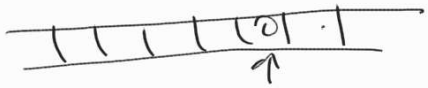
§ Вероятностные классы сложности

Вероятностная М.Т.

– $\delta_{0,1} : \underbrace{Q \times \Sigma^k}_{q_{yes},\ q_{no} \in Q} \to Q \times \Sigma^k \times \{\leftarrow, ;, \rightarrow\}$

– лента случ. битов. $\longrightarrow$



BPP (bounded error probabilistic polynomial)

$L \in BPP \iff \exists$ вероятн. М.Т. M $\exists$ полином p:

- $\forall x$ $\forall$ посл. случ. битов $M(x)$ работает $\leq p(|x|)$ шагов.
- $\forall x$ $\Pr_{\text{по случ. битам}}[M(x) \neq L(x)] \leq \underbrace{1/3}$

RP (randomized polynomial) полин. вероятн. алгоритмы с одност. ошибкой.

$L \in RP \iff \exists$ вер. МТ. M и полином p:

- $\forall x$ $\forall$ посл. сл. битов $M(x)$ раб. $\leq p(|x|)$ шагов
- $\forall x \in L$ $\Pr[M(x)=1] \geq \frac{1}{2}$

$\forall x \notin L$ $\Pr[M(x)=1] = 0$

$$P \subseteq RP \subseteq BPP$$

$$\subseteq NP \quad \cdots$$

$$\boxed{P = BPP}$$

NW

$f \in DTime[2^{cn}]$

$f \notin Size[2^{c'n}]$

3-SAT

Primes $\in coRP$

$\in P$

Лемма (Шварц – Зиппель) $p \in \mathbb{F}[x_1, x_2, \dots, x_\ell]$

$\mathbb{F}$ – конечное поле. $\deg p \le d$. $p \not\equiv 0$.

Тогда
$$\Pr_{a_1, a_2, \dots, a_\ell \in \mathbb{F}} \left[p(a_1, a_2, \dots, a_\ell) \ne 0 \right] \ge 1 - \frac{d}{|\mathbb{F}|}$$

Д-во Индукция по ℓ.

База $\ell = 1$ $\quad \Pr[p(a) \ne 0] \ge \frac{|\mathbb{F}| - d}{|\mathbb{F}|} = 1 - \frac{d}{|\mathbb{F}|}$

Переход $p(x_1, x_2, \dots, x_\ell) = \sum_{i=0}^{d} x_1^i \, p_i(x_2, x_3, \dots, x_\ell)$

Пусть k – наибольшее целое число, что

$p_k \not\equiv 0$. $\deg p_k \le d-k$

По индукц. предположению
$$\Pr_{a_2, a_3, \dots, a_\ell} [p_k(a_2, a_3, \dots, a_\ell) \ne 0] \ge 1 - \frac{d-k}{|\mathbb{F}|}$$

$$\Pr[p(a_1, \dots, a_\ell) \ne 0] \ge \Pr[p(a_1, \dots, a_\ell) \ne 0 \mid p_k(a_2, \dots, a_\ell) \ne 0] \cdot$$
$$\cdot \Pr[p_k(a_2, a_3, \dots, a_\ell) \ne 0] \ge \left(1 - \frac{k}{|\mathbb{F}|}\right)\left(1 - \frac{d-k}{|\mathbb{F}|}\right) \ge$$
$$\ge 1 - \frac{d}{|\mathbb{F}|}.$$

$$\underbrace{(x - y)(z - f) \quad (e - f) \dots}_{m}$$

$\mathbb{F}_q$ $\quad q >> m$

$$1 - \frac{m}{q}$$

P — Q

Лемма $f: \{0,1\}^n \to \{0,1\}$

$\forall$ поле $\mathbb{F}$ f имеет единств. представл. в виде мультилин. мн-на над $\mathbb{F}$.

$\mathbb{F} = \{0, 1, \dots, -1\}$

Д-во $\exists$ $a_1 \dots a_n$

$(x_1 - a_1 + 1)(x_2 - a_2 + 1) \dots (x_n - a_n + 1) = \chi_{a_1 \dots a_n}$

$$\sum_{a \in \{0,1\}^n} \chi_a \cdot f(a)$$

! p - мультилин. мн. $p \equiv 0$ на $\{0,1\}^n$, то p - это тождественный 0

Индукция по числу переменных

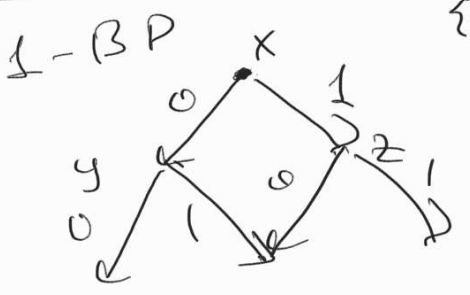
$x_1 q(x_2, \dots, x_n) + r(x_2, \dots, x_n)$

$q + r \equiv 0$

$r \equiv 0$

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

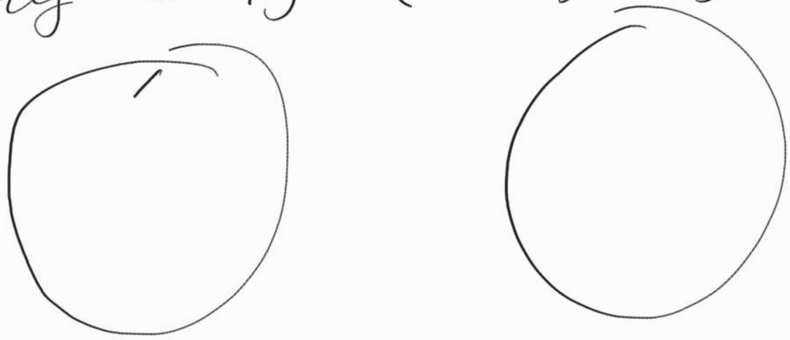
1-BP



1-BP: $\forall$ пути каждая переменная встреч. ≤ 1 раза

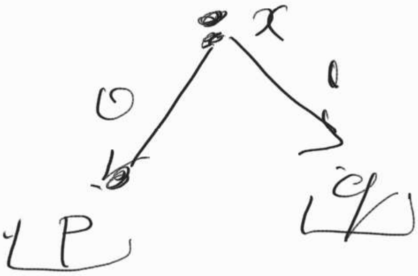
0 1

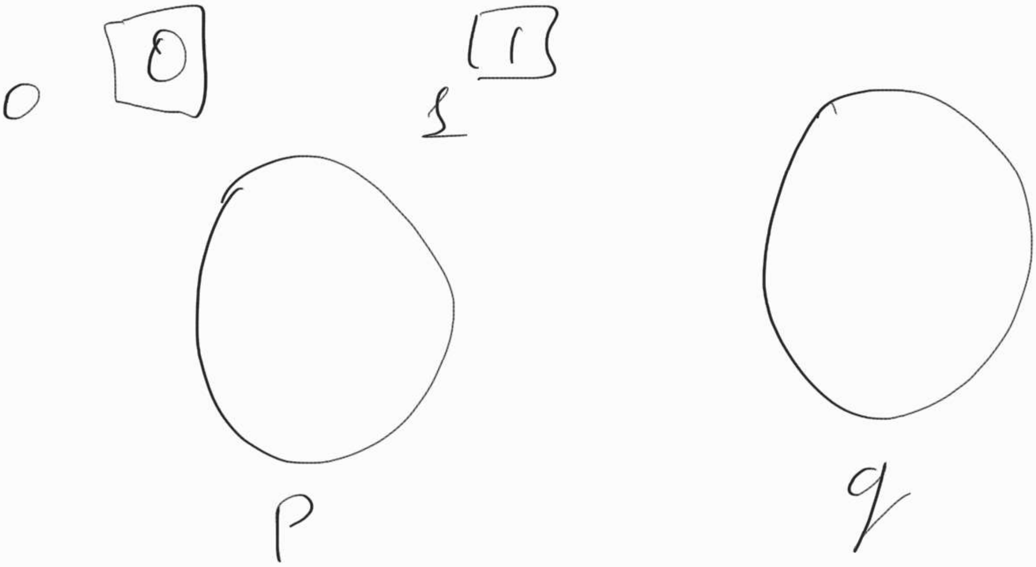
∃ полин. по вр. вер. алг. с огр. ошибкой, кот. проверяет, что две 1-ВР вычисляют одну и ту же функцию.



Мультилинейные мн-ы по 1-ВР

$(1-x)q + xp$





$\deg p \le n$

$\deg q \le n$

$$|F| \ge n^2$$

$$1 - \frac{n}{n^2} \ge 1 - \frac{1}{n}$$

Факт (Оценки Чернова в аддитивной форме)

$X_1, X_2, \ldots, X_n$ один. распр. независ. случ. величины $X_i \in \{0, 1\}$. $E[X_i] = \mu$

Тогда $\forall \varepsilon > 0$ $\Pr\left[\left|\frac{\sum X_i}{n} - \mu\right| \geq \varepsilon\right] \leq 2e^{-2\varepsilon^2 n}$

Теорема Если $L \in BPP$. Тогда $\forall$ полинома $m(n)$ $\exists$ вероятн. полин. по врем. МТ M!

$\forall x$ $\Pr[M(x) \neq L(x)] \leq 2^{-m(n)}$

Д-во Запустим $N = 18m(n) + 1$ независ. копий обычных машин и выдадим самый частый ответ

$X_i = 1$, если i-ый запуск дал верный ответ

$\mu = E[X_i] \geq \frac{2}{3}$

$\Pr\left[\sum_{i=1}^{N} X_i \leq \frac{1}{2}N\right] \leq \Pr\left[\left|\frac{\sum X_i}{N} - \mu\right| \geq \frac{1}{6}\right] \leq$

RSA

$\leq e^{-\frac{1}{18}N} < 2^{-m(n)}$

Теорема $BPP \subseteq P/poly$ (A_днемен)

Д-во $L \in BPP$. По пред. т-ме $\exists$ пол. по вр. вер M: $\forall x$ $\Pr[M(x) \neq L(x)] \leq \frac{1}{2^{n^2}}$

$n = |x|$

x доля плохих сл. битов

$\frac{1}{2^{n^2}}$

2^n $\leq \frac{2^n}{2^{n^2}} \ll 1$

$\exists$ пол-сть случ. битов ! с ней

M дает правильный ответ
на входе длины n.

$L \in P/poly(n) = P/poly$

$NP \subseteq BPP \subseteq P/poly \Rightarrow$

по теореме Карпа-Липтона

$PH = \Sigma_2^P$

Теорема (Сипсер – Гач) $BPP \subseteq \Pi_2^P \cap \Sigma_2^P$

Д-во Достаточно д-ть $BPP \subseteq \Sigma_2^P$

$L \in BPP$ $\exists$ веер. полин. по вр. маш. Тьюринга M:

$\forall x \quad Pr[L(x) \neq M(x)] \leq 2^{-n} \quad n = |x|$

$\exists$ на входах длины n M исп. $m(n)$ (полином) случ. битов

$S_x \subseteq \{0,1\}^{m(n)}$ – мн-во случ. битов, длея которых машина на входе x выдает 1.

$x \in L \quad |S_x| \geq 2^{m(n)} \cdot (1 - 2^{-n})$

$x \notin L \quad |S_x| \leq 2^{m(n)} \cdot 2^{-n}$

$k = \lceil \frac{m}{n} \rceil + 1$

Тогда

Лемма $S \subseteq \{0,1\}^m$

1) Если $|S| \leq 2^{m-n}$, то $\forall x_1, x_2, \dots, x_k \in \{0,1\}^m$

$(x_1 + S) \cup (x_2 + S) \cup \dots \cup (x_k + S) \neq \{0,1\}^m$

2) Если $|S| \geq 2^m (1 - 2^{-n})$, то $\exists x_1, x_2, \dots, x_k \in \{0,1\}^m$

$(x_1 + S) \cup (x_2 + S) \cup \dots \cup (x_k + S) = \{0,1\}^m$

$x \in L \Leftrightarrow \exists S_1, S_2, \dots, S_k \quad \forall r \in \{0,1\}^{m(n)}$

$$r \in \bigcup_{i=1}^{k} S_x + S_i$$

$$\bigvee_{i=1}^{k} \; r \in S_x + S_i$$

$$\bigvee_{i=1}^{k} \; \underbrace{r + S_i \in S_x}$$

$$x \in L \Leftrightarrow \exists S_1, \dots, S_k \; \forall r : \bigvee_{i=1}^{k} \; \mu(x) = 1_{r+S_i}$$

$$L \in \Sigma_2^p$$

$k = \lceil \frac{m}{n} \rceil + 1$ Torga $\qquad m < 2^n$

Лемма $S \subseteq \{0,1\}^m$

1) Если $|S| \le 2^{m-n}$, то $\forall x_1, x_2, \dots, x_k \in \{0,1\}^m$
$(x_1 + S) \cup (x_2 + S) \cup \dots \cup (x_k + S) \neq \{0,1\}^m$

2) Если $|S| \ge 2^m (1 - 2^{-n})$, то $\exists x_1, x_2, \dots, x_k \in \{0,1\}^m$
$(x_1 + S) \cup (x_2 + S) \cup \dots \cup (x_k + S) = \{0,1\}^m$

Д-во 1)

$$\left| \bigcup_{i=1}^{k} (x_i + S) \right| \le k \cdot |S| \le 2^{m-n} \cdot \left(\lceil \frac{m}{n} \rceil + 1 \right) <$$

$$< 2^m \qquad \underline{\frac{m(n)}{n} + 1 < 2^n}$$

2) Выберем $x_1, \dots x_k$ случайно и независимо.

$t \in \{0,1\}^n$

$$\Pr\left[t \notin S + x_1\right] = \Pr\left[x_1 \notin S + t\right] \le$$

$$\le 2^{-n}$$

$$\Pr\left[t \notin S + x_1,\ t \notin S + x_2,\ \dots,\ t \notin S + x_k\right]$$

$$\le 2^{-n-k}$$

$$\Pr\left[\exists t:\ t \notin \bigcup_{i=1}^{k} (S + x_i)\right] \le 2^{-n \cdot k} \cdot 2^n < 1$$