Complexity II: Random.

Теорема о временной иерархии

Теорема $\mathcal{D}\,Time(f) \subsetneq \mathcal{D}\,Time(f \log^2 f)$

Пусть f - time-constructible

$\Updownarrow$

$f(n)$ можно вычислить за $O(f(n))$

Различие про диагонализацию

Теорема $|\mathbb{N}| \neq |2^{\mathbb{N}}|$

Д-во: Пусть $|\mathbb{N}| = |2^{\mathbb{N}}|$

x_1 0 1 0 1 0 1 0 0 0 1 0 0 1 0

x_2 1 0 1 0 0 0 0 . . . . .

x_3 1 1 0 1 1 1 1 1 ⟷ $y = 1\,1\,0\,0 \ldots$

x_4 1 0 1 1 0 1 0 . .

$y_i := \neg[x_i]_i$

$2^{\mathbb{N}} \ni y \neq x_i \quad \forall i$

$\Rightarrow$ y не пронумерован.

Противоречие.

Universal Turing Machine

Теорема: $\exists$ М.Т. M которая по входу $(\tilde{M}, x)$ вычисляет вывод $\tilde{M}(x)$, при чём если $\tilde{M}$ работает T времени, то M работает за $O(T \log T)$

$\leq C T \log T$

C - функция от $\tilde{M}$, но не x.

$DTime(n) \subsetneq DTime(n^{1.5})$

$L \in DTime(n^{1.5})$,

$L \notin DTime(n)$

α_1 0
α_2 1
α_3 01
α_4 10
α_5 11
α_6 00
α_7 100
α_8 011

M_i = М.Т. построенная из строки α_i

$\alpha_i \in L$, если $M: (\alpha_i) = 0$ (*) (неправда)

Тогда получилось бы, что никакая M_i не распознает L

$\alpha_i \in L$?

Запустим M_i на входе α_i с таймером $= n^{2.4}$ шагов.

$\alpha_i \notin L$ $\alpha_i \in L$ невозможно $\alpha_i \in L$ или $\alpha_i \notin L$

Утв 1: Язык L можно распознать за $O(n^{1.5})$ $L \in DTime(n^{1.5})$

$$n^{1.4} \log(n^{1.4}) = O(n^{1.5})$$

из ИТМ.

Утв 2: Язык L нельзя распознать за $O(n)$ $L \notin DTime(n)$

Д-во: Пусть $L \in DTime(n)$ и M_i распознаёт L за $O(n)$

Тогда

L распознаётся верно

$$[\alpha_j \in L] = M_i(\alpha_j) \quad \forall \alpha_j$$

Теперь рассмотрим $M_i(\alpha_i)$

А если M_i успело отработать за таймер, то

$[\alpha_i \in L] \overset{def}{=} \neg[M_i(\alpha_i)]$

$\times$ противоречие.

В M_i не успело отработать. $O(n)$ $n^{1.4}$

M_i работает за $O(n)$,

симуляция M_i работает за $O(n \log n)$ f_U

$\exists n_0 \; \forall n \geq n_0 \quad f(n) \leq n^{1.4}$

т.к. $n \log n = o(n^{1.4})$

То рассмотрим теперь

другую задачу нашим M_i,

такая что эта задача решается

n_0

и придём к противоречию.

Алгоритмическая неразрешимость задача.

1936 Тьюринг.

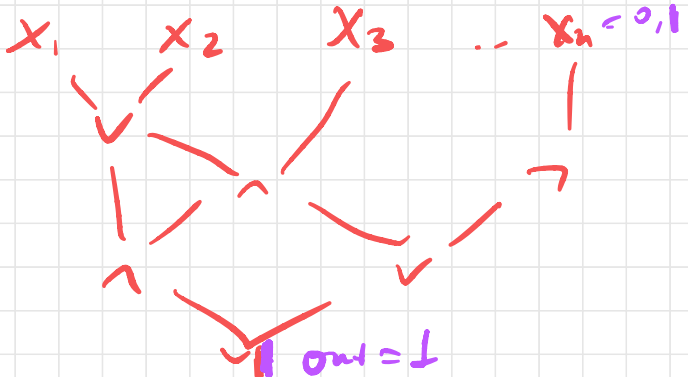
HALTING - PROBLEM.

(M, x) — машина и вход, проверка на, что $M(x)$ останавливается.

Теорема Кука (Cook)

Теорема: CIRCUIT-SAT $\in$ NPhard

Утв: SAT $\in$ NPhard, потому что CIRCUIT-SAT $\in$ SAT.



Д-во теоремы:

CIRCUIT-SAT ∈ NPand

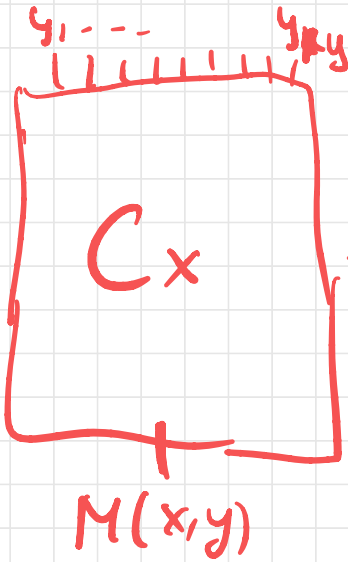
⇕

$\forall L \in NP \quad L \leq$ CIRCUIT-SAT

↑ ЭМ решающая L.

$(x \in L) \Leftrightarrow (\exists y : M(x,y))$

$|y| \leq poly(|x|)$

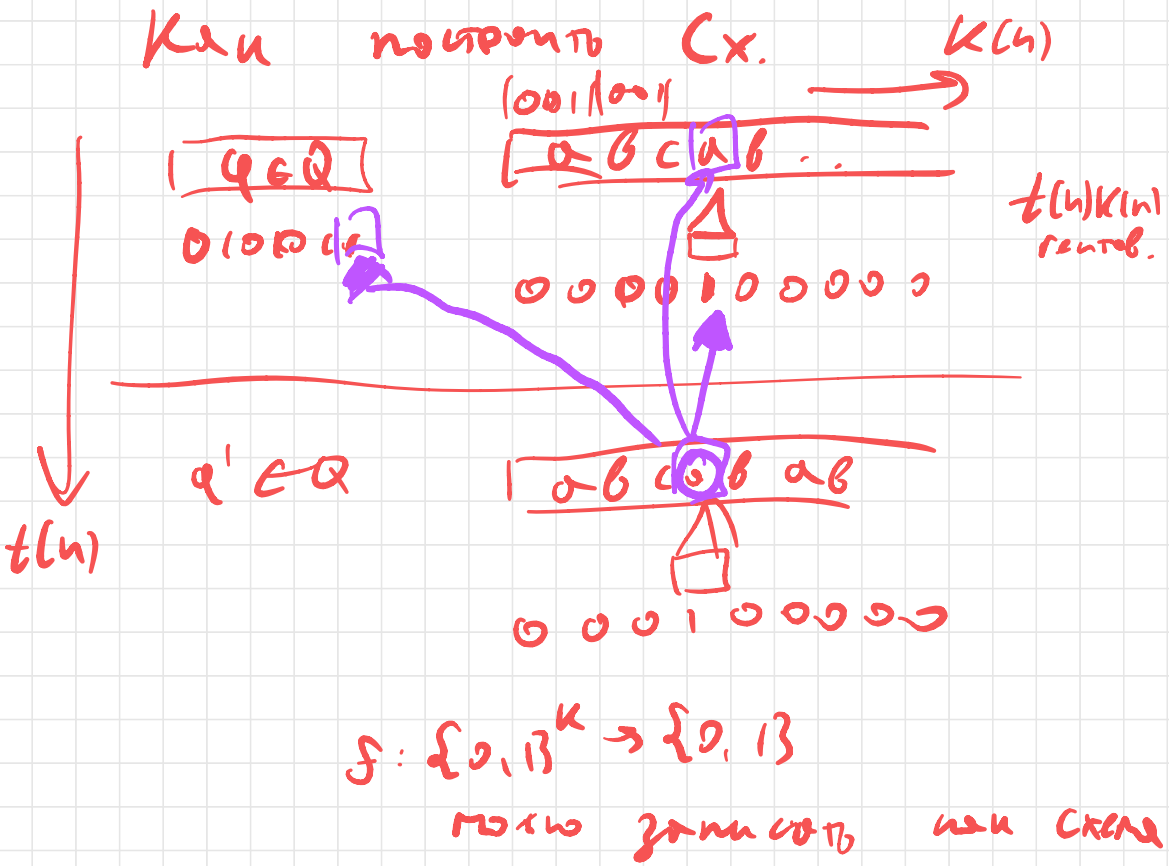


— схема;

poly(|x|) размера.

$x \in L \Leftrightarrow C_x \in$ CIRCUIT-SAT

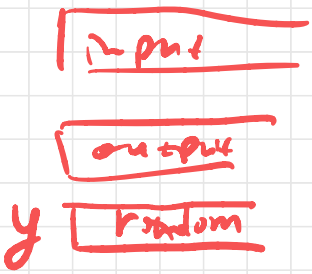
т.е $x \to C_x$ это полином. сведение.



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

можно записать как схему

Вероятностные алгоритмы.



} М.Т. с лентой случайности

Def (RP)

$L \in RP \Leftrightarrow \exists M:$

$$\begin{cases} \forall x \in L & P_y[M(x,y)=1] \geq \frac{1}{2} \\ \forall x \notin L & P_y[M(x,y)=0] = 1 \end{cases}$$

Def: coRP.

$L \in coRP: \exists M$

$$\begin{cases} \forall x \in L & P_y[M(x,y)=1] = 1 \\ \forall x \notin L & P_y[M(x,y)=0] \geq \frac{1}{2} \end{cases}$$

Def: BPP (огран. ошибка)

$L \in BPP$ $\exists M$:

$$\begin{cases} \forall x \in L : \underset{y}{P}[M(x,y)=1] \geq \frac{2}{3} \\ \forall x \notin L : \underset{y}{P}[M(x,y)=0] \geq \frac{2}{3} \end{cases}$$

Утв: Понижение ошибки в RP.

повторим алг k-раз

$$\begin{cases} \forall x \in L & \underset{y}{P}[M(x,y)=0] \geq 1 - \frac{1}{2^k} \\ \forall x \notin L & \underset{y}{P}[M(x,y)=0] = 1 \end{cases}$$

Аналогично с coRP.

Утв Понижение ошибки в BPP.

Повторим $f(\varepsilon)$ раз

$\forall \forall \forall \forall \forall \to \forall$

$f: [0;1] \to \mathbb{N}$

$$\begin{cases} \forall x \in L : \ P_y[M(x,y)=1] \geq 1-\varepsilon \\ \forall x \notin L : \ P_y[M(x,y)=0] \geq 1-\varepsilon \end{cases}$$

ч.т.д.: $RP \subseteq NP$

RP: $\begin{cases} \forall x \in L & P_y[M(x,y)=1] \geq \frac{1}{2} \\ \forall x \notin L & P_y[M(x,y)=0] = 1 \end{cases}$

NP: $\begin{cases} \forall x \in L & \exists y: M(x,y)=1 \\ \forall x \notin L : & \forall y: M(x,y)=0. \end{cases}$

$RP \subseteq NP$,

потому что $\forall x \in L \in RP$ $\Rightarrow$ $L \in NP$

можно взять любой

из 50% y и x или y

сами подсказку

в NP.

50%: хорошие $\Rightarrow \geq 1$ хороших.

Def: ZPP.

$L \in ZPP$: $M(x,y) = [x \in L]$

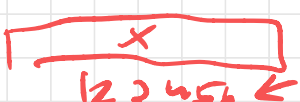
$\mathop{E}_{y}$ [время работы $M(x,y)$] $\leq poly(|x|)$.

Пример:

Quicksort: вероятность в среднем класса ZPP

Primality Test.

PRIME



$x \in PRIME$, если

x - запись простого числа.

$PRIME \in coRP$. '70

$PRIME \overset{?}{\in} P$ 2002

Agrawal, Kayal, Saxena

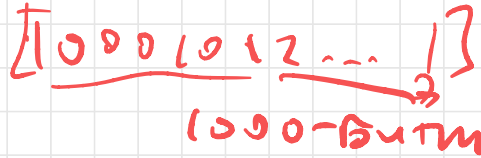
"PRIME IS IN P"

n∈PRIME? $\tilde{O}(\log^6 n)$

длина n равна $\log(n)$,

поэтому $\text{poly}(\log(n))$.

Практические прим. в КВиПТ:



1000-битные.

Миллер-Рабин.

М. Теорема Ферма: p – простое.

$\forall a \in [1, p-1] \quad a^{p-1} = 1 \mod p$

$([\forall a \in \Sigma 0, p] \quad a^p = a \mod p)$

Тест на простоту:

Алгоритм: вход p.

$a \leftarrow U[1; p-1]$

$a^{p-1} = 1 \mod p$?

$= 1$ ↙ Наверно простое

$\neq 1$ ↘ Точно не простое

Числа Кармайкла:

Эф: q - не простое

$\forall a \in [1, q-1]: \quad a^{q-1} = 1 \mod q$

$\simeq 300$

Тест Миллера-Рабина.

$p-1 = 2^s d$ $\quad d$ — нечётное

Пусть p нечётное

$a \leftarrow U[1, p-1]$

Тест Ферма: a^{p-1}

Тест Миллера-Рабина: $a^d \quad a^{2d} \quad \dots \quad a^{2^s d}$

a^{p-1}

$a^{p-1} \stackrel{?}{=} 1 \pmod p$

$=1$ ↓ $\quad \neq 1$ → не простое.

$a^{\frac{p-1}{2}} = ?$

$=1$ ↓ $\quad =-1$ ↓ $\quad \neq \pm 1$ → не простое.

Стоп, наверно простое

$a^{\frac{p-1}{4}} = ?$

$a^{p-1} = 1 \pmod p$

$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1$

$x^2 = 1$

⇓

В поле: $x = 1$ или $x = -1$

Утв: p - простое

$a^{(p-1)/2} = \pm 1$

$p \in PRIME \quad \Pr_y[M(p,y) = 1] = 1$

$p \notin PRIME \quad \Pr_y[M(p,y) = 1] \leq \frac{1}{2} \leq 2^{-k}$

k - длина числа

$PRIME \in coRP$

$\tilde{O}(\log^3 n)$