МТ

$DTime[f(n)]$ $\quad O(f(n))$

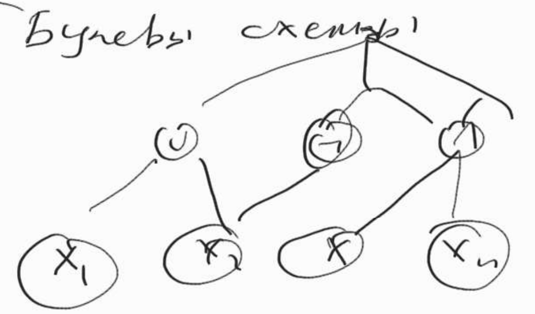
$x \in L$

$P = \bigcup_{c>0} DTime[n^c]$

n^{100000}

$\underbrace{10^{1000} \cdot n}$

Булевы схемы



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

$L \subseteq \{0,1\}^*$

$\{C_n\}_{n=1}$ $\quad C_n$ имеет n входов

$Size[f(n)]$ $\quad \{C_n\}$ $\quad |C_n| \le f(n)$

$P/poly = \bigcup_{c>0} Size[n^c]$

<u>Пример.</u> $P/poly$ содержит неразрешимые языки.

- Унарный язык $\subseteq \{1\}^*$
- U-унарный язык $\Rightarrow$ $U \in P/poly$
- H-неразреш. язык. $\Rightarrow$ $U_H = \{1^n \mid n \in H\}$

U_H - неразрешим.

$P \subseteq P/poly$

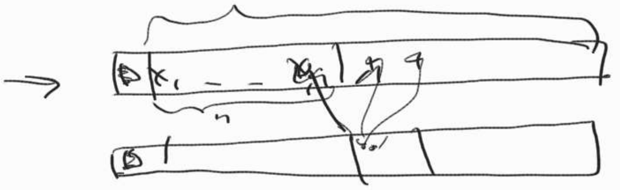
<u>Лемма</u> $L \in DTime[t(n)]$, тогда $L \subseteq \{0,1\}^*$

$L \in Size[O(t^4(n))] = \bigcup_{c>0} Size[c t^4(n)]$

<u>Д-во</u> L реш. однолент. МТ за $O(t(n)^2)$

$T(n)$

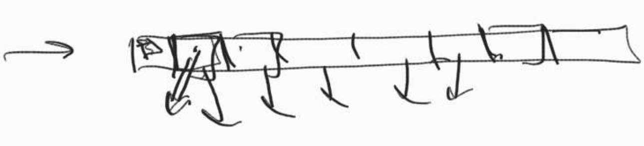
шагов. $T(n)$ $\quad T(n) = O(t(n)^2)$



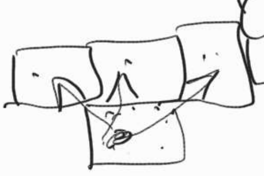
0

1

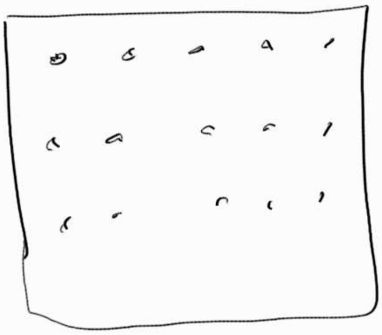
Символ	$O(1)$
Тут ли головка	1
Состояние если головка тут	$O(1)$



$T(n)$



$O(T(n)^2)$



§ Класс NP и всё про него

<u>Опр.</u> Эффективная система д-в для языка L. $x \in L$

Э.С.Д. для L — это алгоритм $\Pi(x,w)$:

1) Корректность: $\exists w: \Pi(x,w)=1 \Rightarrow x \in L$
2) Полнота: $\forall x \in L \ \exists w: \Pi(x,w)=1$
3) Эффективность: время работы $\Pi(x,w)$ не превосходит $poly(|x|+|w|)$.

<u>Опр.</u> $L \in NP \iff \exists$ полин. эффективная система д-в Π для L: $\exists$ полином q: $\forall x \in L \ \exists w: \Pi(x,w)=1$ и $|w| \le q(|x|)$.

<u>Примеры</u>

1) $P \subseteq NP$ A — распозн. алг. для L

$\Pi(x,w) := A(x)$

2) COMPOSITE — множество составных натур. чисел.

2^{100000} 2^{50000}

$a \neq 1, a < n$

n, a

$a \mid n$

3) $GI = \{(G_1, G_2) \mid G_1 \cong G_2\}$

$GNI = \{(G_1, G_2) \mid G_1 \ncong G_2\}$

$O(n^{\log^c n})$

4) SAT — мн-во выполнимых пропозиц. формул

$(\bar{x} \vee y) \to (\bar{x} \vee z)$

UNSAT — мн-во невыполн. ф-л

5) CLIQUE = $\{(G, k) \mid$ в графе G есть полный подграф на k вершинах $\}$

6) Hampath = $\{G \mid$ в G есть гам. путь $\}$

7) 3COL = $\{G$, вершины кот. можно раскр. в 3 цвета прав. образом $\}$

Класс NP не симметричен.

$L \in NP \overset{?}{\Rightarrow} \bar{L} \in NP$

$\left.\begin{array}{l} L \in NP \text{ и } \bar{L} \in NP \end{array}\right\} \overset{?}{\Rightarrow} L \in P$ открытый вопрос

$P = \bigcup_c DTime[n^c]$

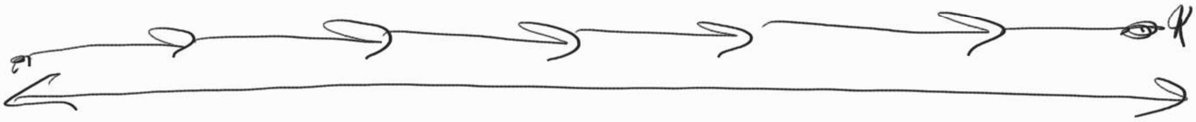
Недетерм. М.Т. только для yes/no задач

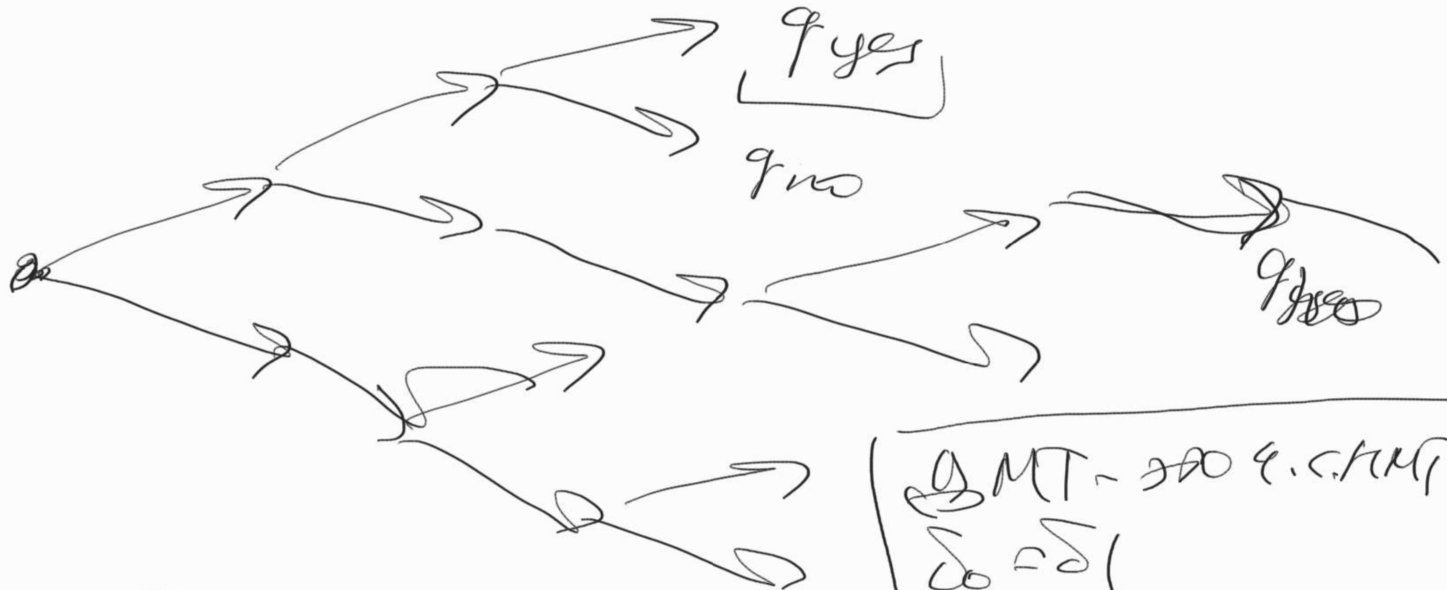
Q q_0 q_{yes}, q_{no}

$\delta_0: Q \times \Sigma^k \to Q \times \Sigma^k \times \{\to, \leftarrow, \cdot\}$

$\delta_1:$

Н.М.Т. принимает вход x, если $\exists$ корректная послед-ть переходов, кот. приводит в сост. q_{yes}. Время работы Н.М.Т — макс. по всем вѣрн. переходам.





Д.М.Т — это ч.с. Н.М.Т
$\delta_0 = \delta_1$

NTime $[f(n)]$ — это мн-во языков L : $\exists$ Н.М.Т. M :

1) $\forall x$ $M(x)$ раб. $O(f(n))$ шагов $n = |x|$

2) $\forall x \in L$ M прин. x

3) $\forall x \notin L$ M отвергает x

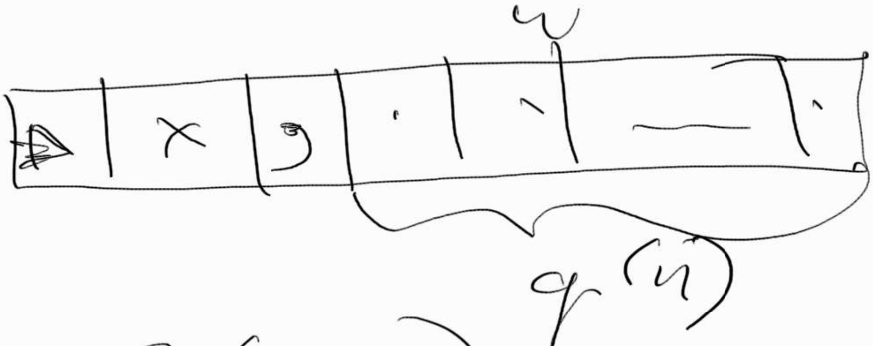
Теорема $NP = \bigcup\limits_c NTime[n^c]$

Д-во $NP \subseteq \bigcup\limits_c NTime[n^c]$

$L \in NP$ $\quad$ Π — эффект. сист. д-в для L

$\forall x$ $\exists$ полином q :

$x \in L \Leftrightarrow \exists w : |w| \leq q(|x|) : \Pi(x, w) = 1$



σ_0

σ_1

$\Pi(x, w)$

$NP \overset{?}{\supseteq} NTime[n^c]$ $\forall c$

L расп. НМТ M

$x \in L$

Д-во того, что

0 1 —— . L $\in$

σ_0 σ_1 σ_{L}

n^c

Опр L сводится за полин. время к L' (сводится по Карпу), если $\exists$ полином. вычисл. ф-ция f: $x \in L \iff f(x) \in L'$. Обозн: $L \le_p L'$

Св-ва $\le_p$

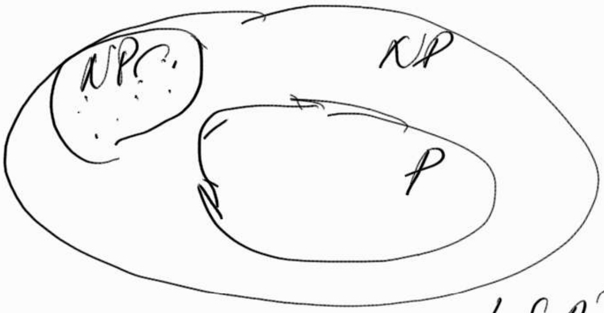
1) транзитивность $L \le_p L'$, $L' \le_p L'' \Rightarrow L \le_p L''$
   f_1 f_2 $f_2(f_1)$

2) $L \le_p L'$, $L' \in P \Rightarrow L$ - тоже из P (замкнутость отн-но P)

X - класс языков

L наз-ся X трудным отн-но $\le_p$, если $\forall L' \in X$ $L' \le_p L$.

L наз-ся X-полным, если $L \in X$ и L - X трудный



CLIQUE
HamPath
SAT
3COL

$$\text{Circuit-SAT} \le_p \text{3-SAT}$$

$$BH \le_p \text{Circuit-SAT}$$

$BH = \{ (M, x, 1^t) \mid$ M — недетерм. М.Т. у $M(x)$ есть приним. вычисление длины $\le t \}$

Утв. $BH \in NP$

$\alpha \in \{0,1\}^t$ кодирует приним. вычисл.

$\Pi((M, x, 1^t), \alpha)$ poly(t) padding

Теорема BH является NP-трудным.

Д-во Рассмотрим $L \in NP$

M — это НМТ, кот. принимает L за $q(n)$ шагов.

$$f : x \longmapsto (M, x, 1^{q(|x|)})$$

$$x \in L \Rightarrow f(x) = (M, x, 1^{q(|x|)}) \in BH$$

$$\text{Пусть } f(x) \in BH \Rightarrow M \text{ прин. } x \Rightarrow x \in L$$

$$BH \le_p \text{CircuitSAT}$$