Т. Бэйкер, Гилл, Соловэй

$\exists A, B$

(1) $P^A = NP^A$

(2) $P^B \neq NP^B$

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

$U_B = \{1^n \mid \exists x \in \{0,1\}^n \cap B\}$

$U_B \in NP^B$

$1^n \quad x \in \{0,1\}^n$

Цель: построить такой B: $U_B \notin P^B$.

$\mathbb{N} \leftrightarrow \Sigma^*$

$M_1, M_2, \ldots$ — нум-я оракульных М.Т., каждая корректная М.Т. встречается ∞ число раз

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

$EXPComp \in EXP$

полный в EXP $\leq_p$

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

$EXPComp = \{(M, x, t) \mid M$ приним. x за t шагов$\}$

ДМТ.

(M, x, t)

$L \in EXP$, L расп. М.Т. M за 2^{n^c} шагов

$L \leq EXPComp \leftarrow$ в бин. виде

$x \mapsto (M, x, 2^{n^c})$

Будем определять язык B так, чтобы $M_k^B(1^k)$ неправильно распознавала U_B за $\leq 2^k/10$ шагов.

$B := \emptyset \qquad M_1^B(1^1) \quad M_2^B(1^2) \ldots$

Для всех $k = 1$ до ∞

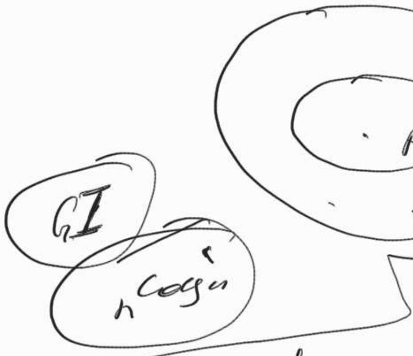
- $M_k^B(1^k)$ на $2^k/10$ шагов
  - если ответ 1, то $B \cap \{0,1\}^k = \emptyset$
  - если ответ 0, то мы добавим в B строку из $\{0,1\}^k$, к которой еще не обращались.

Всего обращений к B было $\leq$

$2^1/10 + 2^2/10 + \ldots + 2^{k-1}/10 + 2^k/10 < 2^k$

Утв. $U_B \notin P^B$. От противного. машина M за время n^c с оракулом B распозн. U_B. $M = M_i$ при этом $\underbrace{2^i/10} > \underbrace{i^c}$.

$$M_i^B(1^i) \neq U_B(1^i).$$



Теорема (Ладнер) Если $P \neq NP$, то $\exists$ язык $L \in NP \setminus P$: L не явл. NP-полным.

$M_1, M_2, \ldots$

$$SAT_H = \{ \underbrace{\varphi}\,0\,\underline{1^{n^{H(n)}}} \mid \varphi \in SAT,\ |\varphi| = n \}$$

$H(n)$ определяется через $H(m)$ при $1 \le m \le \log n$

$H(n)$ — это наименьшее такое число $i < \log\log n$: $\forall x \in \{0,1\}^*: |x| \le \log n$ машина $M_i(x)$ верно выдаёт $SAT_H(x)$ за $\le \underbrace{i|x|^i}$ шагов; если такого i не нашлось то $H(n) = \log\log n$.

- $H(n)$ вычислимо за $poly(n)$ шагов.

$H(1), H(2), \ldots, H(n-1)$

$$\underbrace{O(\log\log n)} \cdot \underbrace{(2n)} \cdot \underbrace{\log\log n} \cdot (\log n)^{\log\log n} \cdot n = \bar{o}(n^3)$$

За $\bar{o}(n^4)$ можно посчитать $H(n)$

Утв. 1) Если $SAT_H \in P$, тогда $H(n) = O(1)$

2) Если $SAT_H \notin P$, тогда $H(n) \to \infty$

Д-во 1) $\exists M$, кот. решает SAT_H за время $\le c \cdot n^c$ $\exists i > c$! M_i совп. с M.

$\Rightarrow H(n) \le i \quad \forall n$

2) $H(n) \nearrow$

Пусть $H(n) = i$ при всех дост. больших n. $\Rightarrow$ M_i реш. SAT_H на всех входах за время $i n^i$, $\Rightarrow SAT_H \in P$

$\exists\, SAT_H \in P \Rightarrow H(n) \le C$

$SAT_H = \{ \varphi\, 0\, 1^{n^{H(n)}} \mid \varphi \in SAT,\ |\varphi| = n \}$

$\varphi \mapsto \varphi\, 0\, 1^{n^{H(n)}}$

$\left.\begin{array}{l} SAT \le_p SAT_H \\ SAT_H \in P \end{array}\right\} \Rightarrow SAT \in P \Rightarrow$

$\Rightarrow P = NP$

SAT_H — NP-полный. f - сведение SAT к SAT_H. Пусть f вычисляется за $\le n^c$ шагов. Т.к. $SAT_H \notin P \Rightarrow H(n)$ не огр. $\Rightarrow$

$\exists n_0: \forall n > n_0 \quad H(n) > 3C$.

Тогда при достаточно больших n

$f: \varphi \mapsto \psi\, 0\, 1^{\underbrace{k^{H(k)}}_{> n^c}}$, где $k = |\psi|$

$|\varphi| = n$

$|f(\varphi)| \le n^c \Rightarrow k \le n^{1/3}$

Т.к. $\varphi \mapsto \psi \qquad |\psi| \le |\varphi|^{1/3}$

$\varphi \mapsto \psi \mapsto \psi' \mapsto \ldots \quad \le n_0$

$\log n \cdot C$

SAT_H — NP-полн $\Rightarrow SAT \in P \Rightarrow P = NP$

$\square$

---

§ Иерархия по времени

Пример. $DTime[n^2] \subsetneq DTime[n^3]$

Д-во $L = \{ M \mid \langle M \rangle (M)$ не принимает за $\le |M|^{2.5}$ шагов $\}$

дет машина Тьюринга

$L \in PTime[n^3]$ $\qquad O(|x|^{2.5} \cdot \log|x|)$

$= O(n^3)$

$L \notin PTime[n^2]$ Пусть M – это машина Тьюринга, кот. реш. L за $C \cdot n^2$ шагов.

$\exists$ описание машины M такой длинное, что $C \cdot |M|^2 < |M|^{2.5}$

$M \overset{?}{\in} L \to$ да $\langle M \rangle (M) = 1$ за $< |M|^{2.5}$ шагов $\Rightarrow M \notin L$

$\to$ нет $\Rightarrow \langle M \rangle (M) = 0$ за $< |M|^{2.5}$ шагов $\Rightarrow M \in L$

Опр. $f: \mathbb{N} \to \mathbb{N}$ назыв. конструкт. по времени, если по n можно вычислить $f(n)$ за $O(f(n))$ шагов

$n^c \quad c \in \mathbb{Q} \qquad \log n, \quad n \log n, \ldots$

Теорема $h(n)$ – конструкт. по времени

ф-ции f, g: $\quad f(n) = o(h(n))$

$h(n) \cdot \log h(n) = \bar{o}(g(n))$

Тогда $DTime[f(n)] \subsetneq DTime[g(n)]$.

<u>Сл-ие</u> $P \subsetneq EXP$

$$P \subseteq DTime[2^n] \subsetneq DTime[2^{n^2}] \subseteq EXP$$

$$\underbrace{P \subseteq NP}\subseteq EXP$$

<u>Теорема об иерархии для недетерм. вычисл.</u>

<u>Пример</u> $NTime[n^2] \subsetneq NTime[n^3]$

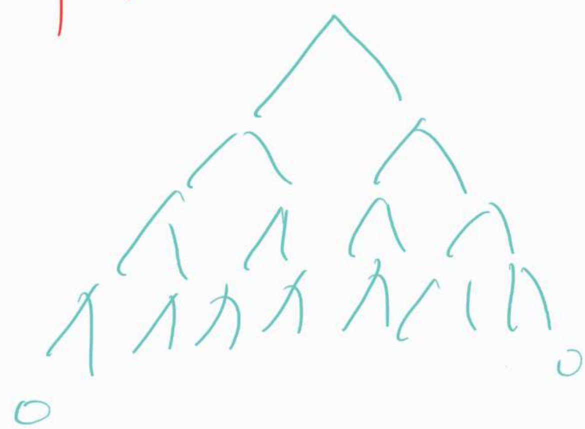
не детерм. М.Т.

$L = \{ M \mid \langle M\rangle(M)$ ~~не~~ принимает за $\leq |M|^{2.5}$ шагов $\}$

НЕ РАБОТАЕТ

$L \in NTime[n^3]$

$L \notin NTime[n^2]$ ✓



M_1, M_2 — — — — НМТ.

M_i $[\, n_i \xrightarrow{\ 1\ } n_i^* \,]$

$n_i^* = 2^{n_i^{(e)}}$

$n_1 \qquad n_1^* \quad n_2 \qquad\qquad n_2^*$

$n_1 = 1 \qquad n_i^* = 2^{n_i^{2.5}} \qquad n_{i+1} = n_i^* + 1$

$L \subseteq \{1\}^* \qquad 2^{n_i^{2.5}}$

1^n

$n_i \le n \le n_i^*$

- Если $n = n_i^*$, тогда

$$L(1^{n_i^*}) = \begin{cases} 1, & \text{если } M_i(1^{n_i}) \text{ отвергает за } \le n_i^{2.5} \text{ шагов} \\ 0, & \text{иначе} \end{cases}$$

$2^{n_i^{2.5}}$

- $n_i \le n < n_i^*$

$$L(1^n) = \begin{cases} 1, & M_i(1^{n+1}) \text{ прин. за } \le n^{2.5} \text{ шагов} \\ 0, & \text{иначе.} \end{cases}$$

$n_i \rightsquigarrow \rightsquigarrow \rightsquigarrow \rightsquigarrow \Rightarrow n_i^*$

$L \in NTime[n^3]$ V

$L \notin NTime[n^2]$?

От противного. Пусть $L \in NTime[n^2]$ M реш.

$M = M_i$ при $n > n_i$

2.5

M_i раб. $< n$

$M_i(1^{n_i}) = L(1^{n_i}) = M_i(1^{n_i+1}) =$

$= L(1^{n_i+1}) = M_i(1^{n_i+2}) = \ldots =$

$= L(1^{n_i^*}) \neq M_i(1^{n_i})$

Теорема $h(n)$ – конструкт. по времени ф-ция, $f(n), g(n)$

$f(n) = \bar{o}(h(n))$, $h(n+1) = \bar{o}(g(n))$

Тогда $NTime[f(n)] \subsetneq NTime[g(n)]$

$n^2 = f(n)$ $n^3 = g(n)$ $h(n) = n^{2.5}$