NP $x \in L$

$|w| \le p(|x|)$ 1-ленточная

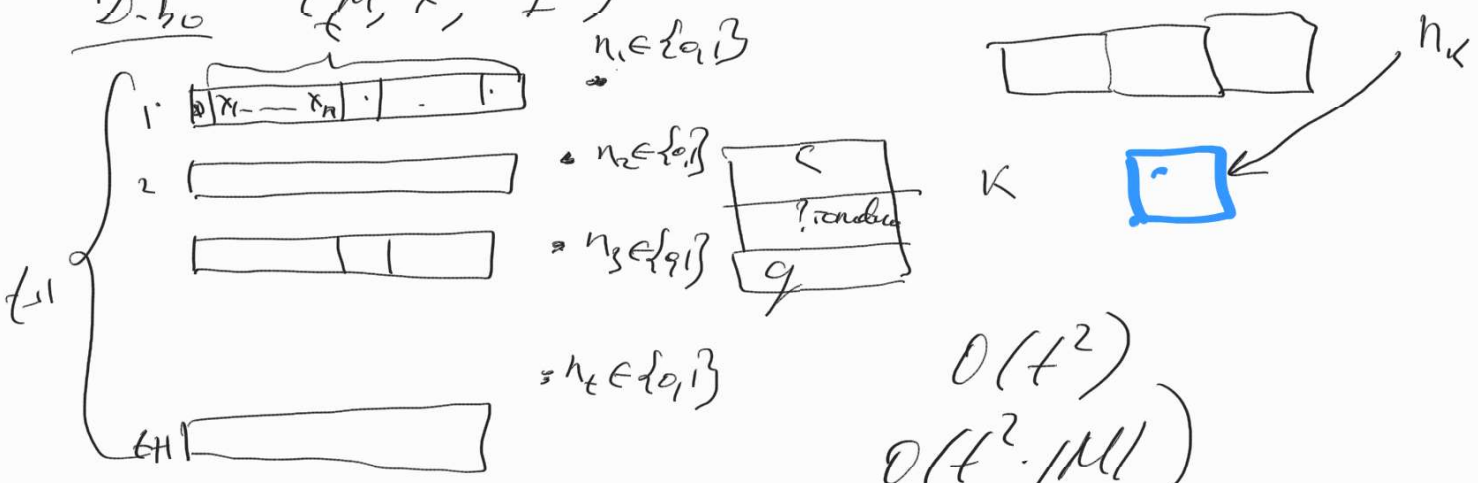
$ВН = \{(M, x, 1^t) \mid$ НМТ M $\exists$ прин. вычисл. $M(x)$ длина $\le t\}$

δ_0, δ_1

Circuit SAT – мн-во выполнимых булевых схем

Лемма $ВН \le_p$ Circuit SAT

Д-во $(M, x, 1^t) \longmapsto$ Схема

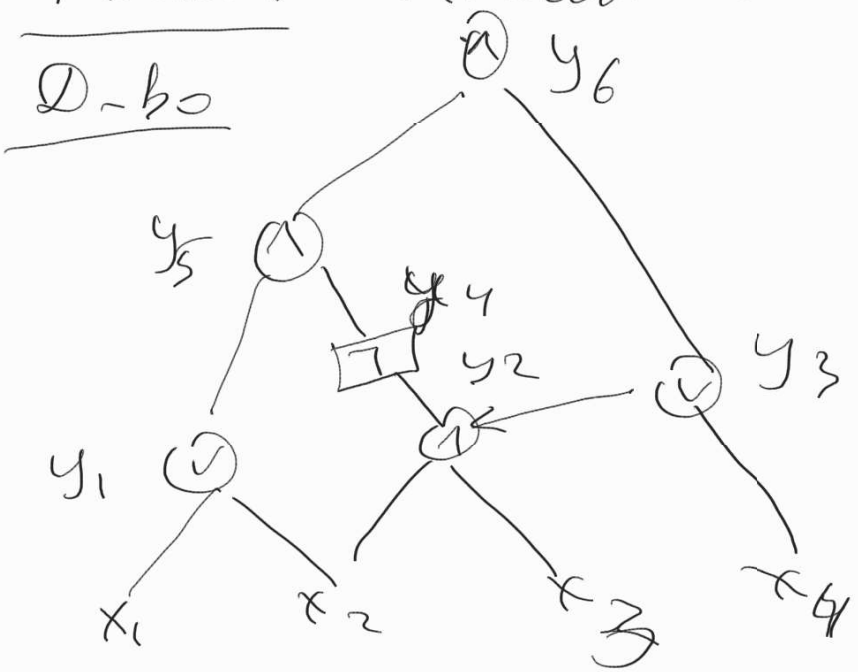


$O(t^2)$

$O(t^2 \cdot |M|)$

Лемма Circuit SAT $\le$ 3 SAT

Д-во



$y_1 = x_1 \vee x_2$

$y_2 = x_2 \wedge x_3$

$y_3 = y_2 \vee x_4$

$y_4 = \neg y_2$

$y_5 = y_1 \wedge y_4$

$y_6 = y_5 \wedge y_3$

$y_6 = 1$

Схема вып $\Leftrightarrow$ система имеет реш.

$y_1 = x_1 \vee x_2$ → в КНФ от 3-нер

3-SAT $\leq_p$

CLIQUE $= \{(G, k) \mid$ в G есть полный подграф. из k вершин $\}$

IndSet $= \{(G, k) \mid$ в G есть независ. мн-во разм. $k\}$

CLIQUE $\leq_p$ IndSet

IndSet $\leq_p$ Clique

Теорема 3-SAT $\leq$ IndSet

Д-во

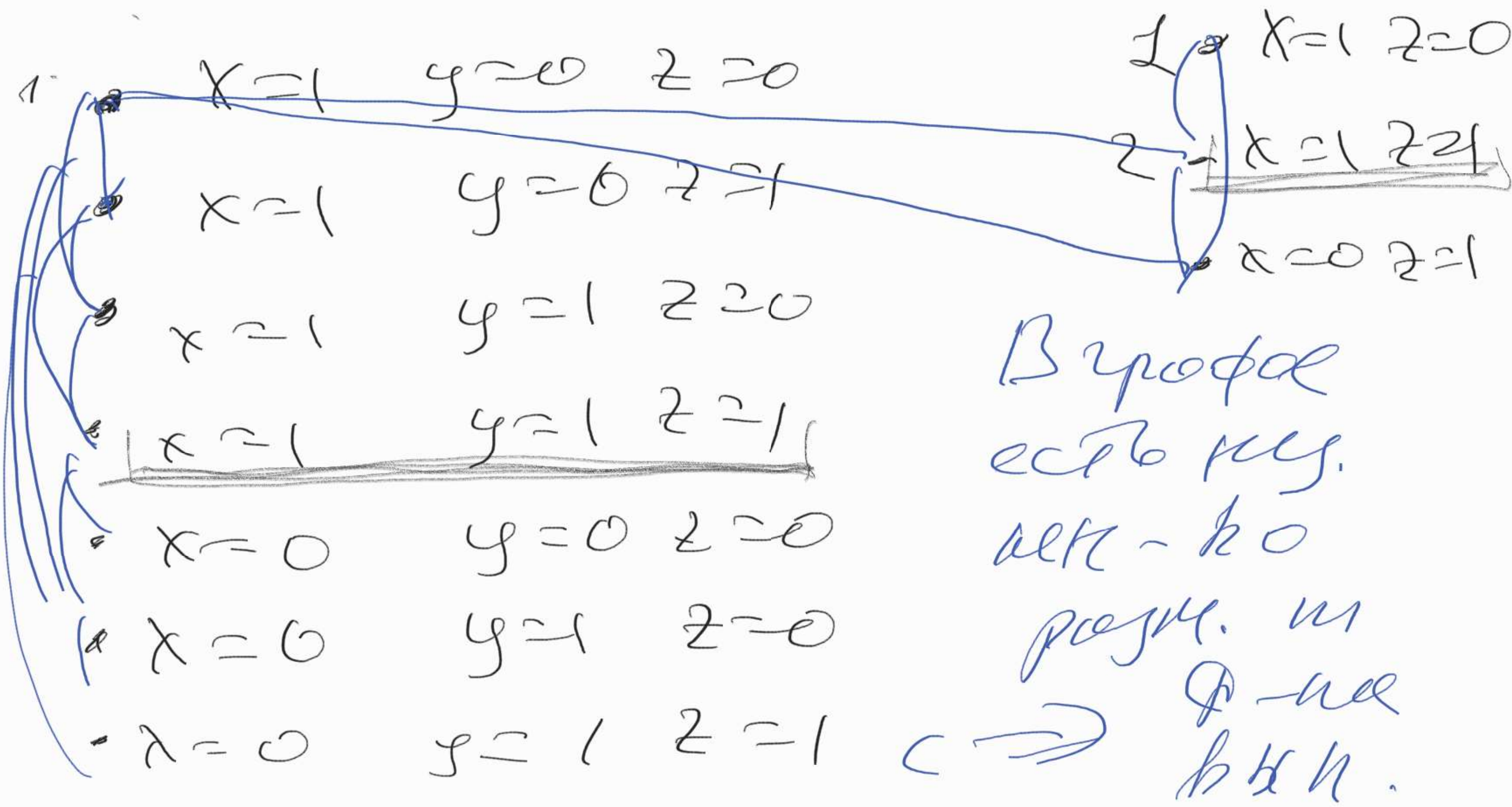
$\varphi \longmapsto (G, k)$

$\varphi = C_1 \wedge C_2 \wedge \dots \wedge C_m$

C_i $x \vee y \vee \bar{z}$

0 0 1 не вып.

7 вып. наборов $x \vee z$



В графе есть нез. мн-во разм. m $\Longleftrightarrow$ ф-ла вып.

---

§ NP задачи поиска.

$\Pi(x, w)$ $\quad x \in L$

$L = \{x \mid \exists y : \Pi(x,y) = 1\}$

Ч

<u>NP задача поиска</u>

Π — это эффективная сист. д-в для языка L

$\tilde{\Pi}$: дан x найти y: $\Pi(x,y) = 1$

$\widetilde{SAT}$ дана ф-ла. Найти вып. набор

FACTORING дано N Найти $x, y \in \mathbb{N}, > 1$: $N = x \times y$

$\widetilde{SAT}$ сводится к SAT

$\tilde{\Pi}$ ~~св-ся~~ $\quad L_\Pi = \{x \mid \exists w : \Pi(x,w) = 1\}$

FACTORING — сложный $\qquad$ COMPOSITE простая

Машина Тьюринга с оракулом

M^A

оракул

оракул да

оракул нет

$$P^A = \bigcup_{c} DTime^A[5(n)]$$

$$DTime^A[n^c]$$

Опр. Язык L алг. задачи поиска Π сводится по Куку (за полин. время по Тьюрингу) к языку A, если $\exists$ полин. по времени $M.T.$ M^A с оракулом A, которая распознает L (решает Π) за полином. время.

Обозначение $L \leq_{PT} A$

$\Pi \leq_{PT} A$

Утв. $L_1 \leq_P L_2 \Rightarrow L_1 \leq_{PT} L_2$

Св-ва сведений

---

1) Транзитивность

$L_1 \leq_{PT} L_2$, $L_2 \leq_{PT} L_3 \Rightarrow L_1 \leq_{PT} L_3$

$\Pi \leq L_2$, $L_2 \leq_{PT} L_3 \Rightarrow \Pi \leq_{PT} L_3$

2) $L_1 \leq_{pT} L_2$, $L_2 \in P \Rightarrow L_1 \in P$

$\widetilde{P}$ – это все NP задачи поиска, которые реш. за полин. время.

$\widetilde{\Pi} \leq L_2$, $L_2 \in P \Rightarrow \widetilde{\Pi} \in \widetilde{P}$.

NP-задач

<u>Теорема</u> (Сведение поиска к языкам) для L

Π - эффект. система д-в. $\widetilde{\Pi} \leq_{pT} A$.

Тогда $\exists A \in NP$:

<u>Сл-ие</u> Если при этом L NP-полный, тогда $\widetilde{\Pi} \leq_{pT} L$

<u>Д-во следствия</u> $\widetilde{\Pi} \leq_{pT} A$, $A \leq_{pT} L \Rightarrow \widetilde{\Pi} \leq_{pT} L$

NP-задач

<u>Теорема</u> (Сведение поиска к языкам) для L

Π - эффект. система д-в. $\widetilde{\Pi} \leq_{pT} A$.

То а $\exists A \in NP$:

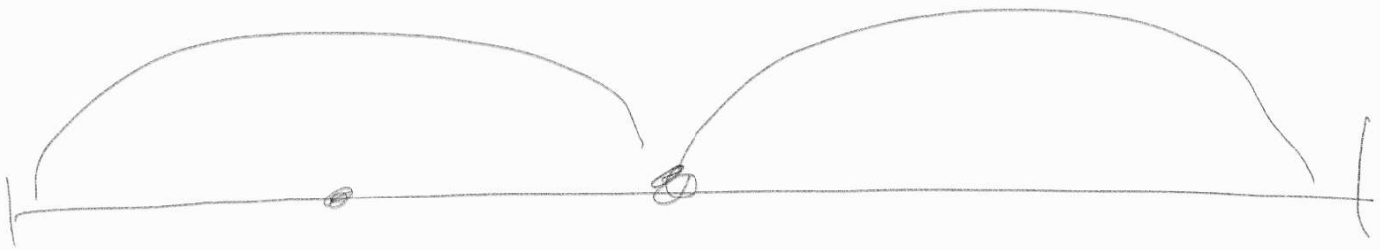
<u>Д-во</u>

~~X~~ $= \{ (y, a) \mid \exists w : w \leq a;\ \Pi(y, w) = 1 \}$

$X \in NP$

$\Pi \leq_{PT} X$ $\Pi(y, w) = 1$

бинарный поиск



SAT SAT

$P \neq NP$

$DTime^A[f(n)]$

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

NP^A $\bigcup_{c>0} NTime^A[n^c]$

Бэйкер, Гилл, Соловей

Теорема

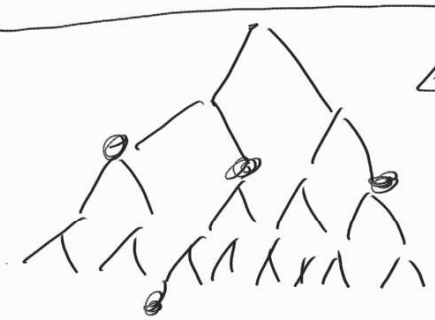
$\exists A, B$:

1) $P^A = NP^A$
2) $P^B \neq NP^B$ ✓

Д-во $EXP = \bigcup_{c>0} DTime[2^{n^c}]$

ExpComp - полный относительно $\leq_p$ языка в EXP

$EXP \subseteq P^{ExpComp} \subseteq NP^{ExpComp} \subseteq EXP$



q_{yes}

$p(n)$

$2^{p(n)}$

$2^{p(n)} \cdot 2^{q(n)}$

$\downarrow$

$2^{poly(n)}$