\beta e \vdash \bullet a\alpha bc\beta de$

$L : a\alpha bc\beta de \vdash \bullet ab\alpha c\beta de$

3 Итерация:

$R : ab\alpha c\beta de \vdash \bullet ab\alpha\beta cde$

$L : ab\alpha\beta cde \vdash \bullet ab\alpha\beta cde$

$\mathscr{A}(ab\alpha\beta cde) = \lambda$

$\mathscr{B}(ab\alpha\beta cde) = ab\$cde$

1.6 Универсальный нормальный алгорифм.

Пусть дан НА:

$$\mathscr{A} : \begin{cases} u_1 \to [\bullet]v_1 \\ \vdots \\ u_n \to [\bullet]v_n \end{cases}$$

$$A^{\text{И}} \leftrightharpoons u_1\alpha[\beta]v_1\gamma u_2\alpha[\beta]v_2\gamma \dots \gamma u_n\alpha[\beta]v_n, \text{ где } \alpha, \beta, \gamma \notin V$$

Пусть

$$\mathscr{A}_0 : \begin{cases} \#a \to a\# \\ \#b \to b\# \\ \# \to \bullet aba \to \# \end{cases}$$

Отсюда

$$A_0^{\text{И}} = \#a\alpha a\#\gamma\#b\alpha b\#\gamma\#\alpha\beta aba\gamma\alpha\#$$

$$\text{Ɛ}A_0\text{З} = \underbrace{01110}_{\#}\underbrace{010}_{a}\underbrace{011110}_{\alpha}\underbrace{010}_{a}\underbrace{01110}_{\#}\underbrace{01111110}_{\gamma}$$

a	b	$\#$	α	β	γ
1	2	3	4	5	6

Теорема 1.7. *(Об универсальном НА). Пусть V - произвольный алфавит. Может быть построен НА U над алфавитом $V \cup V_0$ такой, что для любых НА $\mathcal{A}$ в алфавите V и слова $x \in V^*$ имеет место $U(\text{Ɛ}\mathcal{A}\text{З}\$x) \simeq \mathcal{A}(x)$, где $\$ \notin V \cup V_0$*

1.7 Разрешимые и перечислимые языки.

Определение 19. Язык $L \subseteq V^*$ называется алгоритмически разрешимым, если может быть построен НА $\mathscr{A}_L$ над алфавитом V такой, что

$$(\forall x \in V^*)(!\mathscr{A}_L) \text{ и } \mathscr{A}_L(x) = \lambda \Longleftrightarrow x \in L$$

Пример. Пусть $L = \{\omega\omega : \omega \in V^*\}$

$$x \longrightarrow \boxed{\mathscr{C}} \xrightarrow[\substack{x_1x_2 = x \\ ||x_1| - |x_2|| \leq 1}]{x_1\$x_2} \boxed{EQ} \longrightarrow \mathscr{A}_L(x) = \lambda \Longleftrightarrow x \in L$$

Также стоит заметить, что здесь $\mathscr{A}_L = \mathscr{C} + EQ$. Запись формальная и Белоусов может не понять, что здесь написано. А написано здесь то, что алгорифм $\mathscr{A}_L$ состоит из $\mathscr{C}$ и EQ.

$$\underbrace{\mathscr{C} \to EQ}_{\mathscr{A}_L}$$

Определение 20. НА $\widetilde{\mathscr{A}_L}$ называется полуразрешимым для языка $L \subseteq V^*$, если

$$!\widetilde{\mathscr{A}_L}(x) \Longleftrightarrow x \in L$$

Теорема 1.8. *Если для языка L невозможен полуразрешающий НА, то невозможен и разрешающий.*

Доказательство. От противного. Предполагаем, что для языка L невозможен полуразрешающий, то возможен разрешающий НА.

Пусть $\mathscr{A}_L$ - разрешающий НА для $L \subseteq V^*$

По теореме о разветвлении строим

$$\mathscr{B}_L = {}_{\mathscr{A}_L}(\mathscr{A}_L \vee Null),$$

где

$$Null : \Big\{ \to$$

Если $\mathscr{A}_L(x) = \lambda$, то есть $x \in L$, то $\mathscr{B}_L(x) = \mathscr{A}_L(x) = \lambda$.

Если $\mathscr{A}_L(x) \neq \lambda$, то есть $x \notin L$, отсюда $\neg!\mathscr{B}_L(x)$, так как $\neg!Null(x)$

Итак, $!\mathscr{B}_L(x) \Longleftrightarrow x \in L$, то есть $\mathscr{B}_L$ - полуразрешающий НА для L вопреки условию теоремы. □

Теорема 1.9. *Если язык L разрешим, то и разрешимо его дополнение.*

$$\mathscr{A}_L(x) = \lambda \Longleftrightarrow x \in L, \text{ то есть } \mathscr{A}_L \neq \lambda \Longleftrightarrow x \notin L \text{ при } (\forall x)!\mathscr{A}_L(x)$$

Для универсального языка:

$$L = V^* \quad \mathscr{A}_{V^*} : \begin{cases} \xi \to \ \ //\xi \in V \\ \to \cdot \end{cases}$$

Отсюда следует, что и пустой язык тоже разрешим, потому что он - дополнение универсального.

Определение 21. Конструктивное натуральное число (КНЧ) - это слово вида $0\underbrace{11\ldots1}_{n \geq 0}$. Ноль кодирует ноль, 01 кодирует 1 и так далее. КНЧ $x \in V_0^*$

$$0 \to 0; \quad 01 \to 1; \quad 011 \to 2; \quad \ldots$$

Определение 22. Конструктивное целое число (КЦЧ) - это слово вида $[-]n$, где n - КНЧ.

Определение 23. Конструктивное рациональное число (КРЧ): m/n, где m, n - КЦЧ, то есть слово в $\{0, 1, -, /\}$ и $n \neq 0$

Определение 24. Язык $L \subseteq V^*$ называется алгорифмически перечислимым, если может быть построен НА N_L такой, что для любого КНЧ n $!N_L(n)$ и $N_L(n) \in L$, и $(\forall x \in L)$ <u>осуществимо</u> КНЧ n такое, что $x = N_L(n)$

Определение 25. A, $\quad \nu : \mathbb{N}_0 \to A$ сюръективно, то есть $(\forall x \in A)(\exists n \in \mathbb{N}_0)(x = \nu(n))$. Это называется нумерацией множества A.

Далее будем предполагать, что отображение ν будет биективной.

Проведем нумерацию целых чисел:

Рис. 1.5:

Порядок чисел

Можно записать в виде формулы:

$$\gamma(n) = \begin{cases} -\frac{n}{2}, \text{ если } n \text{ четное} \\ \frac{n+1}{2}, \text{ если } n \text{ нечетное} \end{cases}$$

Сначала сделаем 3 алгорифма, нужных для следующей задачи (?)

$$\mathscr{C} : \begin{cases} 11 \to \\ 0 \to \cdot \end{cases}$$

Можем заметить, что $\mathscr{C}(n) = \lambda \iff n$ четное

$$N_L = {}_{\mathscr{C}}(\mathscr{A} \vee \mathscr{B})$$

Схема $\mathscr{A}$:

$$\mathscr{A} : \begin{cases} \alpha 11 \to 1\alpha \\ \alpha \to \cdot \\ 01 \to -0\alpha 1 \\ 0 \to \cdot 0 \end{cases}$$

Причем $\alpha \notin V_0$

Схема $\mathscr{B}$

$$\mathscr{B} : \begin{cases} \alpha 11 \to 1\alpha \\ \alpha \to \cdot \\ 01 \to 0\alpha 11 \\ \to \cdot \end{cases}$$

Нужно пронумеровать рациональные числа. Это по факту пары двух целых. Значит, учимся упорядочивать пары.

Рис. 1.6:

Предлагаемый Порядок рациональных чисел

Определение 26. Область применимости НА $\mathscr{A}$ относительно алфавита V: пусть $\mathscr{A} = (V' \supset V, S, P)$ - НА над V; Тогда область применимости НА относительно алфавита V есть множество $\mathscr{M}_{\mathscr{A}}^{V} \risingdotseq \{x : x \in V^* \text{ и } !\mathscr{A}(x)\}$, причем $\mathscr{A} : V^* \underset{\bullet}{\to} V^*$. $\mathscr{M}_{\mathscr{A}}^{V}$ и есть область применимости.

Теорема 1.10. *Язык $L \subseteq V^*$ перечислим тогда и только тогда, когда он является областью применимости относительно алфавита V некоторого НА.*

Следствие. Всякий разрешимый язык перечислим.

Доказательство. (следствия). Пусть L - разрешимый язык и $\mathscr{A}_L$ - разрешающий НА.

Строим такой НА $\mathscr{B}_L = Empty \circ \mathscr{A}_L$, где $Empty$ применим только к пустому слову.

$$Empty : \begin{cases} \xi \to \xi \ //\xi \in V \\ \to \cdot \end{cases}$$

Отсюда получаем

$$!\mathscr{B}_L(x) \Longleftrightarrow !\mathscr{A}_L(x) \text{ и } \mathscr{A}_L(x) = \lambda,$$

то есть $L = \mathscr{M}^V_{\mathscr{B}_L}$

Однако обратное неверно! □

1.8 Проблема применимости нормальных алгорифмов Маркова

Частная проблема применимости. Дан НА $\mathscr{A}$ в алфавите V. Можно ли построить НА $\mathscr{B}$ над алфавитом V такой, что $(\forall x \in V^*)!\mathscr{B}(x)$ и $\mathscr{B}(x) = \lambda \Longleftrightarrow \neg!\mathscr{A}(x)$. Алгорифм Б задуман для того, чтобы расширить область применимости алгорфима А.

Общая проблема применимости. Дан алфавит V, $\$ \notin V \cup V_0$. Можно ли построить НА $\mathscr{B}$ над алфавитом $V \cup V_0$ так, что для любых НА $\mathscr{A}$ в алфавите V и слова $x \in V^*$

$$!\mathscr{B}(\text{Ɛ}\mathscr{A}\text{З}\$x) \text{ и } \mathscr{B}(\text{Ɛ}\mathscr{A}\text{З}\$x) = \lambda \Longleftrightarrow \neg!\mathscr{A}(x)$$

1.8.1 Проблема самоприменимости.

Рассмотрим проблему самоприменимости. Мы хотим, чтобы алгорифм работал со своей собственной записью.

Соглашение. В дальнейшем, не оговаривая это особо, мы считаем, что алгорифм в алфавите V заменяем его в алфавит $V \cup V_0$

$$V \to V \cup V_0$$
$$V_1 = V \cup V_0 \cup \{\alpha, \beta\}; \alpha, \beta \notin V \cup V_0$$
$$\mathscr{A} : (V \cup V_0)^* \subset \cdot\!\!\to (V \cup V_0)^*$$
$$V_2 = V_0 \cup \{\alpha, \beta\}$$

Дан алфавит V. Можно ли построить НА $\mathscr{B}$ над алфавитом V_0 такой, что для любого НА $\mathscr{A}$ в $V \cup V_0$ будет верно

$$!\mathscr{B}(\text{Ɛ}\mathscr{A}\text{З}) \text{ и } \mathscr{B}(\text{Ɛ}\mathscr{A}\text{З}) = \lambda \Longleftrightarrow \neg!\mathscr{A}(\text{Ɛ}\mathscr{A}\text{З})$$

Примеры. Построим как самоприменимые, так и несамоприменимые НА.

$$\mathscr{A}_0 : \begin{cases} \#a \to a\# \\ \#b \to b\# \\ \# \to \cdot aba \\ \to \# \end{cases}$$

Дадим ему на вход свою же запись:

$$\mathscr{A}_0 : \text{Ɛ}\mathscr{A}_0\text{З} \vdash \#\text{Ɛ}\mathscr{A}_0\text{З} \vdash \cdot aba\text{Ɛ}\mathscr{A}_0\text{З}$$

Причем $V_0 \cap \{\#, a, b\} = \varnothing$. Этот алгорифм самоприменим.

$$\mathscr{A}_0^f : \begin{cases} 0 \to 0 \\ 1 \to 1 \\ \text{Схема } \mathscr{A}_0 \end{cases}$$

Дадим ему на вход свою же запись:

$$\mathscr{A}_0^f : \text{Ɛ}\mathscr{A}_0^f\text{З} \vdash \text{Ɛ}\mathscr{A}_0^f\text{З} \vdash \dots$$

То есть $\neg!\mathscr{A}_0^f(\text{Ɛ}\mathscr{A}_0^f\text{З})$

Лемма. Невозможен НА $\mathscr{B}$ в алфавите $V \cup V_0$ такой, что для любого НА $\mathscr{A}$ в алфавите $V \cup V_0$ имело бы место

$$!\mathscr{B}(\mathcal{E}\mathscr{A}\mathcal{3}) \iff \neg!\mathscr{A}(\mathcal{E}\mathscr{A}\mathcal{3})$$

Доказательство. Пусть алгорифм $\mathscr{B}$ построен. Тогда при $\mathscr{A} = \mathscr{B}$ имеем:

$$!\mathscr{B}(\mathcal{E}\mathscr{B}\mathcal{3}) \iff \neg!\mathscr{B}(\mathcal{E}\mathscr{B}\mathcal{3})$$

что является противоречием. То есть он применим тогда, когда не применим?) □

Теорема 1.11. *Невозможен НА $\mathscr{B}$ над алфавитом V_0 так, что для любого НА $\mathscr{A}$ в алфавите V_1 имело бы место*

$$!\mathscr{B}(\mathcal{E}\mathscr{A}\mathcal{3}) \iff \neg!\mathscr{A}(\mathcal{E}\mathscr{A}\mathcal{3})$$

Доказательство. По теореме о переводе может быть построен НА $\mathscr{B}_1$ в алфавите $V_0 \cup \{\alpha, \beta\}$ так, что $(\forall x \in V_0^*)\mathscr{B}_1(x) \simeq \mathscr{B}(x)$.

Строим НА $\mathscr{B}_2$ как естественное распространение НА $\mathscr{B}_1$ на алфавит V_1.

Пусть

$$!\mathscr{B}(\mathcal{E}\mathscr{A}\mathcal{3}) \iff \neg!\mathscr{A}(\mathcal{E}\mathscr{A}\mathcal{3}),$$

но тогда $!\mathscr{B}(\mathcal{E}\mathscr{A}\mathcal{3}) \iff !\mathscr{B}_1(\mathcal{E}\mathscr{A}\mathcal{3}) \iff !\mathscr{B}_2(\mathcal{E}\mathscr{A}\mathcal{3}) \iff \neg!\mathscr{A}(\mathcal{E}\mathscr{A}\mathcal{3})$, что невозможно в силу самой леммы. □

Итак, мы доказали невозможность полуразрешимость самоприменимости.
Проблема самоприменимости для алгорифмов алгорифмически неразрешима.

Теорема 1.12. *Язык записей несамоприменимых НА неперечислим.*

Доказательство. Пусть указанный язык $L = \{\mathcal{E}\mathscr{A}\mathcal{3} : \neg!\mathscr{A}(\mathcal{E}\mathscr{A}\mathcal{3})\}$ перечислим. Тогда L есть область применимости относительно алфавита V_0 некоторого НА $\mathscr{B}$, то есть

$$!\mathscr{B}(\mathcal{E}\mathscr{A}\mathcal{3}) \iff \neg!\mathscr{A}(\mathcal{E}\mathscr{A}\mathcal{3}),$$

что невозможно! □

Один вспомогательный НА. Нам нужен такой НА:

$$Double^{\$}(x) = x\$x, \quad x \in V^*, \quad \$ \notin V$$

Его схема:

$$Double^{\$} : \begin{cases} \alpha\xi \to \xi\beta\xi\alpha \\ \beta\xi\eta \to \eta\beta\xi \\ \alpha \to \$ \\ \beta\xi\$ \to \$\xi \\ \$ \to \bullet\$ \\ \to \alpha \end{cases}$$

причем $\alpha, \beta, \# \notin V; \quad \xi, \eta \in V$

Пример его работы. Несколько примеров.
① $\lambda \vdash \alpha \vdash \$ \vdash \bullet\$$
② $a \vdash \alpha a \vdash a\beta a\alpha \vdash a\beta a\$ \vdash a\$a \vdash \bullet a\$a$

$$\begin{aligned} &abc \vdash \\ &\quad \vdash \alpha abc \vdash a\beta a\alpha bc \vdash a\beta ab\beta b\alpha c \vdash \\ &\quad \vdash \ldots \vdash abc\$abc \\ &\quad \vdash \bullet abc\$abc \end{aligned}$$

Теорема 1.13. *Может быть построен НА $\mathscr{A}$ в алфавите V_2 так, что невозможен НА $\mathscr{B}$ над алфавитом V_2, для которого выполнялось бы*

$$!\mathscr{B}(y) \iff \neg!\mathscr{A}(y), y \in V_2^*$$

Доказательство. По теореме об универсальном НА построим НА U над алфавитом V_2 так, что для любых НА D в алфавите V_2 и слово $y \in V_2^*$ выполняется

$$U(\mathcal{E}D3\$y) \simeq D(y).$$

Определим НА U_1 так, что

$$(\forall y \in V_2^*)(U_1(y) \simeq U(y\$y)),$$

то есть $U_1 = U \circ Double^{\$}$.

Тонкий момент здесь! Алгорифм U_1 будучи НА над алфавитом V_2 тем самым является и НА над алфавитом V_0 (V_2 - расширение V_0). По теореме о переводе он может быть заменен вполне эквивалентным ему относительно алфавита V_0 НА U_2 в алфавите V_2 (то есть в двухбуквенном расширении V_0).

$$U_2(x) \simeq U_1(x), \text{ где } x \in V_0^*, U_2 \text{ - НА в } V_2 = V_0 \cup \{\alpha, \beta\}$$

Предположим, что такой НА $\mathcal{B}$ нашелся.

$$!\mathcal{B}(\mathcal{E}D3) \iff \neg!U_2(\mathcal{E}D3) \iff \neg!U_1(\mathcal{E}D3) \iff \neg!U(\mathcal{E}D3\$\mathcal{E}D3) \iff \neg!D(\mathcal{E}D3)$$

Он будет полуразразрешающим НА для несамоприменимых НА в языке V_2, что невозможно. □

Следствие. Может быть построен НА с неразрешимой частной проблемой применимости, следовательно его область применимости будет перечислимая, но неразрешимая (множество?).

Примеры неразрешимых проблем. Проблема соответствия Поста.
$\rho = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \subseteq V^{+^2}$
Существует ли

$$(x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \ldots, (x_{im}, y_{im}) : x_{i1}x_{i2}\ldots x_{im} = y_{i1}y_{i2}\ldots y_{im}?$$

1.9 Порождающие грамматики

Определение 27. $\mathcal{J} = (V, N, S \in N, \Phi), V \cap N = \varnothing$

Правило вывода: $\alpha \to \beta, \quad \to \notin V \cup N$
Левая часть $\alpha \in (V \cup N)^* N (V \cup N)^*$, N - детерминал.

Пусть $\gamma, \delta \in (V \cup N)^*$. Тогда

$$\gamma \underset{\mathcal{J}}{\vdash} \delta \leftrightharpoons \text{сущ правило вывода } \alpha \to \beta \text{ в системе } \Phi \text{ и } \gamma = \gamma_1\alpha\gamma_2, \delta = \gamma_1\beta\gamma_2$$

Определение 28. Вывод в порождающей грамматике $\mathcal{J}$ - это последовательность $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots$, где $(\forall i \geq 0)(\alpha_i \in (V \cup N)^*)$ и $(\forall i \geq 0)(\alpha_i \underset{\mathcal{J}}{\vdash} \alpha_{i+1})$, если α_{i+1} определен в последовательности.

Определение 29. $\gamma \vdash^*_{\mathcal{J}} \delta \leftrightharpoons$ существует вывод
$\gamma = \alpha_0 \vdash \alpha_1 \vdash \ldots \vdash \alpha_n = \delta, n \geq 0$ - длина вывода (к-рая конечна).

Определение 30. $L(\mathcal{J}) \leftrightharpoons \{x : x \in V^*, S \vdash^*_{\mathcal{J}} x\}$

Примеры грамматик.

1) $S \to aSb \big| \lambda$

   $S \vdash aSb \vdash aaSbb \vdash \ldots \vdash a^n S b^n \vdash a^n b^n$

   $\mathcal{J}_1 = (\{a, b\}, \{S\}, S, \Phi_1)$

   Тогда язык, порожденный такой грамматикой
   $L(\mathcal{J}_1) = \{a^n b^n : n \geq 0\}$

2) $\Phi_2 : S \to aSa \big| bSb \big| aa \big| bb \big| a \big| b \big| \lambda$

   $S \vdash aSa \vdash aba$

   $S \vdash aSa \vdash abSba \vdash abbSbba \vdash abbbba$

   $L(\mathcal{J}_2) = \{x : x = x^R, x \in \{a, b\}^*\}$ - палиндром

3) $S \to ()\big|(S)\big|SS$ - правильная скобочная структура

4) $\mathcal{J}_4 = (\{a,b\}, \{S,A,B,C,D\}, S, \Phi_4)$

$$\Phi_4 : \begin{cases} S \to CD \\ c \to aCA\big|bcD\big|\lambda \\ AD \to aD \\ BD \to bD \\ Aa \to aA \\ Ab \to bA \\ Ba \to aB \\ Bb \to bB \\ D \to \end{cases}$$

$S \vdash CD \vdash \lambda D \vdash \lambda\lambda = \lambda$

$S \vdash CD \vdash aCAD \vdash abcBAD \vdash abbCBBAD \vdash abbBBAD \vdash$
$\vdash abbBBaD \vdash abbBaBD \vdash abbaBBD \vdash abbaBbD \vdash abbabBD \vdash$
$\vdash abbabbD \vdash abbabb$

$L(\mathcal{J}_4) \supseteq \{\omega\omega : \omega \in \{a,b\}^*\}$. Можно доказать, что такой язык будет состоять только из двойных слов.

$L(\mathcal{J}_4) = \{\omega\omega : \omega \in \{a,b\}^*\}$

1.10 Классификации грамматик

1) Грамматики типа 0
2) Неукорачивающие грамматики (НК-)
3) Контекстно зависимые грамматики (КЗ-)
4) ОКЗ-грамматики (ограниченно КЗ)
5) Контекстно свободные (КС-)
6) Линейные грамматики
7) Праволинейные грамматики
8) Леволинейные грамматики
9) Регулярные (автоматные) грамматики

Определение 31. Грамматики называются эквивалентными, если они порождают один и тот же язык

$$G_1 \simeq G_2 \leftrightharpoons L(G_1) = L(G_2)$$

Определение 32. Грамматики называют почти эквивалентными, если порождаемые ими языки совпадают с точностью до пустого слова, то есть

$$G_1 \approx G_2 \leftrightharpoons L(G_1) \nabla L(G_2) \subseteq \{\lambda\}$$

Теорема 1.14.
1) Для каждой грамматики типа 0 может быть построена эквивалентная ей ОКЗ-грамматика

2) Для каждой неукорачивающей грамматики может быть построена эквивалентная ей КЗ-грамматика

3) Для каждой КС-грамматики может быть построена почти эквивалентная ей КС-грамматика, не содержащая правил с пустой правой частью (т.н. лямбда-правил)

4) Для каждой леволинейной грамматики может быть построена эквивалентная ей праволинейная грамматика и наоборот.

5) Для каждой праволинейной грамматики может быть построена жквивалентная ей регулярная грамматика

Теорема 1.15. *Язык перечислим тогда и только тогда, когда он порождается грамматикой типа 0.*

Всякий КС-язык разрешим, но обратное неверно.

1.11 МП-автоматы (Pushdown machine)

рис1

$qaZ \to r\gamma$, где $q, r \in Q$, $Z \in \Gamma, \gamma \in \Gamma^*$, $a \in V \cup \{\lambda\}$

рис2

Пример

$$\begin{aligned}
&q_0 aZ \to q_0\ aZ\\
&q_0 aa \to q_0\ aa\\
&q_0 ba \to q_1 \lambda\\
&q_1 ba \to q_1 \lambda\\
&q_1 \lambda Z \to q_2 \lambda
\end{aligned}$$

Машинный автомат может быть описан тоже в виде конфигураций. Начальное:

$$(q, ay, Z\alpha) \quad \alpha \in \Gamma^*, \text{ то есть может быть пустой}$$

Z - все, что есть в магазине.

$$(q_0, aabb, Z) \vdash (q_0, abb, aZ) \vdash (q_0, bb, aaZ) \vdash (q_1, b, aZ) \vdash (q_1, \lambda, Z) \vdash (q_1, \lambda, \lambda)$$

Определение 33. $\mathscr{M} = (Q, V, \Gamma, q_0, F, Z_0(\text{нач. маг. симв.}), \delta(\text{сист. перех.}))$ - магазинный автомат

Определение 34. Конфигурация МП-авт: $(Q, ay, Z\alpha)$, где $q \in Q$, $a \in V \cup \{\lambda\}$, $y \in V^*$, $z \in \Gamma, \alpha \in \Gamma^*$

$$(q, ay, Z\alpha) \underset{\mathscr{M}}{\vdash} (r, y, \gamma\alpha) \leftrightharpoons qaZ \to r\gamma$$

Далее отношение непосредственной выводимости на мн-стве конфигурации рефлексивно-транзитивно замыкается подобно тому, как это было сделано на конфигурации машины Тьюринга.

Определение 35. Язык, допускаемый магазинным автоматом, - это

$$L(\mathscr{M}) \leftrightharpoons \{x : (q_0, x, Z_0)\} \vdash^* (q_f, \lambda, \alpha),$$

где $q_f \in F$.

Мы можем немного переопределить наш язык так:

$$L(\mathscr{M}) = \{x : (q_0, x, Z_0) \vdash^* (q_f, \lambda, \lambda); x \in V^*\}$$

Теорема 1.16. *Язык является контекстно свободным тогда и только тогда, когда он допускается некоторым МП-автоматом.*

Дано: КС-грамматика $\mathcal{J} = (V, N, S, \mathscr{P})$

Строим: МП-автомат $\mathcal{M} = (Q, V, \Gamma, q_0, F, z_0, \delta)$

$\boxed{\text{L(M) = L(J)}}$

$\mathcal{M} = (\{q\}, V, V \cup N, q, \{q\}, S, \delta_{\mathscr{P}})$

Причем $q\lambda A \to q\alpha \in \delta_{\mathscr{P}} \leftrightharpoons A \to \alpha \in \mathscr{P}$

$(\forall a \in V)(qaa \to q\lambda \in \delta_{\mathscr{P}})$

Пример 1.

$\mathcal{J}: \quad S \to aSa \big| bSb \big| aa \big| bb \big| a \big| b \big|$
То есть $L(\mathcal{J}) = \{x : x = x^R, x \neq \lambda\}$
То есть система комманд такая:

$$\delta_{\mathscr{P}} : \begin{cases} q \to qaSa \big| qbSb \big| qaa \big| qbb \big| qa \big| qb \\ qaa \to q\lambda \\ qbb \to q\lambda \end{cases}$$

$\mathcal{J} : S \vdash aSa \vdash abSba \vdash ababa$
Для автомата:
$(q, ababa, S) \vdash (q, ababa, aSa) \vdash (q, baba, Sa) \vdash (q, baba, bSba) \vdash (q, aba, Sba) \vdash (q, aba, aba) \models^3 (q, \lambda, \lambda)$ - допуск

Пример 2.

$S \to ab \big| aSb \big| SS$

$$\delta : \begin{cases} qaS \to qb \big| qsb \\ q\lambda S \to qSS \\ qaa \to q\lambda \\ qbb \to q\lambda \end{cases}$$

$S \vdash SS \vdash aSbS \vdash aabbS \vdash aabbab$
Как автомат ее разберет:
$(q, aabbab, S) \vdash (q, aabbab, SS) \vdash (q, abbab, SbS) \vdash (q, bbab, bbS) \models^2 (q, ab, S) \vdash (q, b, b) \vdash (q, \lambda, \lambda)$ - допуск

Булевы функции

2.1 Булева алгебра

Свойства симметричного полукольца:

- a + (b + c) = (a + b) + c
- a + b = b + a
- a + a = a
- a + 0 = a
- a * (b * c) = (a * b) * c
- a * 1 = 1 * a =a
- a*(b+c) = ab + ac
- a*0=0*b=0
- ab = ba
- aa = a
- a + 1 = 1
- a + bc = (a + b)(a + c)

  Симметричное полукольцо: $\mathscr{S} = (S, +, \cdot, 0, 1)$
  Симметричное ему полукольцо: $\mathscr{S}^* = (S, \cdot, +, 1, 0)$
  $(\forall a)(a^* = 1)$

Принцип двойственности симметрического полукольца. Любое тождество, доказанное для симметрического полукольца, останется справедливым, если в нем произвести взаимные замены операции сложения и умножения, а также взаимные замены нуля и единицы.

Пример.

$$(a + b)(a + c) = a^2 + ac + ab + bc = a + ac + ab + bc = a\underbrace{(1 + c + b)}_{1} + bc = a + bc$$

Свойство 1. $a + ab = a(a + b) = a$

Доказательство. $a(a + b) = a^2 + ab = a + ab = a(1 + b) = a * 1 = a$ □

Свойство 2. $a \leq b \Longleftrightarrow ab = a$

Доказательство.
$a \leq b \implies a + b = b \implies ab = a(a + b) = a$
$ab = a \implies a + b = ab + b = ab + 1 * b = (a + 1)b = 1 * b = b$ □

Свойство 3. $(\forall a)(a \leq 1)$, то есть $(\forall a)(0 \leq a \leq 1)$

Определение 36. Дополнение элемента a: $\overline{a} * a = 0$ и $\overline{a} + a = 1$

Теорема 2.1. *Если дополнение элемента симметрического полукольца определено, то оно определено однозначно.*

Доказательство. Пусть $(\exists x)(a + x = 1, ax = 0)$

Тогда

$$x = x + a * \overline{a} = (x + a)(x + \overline{a}) = 1(x + \overline{a}) = (a + \overline{a})(x + \overline{a}) = ax + \overline{a} = 0 + \overline{a} = \overline{a}$$

□

Следствие. $\overline{\overline{a}} = a$

Определение 37. Булева алгебра - это симметричное полукольцо, в котором каждый элемент имеет дополнение.

Примеры.

$\mathcal{B} = (\{0, 1\}, +, *, 0, 1)$
$\mathcal{S}_M = (2^M, \cup, \cap, \varnothing, M)$

Булева алгебра обозначается так:

$$\mathscr{D} = (B, \vee, \wedge, \Theta, I, \overline{})$$

Теорема 2.2. *В любой булевой алгебре имеет место:*

$$\overline{a \vee b} = \overline{a} \wedge \overline{b}; \quad \overline{a \wedge b} = \overline{a} \vee \overline{b}$$

Доказательство.

$$(a \vee b) \vee (\overline{a} \wedge \overline{b}) = (a \vee b \vee \overline{a}) \wedge (a \vee b \vee \overline{b}) = I$$

$$(a \vee b) \wedge (\overline{a} \wedge \overline{b}) = (\overline{a} \wedge \overline{b} \wedge a) \vee (\overline{a} \wedge \overline{b} \wedge b) = \Theta \vee \Theta = \Theta$$

Отсюда $\overline{a \vee b} = \overline{a} \vee \overline{b}$ □

Пусть дана булева алгебра $\mathscr{B} = (B, \vee, \wedge, \Theta, I, \overline{})$
$\mathscr{B}^n = (B^n, \vee, \wedge, \widetilde{\Theta}, \widetilde{I})$
Тогда пусть $\widetilde{\alpha}, \widetilde{\beta} \in \mathscr{B}^n$; $\alpha = (\alpha_1, \ldots, \alpha_n)$
$\beta = (\beta_1, \ldots, \beta_n)$
Отсюда

$$\widetilde{\alpha} \vee \widetilde{\beta} \risingdotseq (\alpha_1 \vee \beta_1, \ldots, \alpha_n \vee \beta_n)$$

Аналогично и для $\widetilde{\alpha} \wedge \widetilde{\beta}$.

Также $\widetilde{\Theta} = (\Theta, \ldots, \Theta)$ и $\widetilde{I} = (I, \ldots, I)$

Определение 38. Булев куб размерности n: $\mathcal{B}^n = (\{0, 1\}^n, \vee, \wedge, \widetilde{0}, \widetilde{1})$

Рассмотрим всевозможные отображения X в носитель булевой алгебры

$$f : X \to B$$

Тогда можно сказать такое:

1) $(f \vee g)(x) \risingdotseq f(x) \vee g(x)$

2) $(f \wedge g)(x) \risingdotseq f(x) \wedge g(x)$

3) $\overline{f}(x) \risingdotseq \overline{f(x)}$

- (4) $\sigma(x) \risingdotseq \Theta \quad (\forall x)$

5) $\xi(x) = I(\forall x)$

Определение 39. Так обозначается булева алгебра функций:

$$\mathscr{B}^X = (B^X, \vee, \wedge, \sigma, \xi)$$

Булево кольцо, соответствующее булевой алгебре $\mathscr{B}$

$$\mathscr{R}_B = (B, \oplus, \cdot, \Theta, I)$$

Отсюда

$$a \oplus b \leftrightharpoons a\overline{b} \vee \overline{a}b$$
$$a \cdot b \leftrightharpoons a \wedge b$$

$\mathscr{S}_M = (2^M, \cup, \cap, \varnothing, M)$
$\mathscr{R}_M = (2^M, \triangle, \cap, \varnothing, M)$

2.2 Булевые функции. Основные понятия

Определение 40. Булева функция от n переменных:

$$f : \{0,1\}^n \to \{0,1\}$$

Булева переменная - это $x_1, x_2, \ldots, x_n$. Функция выглядит обычно: $y = f(x_1, \ldots, x_n)$

Множество всех булевых функций:

$$\mathscr{P}_2 = \mathscr{P}_2^{(0)} \cup \mathscr{P}_2^{(1)} \cup \ldots \cup \mathscr{P}_2^{(n)} \cup \ldots$$

Нам известно определение н-арной операции: $\omega : A^n \to A$. То есть булевы функции своего рода н-арные операции.

	f_1	f_2	f_3	f_4
0	0	1	0	1
1	0	1	1	0

Можно заметить, что $\overline{x} = x \oplus 1 = x \sim 0$

$h = (0011111010101110) \iff h = \{2, 3, 4, 5, 6, 8, 10, 12, 13, 14\}$

2.3 Равенство булевых функций. Фиктивные переменные

Определение 41. Пусть есть $f, g : \{0,1\}^n \to \{0,1\}$. Тогда функции равны, если

$$f = g \leftrightharpoons (\forall \widetilde{\alpha} \in \{0,1\}^n)(f(\widetilde{\alpha}) = g(\widetilde{\alpha}))$$

$f(x_1, x_2) = x_1 \vee x_2$
$g(x_1, x_2, x_3) = x_1x_3 \vee x_1\overline{x_3} \vee x_2x_3 \vee x_2\overline{x_3} = x_1(x_2 \vee \overline{x_3}) \vee x_2(x_3 \vee \overline{x_3}) = x_1 \vee x_2$

Определение 42. Булевы функции считаются равными, если они отличаются друг от друга, может быть, только фиктивными переменными.

Можно переформулировать так предыдущее определение.

Определение 43. Булевы функции равны, если они существенно зависят от одних и тех же переменных и на каждом наборе значений этих переменных принимают одинаковые значения

Пусть дан набор значений $X = \{x_1, \ldots, x_n\}$. Тогда селектор $pr_i(x_1, \ldots, x_i, \ldots, x_n) = x_n$ и иногда называется i-селектором.

Так можно добавит фиктивные переменные:

$$y = f(x_1, \ldots, x_n) \quad \widetilde{y} = (x_{n+1} \vee \overline{x_{n+1}})f(x_1, \ldots, x_n) = y$$

2.4 Суперпозиции и формулы

Определение 44. Пусть у нас есть $f \in \mathscr{P}_2^{(n)}, \quad g_1, \dots, g_n \in \mathscr{P}_2^{(m)}$

$$f(g_1, \dots, g_n)(\widetilde{\alpha}) = f(g_1(\widetilde{\alpha}), \dots, g_n(\widetilde{\alpha})), \quad \widetilde{\alpha} \in \{0,1\}^m$$

и это называется суперпозицией.

2.5 Дизъюнктивная и конъюнктивная нормальные формы (ДНФ и КНФ)

Определение 45. Литерал - это формула, в которой есть либо переменная, либо отрицание переменной.

$$x^\sigma \leftrightharpoons \begin{cases} x_i, \text{ если } \sigma = 1 \\ \overline{x_i}, \text{ если } \sigma = 0 \end{cases}$$

Обозначение $\widetilde{x_i}$ - это возможное отрицание.

Определение 46. Элементарная конъюнкция - это конъюнкция каких-то литералов.

$$\widetilde{x_{i_1}}\widetilde{x_{i_2}} \dots \widetilde{x_{ik}}$$

Определение 47. ДНФ - это $k_1 \vee k_2 \vee \dots \vee k_m$ от $x_1, x_2, \dots, x_3$, где k_i - элементарная конъюнкция.

Определение 48. В СДНФ в каждую элементарную конъюнкцию входит каждый из $x_1, x_2, \dots, x_n$ либо сам, либо как отрицание.

ДНФ: $\{x_1, x_2, x_3\}: \quad \overline{x_1}x_2 \vee x_2 \vee x_1\overline{x_2x_3}$
СДНФ: $\{x_1, x_2, x_3\}: \quad x_1x_2x_3 \vee x_1\overline{x_2}x_3 \vee \overline{x_1}x_2x_3$

Определение 49. Элементарная дизъюнкция - это дизъюнкция каких-то литералов.

Определение 50. КНФ от $x_1, x_2, \dots, x_n$: $D_1 * D_2 * \dots * D_m, m \geq 1$

Определение 51. В СКНФ в каждую элементарную дизъюнкцию входит каждый из $x_1, x_2, \dots, x_n$ либо сам, либо как отрицание.

Теорема 2.3. *Любая функция, отличная от константы 0, может быть представлена в виде ДНФ. Любая функция, отличная от константы 1, может быть представлена в виде КНФ.*

Доказательство. 1) Так как $f \not\equiv 0$, то $\exists \widetilde{\alpha} \in \{0,1\}^n : f(\widetilde{\alpha}) = 1$ - называется это конституента 1 функции f.
Тогда

$$C_f^1 \leftrightharpoons \{\widetilde{\alpha} : f(\widetilde{\alpha}) = 1\} \neq \varnothing, \widetilde{\alpha} = (\alpha_1, \dots, \alpha_n).$$

$K_{\widetilde{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$
Заметим, что

$$K_{\widetilde{\alpha}}(\widetilde{\beta}) = 1 \Longleftrightarrow \widetilde{\beta} = \widetilde{\alpha}$$

Отсюда получаем:

$$\boxed{f(x_1, \dots, x_n) = \bigvee_{\mathcal{Z} \in C_f^1} K_{\widetilde{\alpha}}}$$

Заметим, что если

$$f(x_1, \dots, x_m) = 1 \implies (\exists \widetilde{\alpha} \in C_f^1)(f(\widetilde{\alpha}) = 1) \implies k_{\widetilde{\alpha}} = 1 \implies \bigvee_{\mathcal{Z} \in C_f^1} k_{\widetilde{\alpha}} = 1,$$

то есть $f(\widetilde{\alpha}) = 1$. Аналогично для КНФ. □

Следствие. Любая булевая функция может быть представлена некоторой формулой над стандартным базисом. То есть стандартным базисом является полным множеством булевых функций.

2.6 Полином Жегалкина

$\mathcal{F}_1 = \{\oplus, *, 1\}$

Отсюда $\overline{x} = x \oplus 1$ и $x_1 \vee x_2 = x_1x_2 \oplus x_1 \oplus x_2$.

Определение 52. Полиномом Жегалкина является

$$P(x_1, x_2, \dots, x_n) = \sum (mod2) a_{i_1 i_2 \dots i_k} x_{i_1} x_{i_2} \dots x_{ik}, \quad \{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}.$$

Здесь 2^n слагаемых. $a_{i_1 i_2 \dots i_k} \in \{0, 1\}$

Общий вид полинома Жегалкина от двух переменных:

$$P(x_1, x_2) = a_{12}x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0$$

Общий вид от трех:

$$P(x_1, x_2, x_3) = a_{123}x_1x_2x_3 \oplus a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus a_{23}x_2x_3 \oplus a_1x_1 \oplus x_2x_2 \oplus a_3x_3 \oplus a_0$$

Теорема 2.4. *Каждая булева функция однозначно представима в виде полинома Жегалкина.*

Метод неопределенных коэффициентов.

$f = (00010111)$
$f(0,0,0) = a_0 = 0$
$f(1,0,0) = a_1 \oplus a_0 = 0 \implies a_1 = 0$
$f(0,1,0) = a_2 \oplus a_0 = 0 \implies a_2 = 0$
$f(0,0,1) = a_3 \oplus a_0 = 0 \implies a_3 = 0$
$f(1,1,0) = a_{12} \oplus a_2 \oplus a_1 \oplus a_0 = 1 \implies a_{12} = 1$
$f(1,0,1) = a_{13} \oplus a_1 \oplus a_3 \oplus a_0 \implies a_{13} = 1$
$f(0,1,1) = a_{23} \oplus a_2 \oplus a_3 \oplus 3 \implies a_{23} = 1$
$f(1,1,1) = a_{123} \oplus a_{12} \oplus a_{13} \oplus a_{23} \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_0 = 1 \implies a_{123} \oplus 1 = 1 \implies a_{123} = 0$

Определение 53. Булева функция называется линейной, если она может быть представлена полиномом Жегалкина первой степени.

$$f \in L \leftrightharpoons f(x_1, \dots, x_n) = \sum_{i=1}^{n} (mod2) a_i x_i \oplus a_0$$

2.7 Классы Поста

Всего 5 классов.

1) $\mathcal{T}_0 \leftrightharpoons \{f : f(0, \dots, 0) = 0\}$
2) $\mathcal{T}_1 \leftrightharpoons \{f : f(1, \dots, 1) = 1\}$
3) $\mathcal{S} \leftrightharpoons \{f : (\forall \widetilde{\alpha})(f(\overline{\widetilde{\alpha}}) = \overline{f(\widetilde{\alpha})})\}$
   $f \notin S \iff (\exists \widetilde{\alpha})(f(\widetilde{\alpha}) = f(\overline{\widetilde{\alpha}}))$
   $f, \quad f^*(\widetilde{\alpha}) = \overline{f(\overline{\widetilde{\alpha}})} \iff \overline{f^*(\widetilde{\alpha})} = f(\overline{\widetilde{\alpha}})$
4) $\mathcal{M} \leftrightharpoons \{f : (\forall \widetilde{\alpha}, \widetilde{\beta})(\widetilde{\alpha} \le \widetilde{\beta} \implies f(\widetilde{\alpha}) \le f(\widetilde{\beta}))$
   $\widetilde{\alpha} = (\alpha_1, \dots, \alpha_n) \le \widetilde{\beta} = (\beta_1, \dots, \beta_n) \iff (\forall i = \overline{1, n})(\alpha_i \le \beta_i)$
   $\overline{\mathcal{T}_0} \cap \overline{\mathcal{T}_1} \subseteq \overline{\mathcal{M}}$
5) $\mathcal{L} \leftrightharpoons \{f : f = \sum_{i=1}^{n} (mod2) a_i x_i \oplus a_0\}$
   $x_1 \sim x_2 = x_1 \oplus x_2 \oplus a_0 \in \mathcal{L}$

Есть функции, которые принадлежат всем классам Поста, и есть такие, которые не принадлежат никакому.

Лемма 1 (О несамодвойственной функции). Пусть $f_S \notin \mathcal{S}$. Тогда обе константы (0 и 1) представимы формулами над множеством $\{f_S, \overline{}\}$

Доказательство. Так как $f_S \notin \mathcal{S}$, то $(\exists\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n))(f(\widetilde{\alpha}) = f(\overline{\widetilde{\alpha}}))$

Определим

$$h(x) \leftrightharpoons f_S(x^{\alpha_1}, \ldots, x^{\alpha_n}); \quad h(x) = const \in \{0, 1\}.$$

Подставим 1 или 0:

$$h(0) = f_S(0^{\alpha_1}, \ldots, 0^{\alpha_n}) = f_S(\overline{\widetilde{\alpha}})$$
$$h(1) = f_S(1^{\alpha_1}, \ldots, 1^{\alpha_n}) = f_S(\widetilde{\alpha})$$

То есть

$$h(0) = h(1) = f_S(\widetilde{\alpha}) = f(\overline{\widetilde{\alpha}}) \in \{0, 1\}.$$

Представим ее как отрицание: $\overline{h(x)} \in \{0, 1\}$ - и получим вторую константу. □

Лемма 2 (О немонотонной функции). Если функция $f_M \notin \mathcal{M}$, то существует два набора (вектора) $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$ и $\widetilde{\beta} = (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$, и $f(\widetilde{\alpha}) = 1, f(\widetilde{\beta}) = 0$

Рассмотрим такую функцию: $f_M = (1000\ 0011\ 1111\ 1100) \in \overline{\mathcal{T}_0} \cap \overline{\mathcal{T}_1} \implies f_M \notin \mathcal{M}$

Лемма 3 (О немонотонной функции). Отрицание может быть представлено формулой над множеством $\{f_M, 0, 1\}$, где $f_M \notin M$

Доказательство. В силу леммы 2 берем два набора $\widetilde{\alpha}$ и $\widetilde{\beta}$. Тогда очевидно отрицание представимо формулой

$$\overline{x} = f_M(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_{i+1}, \ldots, \alpha_n)$$

$f_M(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) = 1$ и 0 иначе. □

Лемма 4 (О нелинейной функции). Пусть $f_L \notin \mathcal{L}$. Тогда конъюнкция может быть представлена формулой над множеством $\{f_L, 0, \overline{}\}$

Доказательство. Поскольку f_L нелинейная функция, в ее полиноме Жегалкина обязательно будет нелинейное слагаемое. Среди всех нелинейных слагаемых функции f_L выбираем самое короткое. Пусть это самое короткое слагаемое будет $x_{i1}, x_{i2}, \ldots, x_{ik}$. $(k \geq 2)$

Строим новую функцию

$$f'_L = f_L\Bigg|_{x_j = 0 \text{ при } j \neq \{i_1, i_2, \ldots, i_k\}} = x_{i1}x_{i2}\ldots x_{ik} \oplus a_{i1}x_{i1} \oplus a_{i2}x_{i2} \oplus \ldots \oplus a_{ik}x_{ik} \oplus a_0$$

Произвольно делим переменные на две части. Мы строим функцию от двух переменных. Первая часть переменных есть x, вторая - y.

$$\chi(x, y) = f'_L\Bigg|_{\substack{x_{i1} = \ldots = x_{i_s} = x \\ x_{i_{s+1}} = \ldots = x_{i_k} = y \\ 1 \leq s < k}} = xy \oplus ax \oplus by \oplus c,$$

где $a = \sum\limits_{j=1}^{s}(mod2)a_{ik}, \quad b = \sum\limits_{l=s+1}^{k}(mod2)a_{il}, \quad c = a_0$

Утверждается, что конъюнкция $xy = \chi(x \oplus b, y \oplus a) \oplus ab \oplus c$.

Посмотрим:

$$(x \oplus b)(y \oplus a) \oplus a(x \oplus b) \oplus b(y \oplus a) \oplus c \oplus ab \oplus c =$$
$$xy \oplus ax \oplus by \oplus ab \oplus ax \oplus ab \oplus by \oplus ab \oplus c \oplus ab \oplus c = xy$$

Что и требовалось доказать.

□

Теорема 2.5. *Каждый класс Поста замкнут.*

2.8 Теорема поста

Теорема 2.6. *Множество булевых функций полно тогда и только тогда, когда оно не содержится (целиком) ни в одном из классов Поста.*

Доказательство. Необходимость. Полагая, что множество булевых функций содержится в каком-то классе Поста, получим, в силу замкнутости каждого класса Поста, что формулами над этим множеством могут быть представлены только функции этого класса, а, стало быть, не может быть представлена ни одна функция, не содержащаяся ни в одном из классов Поста, например, штрих Шеффера. Значит, такое множество не может быть полным.

Достаточность. Достаточно показать, что формулами над множеством $\mathcal{F}$, удовлетворяющем условию теоремы, могут быть представлены функции какого-то уже известного полного множества. В качестве такого множества можно взять такое, состоящее из конъюнкции и дизъюнкции.

Так как множество $\{*, \overline{}\}$ является полным, достаточно указать способ построения формул для конъюнкции и отрицания над базисом $\mathcal{F}$, который удовлетворяет условию теоремы Поста, то есть не содержится ни в одном из классов Поста, что можно выразить следующим образом:

$$(\forall C \in \{T_0, T_1, S, M, L\})(\exists f_c \in F \setminus C)$$

1 случай) Представим константу 1:

$$1 = f_0(x, \ldots, x),$$

а константу 0 представим с использованием какой-нибудь функции $g_1 \in F \setminus T_1$:

$$0 = g(1, \ldots, 1) = g(f(x, \ldots, x), \ldots, f(x, \ldots, x))$$

Имея формулы для обеих констант, отрицание представим формулой, используя немонотонную функцию.

2 случай) Всякая функция $f_0 \in F \setminus T_0$ не сохраняет и константу 1, а всякая функция $f_1 \in F \setminus T_1$ не сохраняет и константу 0. В этом случае сразу получаем формулу для отрицания.

$$\overline{x} = f_0(x, \ldots, x)$$

Тут используется лемма о несамодвойственной функции. $\square$

Элементы математической логики

3.1 Предпосылки возникновения математической логики

Пример Гиберта.

$Y = \{x : |x| \geq 3\}$ x - множество

То есть возьмем такие примеры и получим:

$$\{1,2,3\} \in Y, \{1,2,3,4\} \in Y, \{1,2,3,4,5\} \in Y \implies Y \in Y$$

Определение 54. Нормальные множества - это такие множества, которые не содержат самих себя.

Пусть мы хотим найти все Нормальные множества: $Z = \{x : x \notin x\} \quad Z \notin Z \implies Z \in Z \implies Z \notin Z$.
Это называется парадокс Рассела.

3.2 Понятие формальной аксиоматической теории

Определение 55. $\mathcal{T} = (\underbrace{V}_{\text{алфавит}}, \underbrace{\mathcal{F}}_{\text{формулы}}, \underbrace{\mathcal{A} \subseteq \mathcal{F}}_{\text{Мн. аксиом}}, \underbrace{\mathcal{P}}_{\text{Мн. правил вывода}})$ называется теорией.

Определение 56. Фиксируется некоторое множество $\Gamma \subseteq \mathcal{F}$ - гипотеза. Среди гипотез нет ни одной аксиомы: $\Gamma \cap \mathcal{A} = \varnothing$.

Определение 57. Вывод теории $\mathcal{T}$ из множества гипотез Γ - это последовательность формул (конечная или бесконечная): $\theta_0, \theta_1, \dots, \theta_n, \dots, \quad n \geq 0$, где для каждого $\forall i \geq 0 : 1)$ $\theta_i \in \Gamma$, 2) $\theta_i \in \mathcal{A}$, 3) существует правило вывода в $\mathcal{P} : \frac{\theta_{j1} \dots \theta_{jm}}{\theta_i}$, где $j_1, \dots, j_m < j$.

Если $\Phi = \theta_i$, то $\Gamma \vdash_{\mathcal{T}} \Phi$. Если $\Gamma = \varnothing$, то пишем $\vdash_{\mathcal{T}} \Phi$.

Теорема 3.1. *Если формула Φ выводима из гипотезы ($\Gamma \vdash_{\mathcal{T}} \Phi$), то для любого $\Gamma' \supset \Gamma$ верно $\Gamma' \vdash_{\mathcal{T}} \Phi$.*

Следствие. Если $\vdash_{\mathcal{T}} \Phi$, то для любого $\Gamma : \Gamma \vdash_{\mathcal{T}} \Phi$.

3.3 Алгебра высказываний. Тавтологии

У нас есть высказывания $p, q, r, \dots$ и они могут принимать значения Ложь (Л) или Истина (И). Указываются по-русски, однако для упрощения разметки буду использовать F, T (False, True).

p	q	$\vee$	$\&$	$\to$	$\oplus$
F	F	F	F	T	F
F	T	T	F	T	T
T	F	T	F	F	T
T	T	T	T	T	F

Функции также аналогичны тем, что описаны в математической логике:

$$G : \{F, T\}^n \to \{F, T\}$$
$$f : \{0, 1\}^n \to \{0, 1\}$$

Определение 58. Тавтология - это то, что говорит само за себя

3.4 Исчисление высказываний

Мы строим ее на основе Теории L.

Определение 59. Теория $L = (V_L, \mathcal{F}_L, \mathcal{A}_L, \mathcal{P}_L)$. Причем $V_L = Var \cup \{\neg, \to\} \cup Aux$, $\quad \mathcal{F}_L$: 1) Каждая переменная есть формула, 2) Если Φ - формула, то $(\neg\Phi)$ - формула, 3) если Φ и Ψ - формулы, то $(\Phi \to \Psi)$ - формула, 4) Никаких других формул нет.

Наше "подсахаривание"формул: 1) $\Phi \vee \Psi = \neg\Phi \to \Psi$, 2) $\Phi \& \Psi = \neg(\Phi \to \neg\Psi)$

Схем аксиом всего три:

$$\mathcal{A}_L : \begin{array}{cc} (1) & A \to (B \to A) \\ (2) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\ (3) & (\neg B \to \neg A) \to ((\neg B \to A) \to B) \end{array}$$

И наши правила вывода:

$$\mathcal{P}_L : \frac{A, A \to B}{B} \quad \textit{modus ponens } (MP)$$

Пример Тавтологии.

$\vdash (A \to A)$

Доказательство.

1. $A \to ((A \to A) \to A) \to ((A \to (A \to A)) \to (A \to A))$ - схема (2) при $B := A \to A, \quad C := A$
2. $A \to ((A \to A) \to A)$ - схема (1) при $B := A \to A$
3. $(A \to (A \to A)) \to (A \to A)$ - Modus ponens к шагам (1) и (2)
4. $A \to (A \to A)$ - схема (1) при $B := A$
5. $A \to A$ - modus ponens шагов (3) и (4) $\square$

3.5 Теорема дедукции

Теорема 3.2. *(Эрбрам). Пусть дано некоторое множество формул, A - произвольная формула, тогда если из Γ, A выводится формула B ($\Gamma, A \vdash B$), то $\Gamma \vdash (A \to B)$.*

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash (A \to B)}$$

Пример применения.

$\vdash (\neg B \to \neg A) \to (A \to B)$
1. $\neg B \to \neg A$ - гипотеза
2. A - гипотеза
3. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$ - схема 3
4. $(\neg B \to A)$ - MP, (1) и (3)
5. $A \to (\neg B \to A)$ - схема 1 при $B := \neg B$
6. $\neg B \to A$ - MP, (2) и (5)
7. B - MP, (4) и (6)

То есть $\neg B \to \neg A, A \vdash B$ по теореме дедукции $\neg B \to \neg A \vdash A \to B$ по теореме дедекции $\vdash (\neg B \to \neg A) \to (A \to B)$

Доказательство. Индукция по длине n вывода формулы B из $\Gamma, A \quad (\Gamma, A \vdash^n B)$, то есть число MP.

Базис: $\; n = 0$, то есть 1) $B \in \Gamma$; 2) B - аксиома; 3) $B = A$

1-й случай.

1) B - гипотеза ($B \in \Gamma$)
2) $B \to (A \to B)$ - схема (1) при $A := B, B := A$
3) $A \to B$ - MP, (1) и (2)
То есть $\Gamma \vdash (A \to B)$

2-й случай

1) B - аксиома
2) $B \to (A \to B)$ - схема (1)
3) $A \to B$ - MP, (1) и (2)
То есть $\vdash (A \to B)$, то есть для всякого $\Gamma : \Gamma \vdash (A \to B)$

3-й случай

Тогда $\vdash (A \to A)$, и $\Gamma \vdash (A \to A)$

Предположение: Пусть для любой формулы Φ такой, что $\Gamma, A \vdash^{l \leq n-1} B$ влечет $\Gamma \vdash (A \to \Phi)$; $\quad n \geq 1$

Переход: $\Gamma, A \vdash^{n} B$, то есть $\Gamma, A, \ldots, \Phi, \ldots, \Phi \to B, B$, и $\Gamma, A \vdash^{l_1} \Phi$, $\quad l_1 < n$; $\quad \Gamma, A \vdash^{l_2} \Phi \to B$; $\quad l_2 < n$
По предположению индукции: $\Gamma \vdash A \to \Phi, \quad A \to (\Phi \to B)$
Предположим вывод из Γ :

1.$(A \to (\Phi \to B)) \to ((A \to \Phi) \to (A \to B))$ - схема (2) при B:=Φ, C := B
2.$(A \to \Phi) \to (A \to B)$ - MP, (1) и формуле $A \to (\Phi \to B)$
3.$A \to B$ - MP, (2) и формуле $A \to \Phi$

Итак, $\Gamma \vdash (A \to B)$

□

Теорема 3.3. *(Обратная). Если* $\Gamma \vdash (A \to B)$*, то* $\Gamma, A \vdash B$

То есть из этих двух теорем верно:

$$\boxed{\Gamma, A \vdash B \Longleftrightarrow \Gamma \vdash (A \to B)}$$

Далее любую формулу будем называть секвенцией.

Теорема 3.4. *В теории* L *имеют место следующие секвенции:*
1) $A \to B, B \to C \vdash A \to C$
2) $A \to (B \to C), B \vdash A \to C$
3) $\vdash (\neg\neg A \to A)$
4) $\vdash (A \to \neg\neg A)$
5) $\vdash (A \to (\neg A \to B))$
6) $\vdash (\neg B \to \neg A) \to (A \to B)$
7) $\vdash (A \to B) \to (\neg B \to \neg A)$
8) $\neg A \to (\neg B \to \neg(A \to B))$
9) $\vdash (A \to B) \to ((\neg A \to B) \to B)$

Доказательство.

1)

1) $A \to B$ - гипотеза
2) $B \to C$ - гипотеза
3) A - гипотеза
4) B - MP, (1) и (3)
5) C - MP, (2), (4)

2)

1) $A \to (B \to C)$ - гипотеза
2) B - гипотеза
3) A - гипотеза
4) $B \to C$ - MP, (1) и (3)
5) C - MP, (2) и (3)

3)

1) $\neg\neg A$ - гипотеза
2) $(\neg A \to \neg\neg A) \to ((\neg A \to \neg A) \to A)$ - схема 3 при замене $A := \neg A, B := A$
3) $\neg\neg A \to (\neg A \to \neg\neg A)$ - схема 1 при $A := \neg\neg A, B :=$
4) $\neg A \to \neg\neg A$ - MP, (1) и (3)
5) $(\neg A \to) \to A$ - MP, (2) и (4)
6) $\neg A \to \neg A$ - теорема $\vdash (A \to A)$ при $A := \neg A$
7) A - MP, (5) и (6)

4)

1) $(\neg\neg\neg A \to \neg A) \to ((\neg\neg\neg A \to A) \to \neg\neg A)$ - схема 3 при $B := \neg\neg A$
2) $\neg\neg\neg A \to \neg A$ - секвенция 3 при $A := \neg A$
3) $A \to (\neg\neg\neg A \to A)$ - схема 1 при $B := \neg\neg\neg A$
4) $(\neg\neg\neg A \to A) \to \neg\neg A$ - MP, (1) и (2)
5) $A \to \neg\neg A$ - R1, (3) и (4)

5)

1) A - гипотеза
2) $\neg A$ - гипотеза
3) $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$ - схема 3
4) $\neg A \to (\neg B \to \neg A)$ - схема 1 при $A := \neg A$, $B := \neg B$
5) $\neg B \to \neg A$ - MP, (2) и (4)
6) $(\neg B \to \neg A) \to B$ - MP, (3) и (5)
7) $A \to (\neg B \to A)$ - схема 1 при $B := \neg B$
8) $\neg B \to A$ - MP, (1) и (7)
9) B - MP, (6) и (8)

6)

Уже доказана

7)

1) $A \to B$ - гипотеза
2) $\neg\neg A \to A$ - секвенция 3
3) ${}_5 A \to B$ - R1, (2) и (1)
4) $B \to \neg\neg B$ - секвенция 4
5) $\neg\neg A \to \neg\neg B$ - R1, (3) и (4)
6) $\neg B \to \neg A$ - R6, (5) при $A := \neg B, B := \neg A$

8)

$\vdash (A \to ((A \to B) \to B))$ - вспомогательная секвенция
1) A - гипотеза
2) $A \to B$ - гипотеза
3) B - MP, (1) и (2)

Само док-во:
1) A - гипотеза
2) $A \to ((A \to B) \to B)$ - теорема
3) $(A \to B) \to B$ - MP, (1) и (2)
4) $\neg B \to \neg(A \to B)$, R7, (3)

9)

1) $A \to B$ - гипотеза
2) $\neg A \to B$ - гипотеза
3) $\neg B \to \neg A$ - R7, (1)
4) $\neg B \to \neg\neg A$ - R7, (2)
5) $(\neg B \to \neg\neg A) \to ((\neg B \to \neg A) \to B)$ - схема 3 при $A := \neg A$
6) $(\neg B \to \neg A) \to B$ - MP, (4) и (5)
7) B - MP, (3) и (6)

$\square$

Следствие 1. Если $\Gamma, A \vdash B$ и $\Gamma, \neg A \vdash B$, то $\Gamma \vdash B$

Доказательство. $\Gamma, A \vdash B \implies \Gamma \vdash A \to B$; $\Gamma, \neg A \vdash B \implies \Gamma \vdash (\neg A \to B)$, тогда по R9 $\Gamma \vdash B$ $\square$

Следствие 2. (Свойства дизъюнкции).
1) $A \vdash A \vee B$; $B \vdash A \vee B$
2) $A \vee B \vdash B \vee A$
3) Если $A \vdash B$, то для любой формулы $\Phi : \Phi \vee A \vdash \Phi \vee B$; $A \vee \Phi \vdash B \vee \Phi$

Доказательство.

1 пункт.

1) A - гипотеза
2) $A \to (\neg A \to B) = A \to (A \vee B)$ - секвенция 5
3) $\neg A \to B = A \vee B$

2 пункт.

1) $A \vee B = \neg A \to B$ - гипотеза
2) $\neg B \to \neg\neg A$ - R7, (1)
3) $\neg\neg A \to A$ - секвенция 3
4) $\neg B \to A$ - R1, (2) и (3) $(= B \vee A)$

3 пункт.

1) $A \to B$ - теорема, так как $A \vdash B$
2) $\Phi \vee A = \neg\Phi \to A$ - гипотеза
3) $\neg\Phi \to B = \Phi \vee B$ - R1, (2) и (1)

$\square$

Следствие 3. (Свойства конъюнкции).
1) $A, B \vdash A \,\&\, B$
2) $A \,\&\, B \vdash A, B$
3) $A \,\&\, B \vdash B \,\&\, A$

Доказательство.

1 пункт.

1) A - гипотеза
2) B - гипотеза
3) $\neg\neg B$ - R4, (2)
4) $\neg(A \to \neg B)$ - R8, (1) и (3)

2 пункт

1) $\neg A$ - гипотеза
2) $\neg A \to (A \to \neg B)$ - секвенция 5
3) $A \to \neg B$ - MP, (1) и (2)
4) $\neg\neg(A \to \neg B)$ - R4, (3)

3 пункт.

1) $B \to \neg A$ - гипотеза
2) $\neg\neg A \to \neg B$ - R7, (1)
3) $A \to \neg\neg A$ - секвенция 4
4) $A \to \neg B$ - R1, (3) и (2)

□

3.6 Непротиворечивость и полнота теории L

Теорема 3.5. *Любая теорема теории L есть тавтология.*

Доказательство. Легко проверить, что каждая формула, получаемая из схемы аксиомы, будет тавтологией.

Φ - тавтология, $\Phi \to \Psi$ - тавтология.

Пусть Ψ - не есть тавтология.

$$(\forall\widetilde{\alpha})\Phi(\alpha) = T, \quad (\Phi \to \Psi)(\alpha) = \Phi(\widetilde{\alpha}) \to \Psi(\widetilde{\alpha}) = T$$

То есть

$$\Phi(\widetilde{\alpha}) \to \Psi(\widetilde{\alpha}) = T \to F$$

есть противоречие. □

Следствие. В теории L нельзя доказать формулу и ее отрицание.

Теорема 3.6. *Любая тавтология доказуема в теории L.*

Доказательство. Будем считать, что

$$\Phi = \Phi(x_1, \dots, x_n); \quad \widetilde{\alpha} = (\alpha_1, \dots, \alpha_n); \quad \Phi^{\widetilde{\alpha}} \leftrightharpoons \begin{cases} \Phi, \text{ если } \Phi(\widetilde{\alpha}) = T \\ \neg\Phi, \text{ если } \Phi(\widetilde{\alpha}) = F \end{cases}$$

Лемма (Кальмара) . $x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \Phi^{\widetilde{\alpha}}$

Доказательство. (Док-во леммы). Индукция по числу $l(\Phi)$ логических связок в формуле Φ.

Базис: $l(\Phi) = 0$, значит формула Φ есть переменная. $\Phi = x_i$ - переменная.
Тогда очевидна такая секвенция $x_i^{\alpha_i} \vdash x_i^{\alpha_i}$, то есть $x_i \vdash x_i$ или $\neg x_i \vdash \neg x_i$ - очевидно В силу $\vdash (A \to A)$.

Предположение: Пусть утверждение леммы справедливо при любом значении $l(\Phi) \leq n - 1, n \geq 1$

Переход: Полагаем, что $l(\Phi) = n$.

1 случай.

$\Phi = \neg\Psi$, где $l(\Psi) = n-1$
1.1 $\Psi(\widetilde{\alpha}) = F$
$\Phi(\widetilde{\alpha}) = n, \Phi^{\widetilde{\alpha}} = \Phi, \Psi^{\widetilde{\alpha}} = \neg\Psi$
По предположению индукции $x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \Psi^{\widetilde{\alpha}} = \neg\Psi = \Phi = \Phi^{\widetilde{\alpha}}$

1.2 $\Psi(\widetilde{\alpha}) = T$
$\Phi(\widetilde{\alpha}) = F, \quad \Phi^{\widetilde{\alpha}} = \Phi, \quad \Psi^{\widetilde{\alpha}} = \Psi$
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \Psi^{\widetilde{\alpha}} \vdash \neg\neg\Psi = \neg\Phi = \Phi^{\widetilde{\alpha}}$

2 случай.

$\Phi = q \to \psi$, где $l(Q) + l(\Psi) = n-1, \quad l(Q), l(\Psi) < n.$

2.1 $Q(\widetilde{\alpha}) = \Psi(\widetilde{\alpha}) = F$
$Q^{\widetilde{\alpha}} = \neg Q, \Psi^{\widetilde{\alpha}} = \neg\Psi, \Phi(\widetilde{\alpha}) = F \to F = T$
По предположению индукции:
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \neg Q, \neg\Psi; \quad \neg Q \to (Q \to \Psi)$ - секвенция 5; $Q \to \Psi$ - MP
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash Q \to \Psi = \Phi = \Phi^{\widetilde{\alpha}}$

2.2 $Q(\widetilde{\alpha}) = F \quad \Psi(\widetilde{\alpha}) = T$
$Q^{\widetilde{\alpha}} = \neg Q, \Psi^{\widetilde{\alpha}} = \Psi, \Phi(\widetilde{\alpha}) = F \to T = T$
По предположению индукции:
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \neg Q, \Psi; \quad \neg Q \to (Q \to \Psi)$ - секвенция 5; $Q \to \Psi$ - MP
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash Q \to \Psi = \Phi = \Phi^{\widetilde{\alpha}}$

2.3 $Q(\widetilde{\alpha}) = T \quad \Psi(\widetilde{\alpha}) = F$
$Q^{\widetilde{\alpha}} = Q, \Psi^{\widetilde{\alpha}} = \neg\Psi, \Phi(\widetilde{\alpha}) = T \to F = F$
По предположению индукции:
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash Q, \neg\Psi; \neg(Q \to \Psi)$ - по R8
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \neg(Q \to \Psi) = \neg\Phi = \Phi^{\widetilde{\alpha}}$

2.4 $Q(\widetilde{\alpha}) = T \quad \Psi(\widetilde{\alpha}) = T$
$Q^{\widetilde{\alpha}} = Q, \Psi^{\widetilde{\alpha}} = \Psi, \Phi(\widetilde{\alpha}) = T \to T = T$
По предположению индукции:
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash Q, \Psi; \Psi \to (\Phi \to \Psi), Q \to \Psi$ - MP
$x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash (Q \to \Psi) = \Phi = \Phi^{\widetilde{\alpha}}$

□

Продолжаем доказательство теоремы.
Пусть Φ - тавтология, то есть $(\forall\widetilde{\alpha})(\Phi(\widetilde{\alpha}) = T)$.
В силу леммы: $x_1^{\alpha_1}, \dots, x_n^{\alpha_n} \vdash \Phi \left[(\forall\widetilde{\alpha})Phi^{\widetilde{\alpha}} = \Phi\right]$

$$\widetilde{\alpha}_1 = (\alpha_1, \dots, \alpha_{n-1}, \neg\alpha_n) \quad x_1^{\alpha_1}, \dots, x_n^{\alpha_n - 1}, x_{n-1}^{\alpha_n} \vdash \Phi$$

То есть

$$x_1^{\alpha_1}, \dots, x_{n-1}^{\alpha_{n-1}} \vdash \Phi,$$

где стало на 1 меньше. Так отсчипываем, пока не получим:

$$x_1^{\alpha_1} \vdash \Phi_1, \neg x_1^{\alpha_1} \vdash \Phi$$

$$\vdash \Phi$$

□

Следствие. Формула является тавтологией тогда и только тогда, когда она доказуема в теории L.

3.7 Эквивалентные формулы

Определение 60. Две формулы называют эквивалентными, если они выводимы друг из друга

$$\Phi \equiv \Psi \leftrightharpoons \Phi \vdash \Psi \quad \Psi \vdash \Phi$$

$$\Phi \equiv \Psi \Longleftrightarrow \vdash (\Phi \to \Psi)\,\&(\Psi \to \Phi)$$

Также $\Phi \equiv \Psi \Longleftrightarrow \neg\Phi \equiv \neg\Psi$

Утверждение. Если $\Phi \equiv \Psi$, то $(\forall\widetilde{\alpha})(\Phi(\widetilde{\alpha}) = \Psi(\widetilde{\alpha}))$

Примеры эквивалентности.

1) $\neg\neg A \equiv A$
2) $(A \to B) \equiv (\neg B \to \neg A)$
3) $\neg(A \vee B) \equiv \neg A \,\&\, \neg B \quad \neg(A \,\&\, B) \equiv \neg A \vee \neg B$
4) $A \vee A \equiv A$
5) $A \to (B \to C) \equiv (A \,\&\, B) \to C$
6) $\neg(A \to B) \equiv A \,\&\, \neg B$

Определение 61. Подформула - это часть формулы, которая сама является формулой. Формула Фи содержит Тета в виде подформулы - $\Phi[\Theta]$. $\Phi[\Theta'/\ \Theta]$ - формула, получаемая заменой Θ на формулу Θ'

Теорема 3.7. *Пусть* $\Phi[\Theta](x_1, \ldots, x_n)$. *Тогда, если* $\Theta' \equiv \Theta$, *то* $(\forall\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n))\Phi(\Theta'/\ \Theta)(\widetilde{\alpha}) = \Phi[\Theta](\widetilde{\alpha})$

Следствие. Если $\vdash \Phi[\Theta]$, то при $\Theta' \equiv \Theta \vdash \Phi[\Theta'/\ \Theta]$

3.8 Исчисление предикатов первого порядка

3.8.1 Понятие алгебраической системы

Определение 62. $\mathscr{A} = (A, \Omega, \prod)$ - алгебраическая система. A - множество, далее сигнатура операций, сигнатура предикатов.
$\omega : A^n \to A, \quad n \geq 0, \omega \in \Omega$ - операция
$p : A^n \to \{T, F\}, \quad n \geq 1$ - предикат

$p(x_1) = T \leftrightharpoons x_1$ есть четное число
$p(x_1, x_2) = T \leftrightharpoons x_1 + x_2 \geq x_1 * x_2$

Если множество предикатов $\prod = \varnothing$, то получаем алгебру $\mathscr{A} = (A, \Omega)$
Если множество операций $\Omega = \varnothing$, то получаем модель $\mathscr{A} = (A, \prod)$

Модель - это, например, граф $\mathcal{J} = (V, \rho)$.

3.8.2 ИП1: алфавит, понятие формулы

Определение 63. Алфавит состоит из таких частей:

1) $X = \{x_1, x_2, \ldots, x_n\}$ - множество предметных элементов
2) $\mathcal{F} = \mathcal{F}^{(0)} \cup \mathcal{F}^{(1)} \cup \ldots \cup F^{(n)} \cup \ldots$ - множество функциональных символов
3) $\mathscr{P} = \mathscr{P}^{(1)} \cup \mathscr{P}^{(2)} \cup \ldots \cup \mathscr{P}^{(n)} \cup \ldots$ - множество предикатных символов
4) $C = \mathcal{F}^{(0)}$ - множество предметных констант
5) Множество логических символов: $\to, \neg, \forall$. $\forall$ - квантор общности.
6) Множество вспомогательных символов Aux

Определение 64. Термы - это

1) Любая предметная переменная и любая переменная константа есть терм

2) Если $t_1, \ldots, t_n$ - термы, а $f^{(n)} \in \mathcal{F}^{(n)}$, то $f^{(n)}(t_1, \ldots, t_n)$ - терм

3) Других термов нет

Вместо $f^{(2)}(t_1, t_2)$ пишем $t_1 f^{(2)} t_2$

$t = (x_1 + x_2) \cdot ((-x_3) + x_1)$
$+, \cdot \in \mathcal{F}^{(2)}, \quad - \in F^{(1)}$

Определение 65. Атомарная формула - это выражение вида $p^{(n)}(t_1, \ldots, t_n)$, где $p^{(n)}$ - n-арный предикатный символ, а $t_1, \ldots, t_n$ - термы.

$\underbrace{\geq}_{p^{(2)}}(\underbrace{x_1 + x_1}_{t_1}, \underbrace{x_1 * x_2}_{t_2})$

Определение 66. Формула - это

1) Атомарная формула есть формула.

2) Если Φ, Ψ - формулы, то $(\Phi \to \Psi)$ - формула

3) Если Φ - формула, то $(\overline{\Phi})$ - формула

4) Если Φ - формула, а $x_i \in X$, то $(\forall x_i)\Phi$ - формула

5) Других формул нет

Определение 67.

1) $\Phi \vee \Psi = \neg\Phi \to \Psi$

2) $\Phi \,\&\, \Psi = \neg(\Phi \to \neg\Psi)$

3) $(\exists x_i)\Phi = \neg(\forall x_i)\neg\Phi$

$F \vee (\Phi)$ - множество свободных переменных в формуле Φ

Определение 68. Терм t свободен для переменной X_i в формуле $\Phi(x_i)$, если никакое свободное вхождение переменной X_i в формулу $\Phi(x_i)$ не находится в области действия квантора по переменной, входящей в терм.

3.8.3 Понятие интерпретации. Выполнимость, истинность, логическая общезначность.

Определение 69. Интерпретация - это $\mathcal{J} = (\underbrace{\mathscr{A} = (A, \Omega, \prod)}_{\text{Область интерпретации}}, i_F, i_P)$

$$i_F : \mathcal{F} \to \Omega, \text{ причем } (\forall n \geq 0) i_F(f^{(n)}) \in \Omega^{(n)}$$

$$I_P : \mathscr{P} \to \prod, \text{ причем } (\forall n \geq 1) i_P(P^{(n)}) \in \Pi^{(n)}$$

Определение 70. Состояние - это $\sigma : X \to A$

Определение 71. $\sigma \underset{i}{=} \tau \leftrightharpoons$ для всех $i \neq j$ верно $\sigma(x_j) = \tau(x_j)$

Определение 72. Значение $t^\sigma_{\mathcal{J}}$ терма t в состоянии σ при интерпретации $\mathcal{J}$

1) Если $t = x_i \in X$, то $t^\sigma \leftrightharpoons \sigma(x_i)$

2) Если $t = c \in C = \mathcal{F}^{(0)}$, то $t^\sigma = i_F(c) \in A$

3) Если $t = f^{(n)}(s_1, \ldots, s_n)$, то $t^\sigma \leftrightharpoons i_F(f^{(n)})(s_1^\sigma, \ldots, s_n^\sigma)$
Пусть $t = (x_1 + x_2)((-x_3) + x_1 x_2)$. Состояние $\sigma = \{1|x_1, 2|x_2, 3|x_3, \ldots\} = \{x_1 := 1, x_2 := 2, x_3 := 3, \ldots\}$
То есть $t^\sigma = (3)(-1) = -3$ (просто подставили в формулу и посчитали)

4) (Истинностное) значение Φ^σ формулы Φ в состоянии σ (при заданной интерпретации)

Определение 73. Значение формулы с квантором

1) Если $\Phi = p^{(n)}(t_1, \dots, t_n)$, то $\Phi^\sigma \leftrightharpoons i_P(p^{(n)})(t_1^\sigma, \dots, t_n^\sigma)$
2) Если $\Phi = \neg\Psi$, то $\Phi^\sigma = \neg(\Psi^\sigma)$
3) Если $\Phi = \Theta \to \Psi$, то $\Phi^\sigma \leftrightharpoons \Theta^\sigma \to \Psi^\sigma$
4) Если $\Phi = (\forall x_i)\Psi$, то $\Phi^\sigma = T \leftrightharpoons$ Для любого состояния $\tau \underset{i}{=} \sigma :\ \Psi^\tau = T$

Определение 74.

$\underset{\mathcal{J}}{\models} \Phi \leftrightharpoons$ существует состояние σ, для которого $\Phi^\sigma = T$
$\underset{\mathcal{J}}{\vdash} \Phi \leftrightharpoons$ Для всех состояний σ $\Phi^\sigma = T$
Формула называется логически общезначной, если она истинна в любой интерпретации.

3.8.4 Аксиомы и правила вывода ИП1

$$\begin{array}{lc}
(1) & A \to (B \to A) \\
(2) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\
(3) & (\neg B \to \neg A) \to ((\neg B \to A) \to B) \\
(4) & (\forall x_i)A(x_i) \to A(t|x_i) \text{ при } Free(t, x_i, A) \\
(5) & (\forall x_i)(A \to B) \to (A \to (\forall x_i)B) \text{ при } x_i \notin F \vee (A)
\end{array}$$

Правило A4: $\frac{(\forall x_i)A(x_i)}{A(t)}$, где $Free(t, x_i, A)$.

Теорема 3.8. *Всякая теорема исчисления предикатов первого порядка логически общезначима.*

По определению в исчислении предикатов первого порядка считается, что тавтологией считается любая формула, выводимая исключительно из первых трех схем с применением только правила *modus ponens*

Исчисление предикатов первого порядка не противоречиво.

Теорема 3.9. *Исчисление предикатов первого порядка полно, то есть любая логически общезначимая формула доказуема в этом исчислении.*

Следствие. Формула логически общезначимая тогда и только тогда, когда она доказуема в исчислении предикатов первого порядка. (Теорема Бёдаля о Полноте).

Гедаль, а не бедаль!!!

3.8.5 Теорема Дедукции для ИП1

Теорема 3.10. *(Дедукции для ИП1). Если $\Gamma, A \vdash B$, причем существует такой вывод формулы B из множества формул $\Gamma \cup \{A\}$, в котором ни при каком применении правила Gen к формулам, зависящем в этом выводе от формулы A, не связывается квантором никакая свободная переменная формулы A, то $\Gamma \vdash A \to B$.*

В ИП эквивалентность отличается отэквивалентности в исчислении выражений:

$$\Phi \equiv \Psi \leftrightharpoons \vdash (\Phi \to \Psi)\,\&(\Psi \to \Phi)$$

3.8.6 Некоторые дополнительные правила

Одно мы уже знаем (A4):

$$\frac{(\forall x_i)A(x_i)}{A(t)} \text{ при } Free(t, x_i, A)$$

Вот еще одно схожее (E4):

$$\frac{A(t)}{(\exists x_i)A(x_i)} \text{ при } Free(t, x_i, A)$$

Правило выбора (C):

$$\frac{(\exists x)A(x)}{A(b)}$$

3.9 Теории первого порядка

Аксиомы теории первого порядка имеет две части:

1. Логически общезначимые формулы (ИП1)
2. Нелогические аксиомы (это такие, к-рые не являются общезначимыми, но верны в широком классе интерпретации)

Определение 75. Любая интерпретация, в которой верна нелогическая аксиома, называется моделью.

Теория первого порядка с равенством

(НЛ) - это нелогическая теория.

(НЛ1) $(\forall x)(x = x)$

(НЛ2) $(x = y) \to (A(x, x) \to A(x, y))$, $x \in F \vee (A)$

Теорема 3.11.

1. $\vdash (x = y) \to (y = x)$

2. $\vdash (x = y) \to ((y = z) \to (x = z))$

Доказательство.

1.1 $(x = y) \to ((x = x) \to (y = x))$ - (НЛ2) при $A(x, x) := (x = x), A(x, y) := (y = x)$
1.2 $(\forall x)(x = x)$ - (НЛ1)
1.3 $x = x$ - A4, (2)
1.4 $(x = y) \to (y = x)$ - R2, (1) и (3)

2.1 $x = y$ - гипотеза
2.2 $y = z$ - гипотеза
2.3 $(y = x) \to ((y = z) \to (x = z))$ - (НЛ2) при $A(y, y) := (y = z), A(y, x) := (x = z)$
2.4 $(x = y) \to (y = x)$ - теорема (п. 1)
2.5 $y = x$ - MP, (1) и (4)
2.6 $(y = z) \to (x = z)$ - MP, (3) и (5)
2.7 $x = z$ - MP, (2) и (6) □

Теорема 3.12. *Для произвольных термов s, t и 'u' имеет место:*

1. $\vdash (t = t)$

2. $\vdash ((s = t) \to (t = s))$

3. $\vdash (s = t) \to ((t = u) \to (s = u))$

Доказательство.

1.1 $(\forall x)(x = x) \to (t = t)$ - схема (4)
1.2 $(\forall x)(x = x)$ - (НЛ1)
1.3 $t = t$ - MP, (1) и (2)

2.1 $(x = y) \to (y = x)$ - теорема
2.2 $(\forall y)((x = y) \to (y = x))$ - Gen, (1)
2.3 $(\forall x)(\forall y)((x = y) \to (y = x))$ - Gen, (2)
2.4 $(\forall y)((s = y) \to (y = s))$ - A4, (3), $x, y \notin Var(s)$
2.5 $(s = t) \to (t = s)$ - A4, (4), $x, y \notin Var(t)$ □

3.10 Метод резолюций (МР)

МР - это формализованное доказательство от противного.

3.10.1 МР в ИВ

Идея метода резолюции состоит в том, что надо доказать $\vdash \Phi$. Для этого мы подвергаем формулу Φ в отрицание и преобразуем в конъюнктивной нормальной форме (КНФ).

Мы понимаем под $\neg\Phi =$ дизъюнкты $= (A_1 \vee \ldots \vee A_n)(B_1 \vee \ldots \vee B_n)\ldots(C_1 \vee \ldots \vee C_n)$

Правило R(esolution) :

$$\frac{A \vee L_1, \neg A \vee L_2}{L_1 \vee L_2}$$

$L_1 \vee L_2$ называется резолвентой.

$\square$ - пустой дизъюнкт.
Например,

$$\frac{A, \neg A}{\square}$$

При нахождении пустого дизъюнкта доказательство завершается, доказываемая формула считается тавтологией.

Пусть $\Phi = \Theta \to \Psi$. Тогда Θ преобразуется к КНФ и $\neg\Psi$ преобразуется в КНФ.

Пример.

$\vdash \underbrace{((A \to B) \to A)}_{\Theta} \to \underbrace{A}_{\Psi}$
$\Theta = (A \to B) \to A = (\neg A \vee B) \to A = \neg(\neg A \vee B) \vee A = (A \,\&\, \neg B) \vee A = A$
1. A - из посылки
2. ¬A - из отрицания заключения
3. $\square$ - (1) и (2)

Докажем в теории L, что резолвента в правиле является логическим следствием своих посылок, то есть

$$A \vee L_1, \neg A \vee L_2 \vdash L_1 \vee L_2$$

$$\neg A \to L_1, \neg\neg A \to L_2 \vdash \neg L_1 \to L_2$$

1. $\neg A \to L_1$ - гипотеза
2. $\neg\neg A \to L_2$ - гипотеза
3. $\neg L_1$ - гипотеза
4. $\neg L_1 \to \neg\neg A$ - R7, (1)
5. $\neg L_1 \to L_2$ - R1, (4) и (2)
6. L_2 - MP, (3) и (5)

3.10.2 МР в ИП1

Сначала нужно для МР в ИП1:

1. ПНФ - предваренная нормальная формула
2. Сколемовская стандартная формула (Тудальф Сколем, 1887-1963)
3. Унификация формул