Введение в теорию сложности вычислений

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

СПбГУ и ПОМИ РАН

лекция 17 декабря 2020 г.

Односторонняя ошибка:
$L \in$ **NP**, если имеется п.о. п.п. R, такое, что $\forall x \in \{0,1\}^*$

$$x \notin L \quad \Rightarrow \quad \forall w \; (x, w) \notin R,$$
$$x \in L \quad \Rightarrow \quad \exists w \; (x, w) \in R.$$

Классы ZPP, RP, BPP

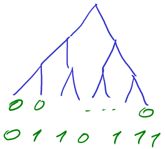
Вероятностные вычисления с ограниченной вероятностью ошибки

Односторонняя ошибка:

$L \in$ **RP**, если имеется п.о. п.п. R, такое, что $\forall x \in \{0,1\}^*$

$$x \notin L \quad \Rightarrow \quad \forall w\ (x, w) \notin R,$$

$$x \in L \quad \Rightarrow \quad \frac{|\{w \mid (x, w) \in R\}|}{\underbrace{|\{\text{всех } w\}|}_{\sim 2^{p(n)}}} > \frac{1}{2}.$$



$x \notin L$

$x \in L$

Классы ZPP, RP, BPP

Вероятностные вычисления с ограниченной вероятностью ошибки

Односторонняя ошибка:

$L \in$ **RP**, если имеется п.о. п.п. R, такое, что $\forall x \in \{0,1\}^*$

$$\begin{aligned} x \notin L &\Rightarrow \forall w\ (x, w) \notin R, \\ x \in L &\Rightarrow \frac{|\{w \mid (x, w) \in R\}|}{|\{\text{всех } w\}|} > \frac{1}{2}. \end{aligned}$$

Без ошибки:

ZPP $=$ **RP** $\cap$ **co-RP**

Классы ZPP, RP, BPP

Вероятностные вычисления с ограниченной вероятностью ошибки

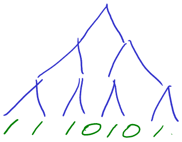
Односторонняя ошибка:

$L \in$ **RP**, если имеется п.о. п.п. R, такое, что $\forall x \in \{0,1\}^*$

$$x \notin L \;\Rightarrow\; \forall w\ (x, w) \notin R,$$

$$x \in L \;\Rightarrow\; \frac{|\{w \mid (x, w) \in R\}|}{|\{\text{всех } w\}|} > \frac{1}{2}.$$

BPP



$\geq 2/3$

000001001 $< 1/3$

Без ошибки:

ZPP $=$ **RP** $\cap$ **co-RP**

Двусторонняя ошибка:

$L \in$ **BPP**, если имеется п.о. п.п. R, такое, что $\forall x \in \{0,1\}^*$

$$x \notin L \;\Rightarrow\; \frac{|\{w \mid (x, w) \in R\}|}{|\{\text{всех } w\}|} < \frac{1}{3},$$

случ. строка

$$x \in L \;\Rightarrow\; \frac{|\{w \mid (x, w) \in R\}|}{|\{\text{всех } w\}|} > \frac{2}{3}.$$

$P\{R$ принимает$\}$

Понижение вероятности ошибки

RP: повторим k раз (или до первого ответа "да");

напр., $p(n)$

$$\Pr\{k \text{ неудач}\} \leq \frac{1}{2^k}.$$

$x \notin L \Rightarrow Pr = 0$

$x \in L \Rightarrow Pr \geqslant 1 - \frac{1}{2^k}$

Понижение вероятности ошибки

RP: повторим k раз (или до первого ответа "да");

$$\Pr\{k \text{ неудач}\} \leq \frac{1}{2^k}.$$

BPP: повторим k раз и выдадим самый частый ответ;

$$\Pr\{\text{ошибок более } k/2\} \leq 2^{-\Omega(k)}.$$

Понижение вероятности ошибки

RP: повторим k раз (или до первого ответа “да”);

$$\Pr\{k \text{ неудач}\} \le \frac{1}{2^k}.$$

BPP: повторим k раз и выдадим самый частый ответ;

$$\Pr\{\text{ошибок более } k/2\} \le 2^{-\Omega(k)}.$$ ← можно полином

Факт (Chernoff inequality)

$$\Pr\{X > \underbrace{(1+\varepsilon)pk}^{\frac{3}{2}\cdot\frac{1}{3}\cdot k}\} < \left(\frac{e^{\varepsilon}}{(1+\varepsilon)^{1+\varepsilon}}\right)^{pk} \le e^{-\frac{pk\varepsilon^2}{4}},$$

где $X = \sum_{i=1}^{k} x_i$, а x_i — независимые случайные величины, принимающие 1 с вероятностью p и 0 с вероятностью $(1-p)$.

Для нас x_i — наличие ошибки при i-м вычислении, $p = \frac{1}{3}$, $\varepsilon = \frac{1}{2}$.

Понижение вероятности ошибки

RP: повторим k раз (или до первого ответа “да”);

$$\Pr\{k \text{ неудач}\} \leq \frac{1}{2^k}.$$

BPP: повторим k раз и выдадим самый частый ответ;

$$\Pr\{\text{ошибок более } k/2\} \leq 2^{-\Omega(k)}.$$

Альтернативное определение **ZPP**: алгоритмы без ошибки с полиномиальным мат. ожиданием времени работы.

RP 0000

co-RP 1111$\boxed{0}$

E $O\left(\left(\frac{1}{2} + 2\frac{1}{4} + 3\frac{1}{8} + \dots\right) t(n)\right) = O(t(n))$

A $\quad E\, t_A(n) \leq p(n)$

Прервём $\to 1$, $\to 0$

Нер-во Маркова

10р. дольше — он $\frac{1}{10}$

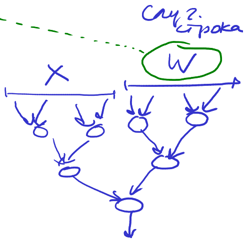
BPP $\subset$ P/poly

$A(x, w) \stackrel{?}{=} x \in L$

Случ. строки одной длины $\le t(n)$

- Для входа x случайная строка может быть “хорошей” (правильный ответ) или “плохой”.
- Можно считать, что доля “хороших” $1 - \frac{1}{4^n}$. ← уменьшим ошибку
- Случайную строку, хорошую для всех $x \in \{0, 1\}^n$, можно зашить в схему.
- Покажем, что такая существует:

$$\frac{1}{4^n} \times 2^n < 1.$$



$\mathrm{BPP} \subseteq \Sigma^2\mathrm{P} \cap \Pi^2\mathrm{P}$

Теорема

$\mathrm{BPP} \subseteq \Sigma^2\mathrm{P}$. $\mathrm{BPP} = \text{co-}\mathrm{BPP}$

R^w

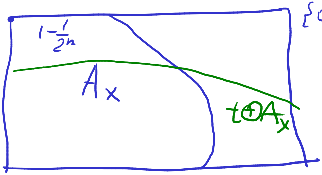
- Пусть вер. ошибки $\frac{1}{2^n}$, $A_x = \{w \in \{0,1\}^{p(n)} \mid R(x, w) = 1\}$.
- Для $x \in L$ можно k копиями A_x покрыть все возможные случайные строки $U = \{0,1\}^{p(n)}$: что

$$\exists \{t_i\}_{i=1}^{k}\ \forall r \in U\ \bigvee_{i=1}^{k} (r \in A_x \oplus t_i), \tag{1}$$

а для $x \notin L$ — нельзя из мощностных соображений.

$\frac{1}{2^n} \times \underbrace{poly(n)}_{= k} < 1$

$t \oplus A_x =$
$= \{t \oplus w \mid w \in A_x\}$



$\{0,1\}^{p(n)}$
все случ. строки

BPP $\subseteq \Sigma^2$P $\cap\ \Pi^2$P

Теорема

BPP $\subseteq \Sigma^2$P.

$R(x, w)$ $x \in \{0,1\}^n$ $w \in \{0,1\}^{p(n)}$ $t_R(n) = p(n)$ полином

- Пусть вер. ошибки $\frac{1}{2^n}$, $A_x = \{w \in \{0,1\}^{p(n)} \mid R(x, w) = 1\}$.
- Для $x \in L$ можно k копиями A_x покрыть все возможные случайные строки $U = \{0,1\}^{p(n)}$: что

$$\exists \{t_i\}_{i=1}^{k}\ \forall r \in U\ \bigvee_{i=1}^{k} (r \in A_x \oplus t_i), \tag{1}$$

  а для $x \notin L$ — нельзя из мощностных соображений.
- Проверка $r \in A_x \oplus t_i$ за полиномиальное время: проверка $r \oplus t_i \in A_x$, т.е. запуск $R(x, r \oplus t_i)$.

$\mathsf{BPP} \subseteq \Sigma^2\mathsf{P} \cap \Pi^2\mathsf{P}$

Теорема

$\mathsf{BPP} \subseteq \Sigma^2\mathsf{P}$.

$p(n)$

- Пусть вер. ошибки $\frac{1}{2^n}$, $A_x = \{w \in \{0,1\}^{p(n)} \mid R(x,w) = 1\}$.
- Для $x \in L$ можно k копиями A_x покрыть все возможные случайные строки $U = \{0,1\}^{p(n)}$: что

$$\exists \{t_i\}_{i=1}^{\overset{p(n)}{\overset{\|}{k}}} \forall r \in U \bigvee_{i=1}^{k} (r \in A_x \oplus t_i), \tag{1}$$

$\forall r \; r \oplus t_i$ равн. распр.

  а для $x \notin L$ — нельзя из мощностных соображений.
- Осталось показать, что это так, т.е. $\exists \{t_i\}_i$. Возьмём их случайно:

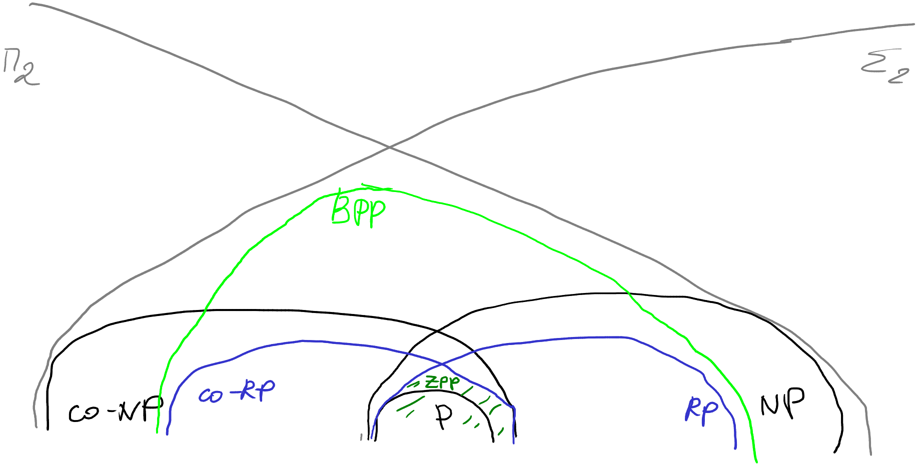
Лемма:

$$\Pr\{\neg(\forall r \in U \bigvee_{i=1}^{k} (r \in A_x \oplus t_i))\} = \Pr\{\exists r \in U \bigwedge_{i=1}^{k} (r \notin A_x \oplus t_i)\} \leq$$

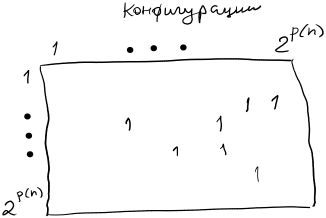
$$\sum_{r \in U} \Pr\{\bigwedge_{i=1}^{k} (r \notin A_x \oplus t_i)\} = \sum_{r \in U} \prod_{i=1}^{k} \underbrace{\Pr\{r \notin A_x \oplus t_i\}}_{1/2^n} \leq \frac{1}{2^{nk}} 2^{p(n)} < 1$$

Классы

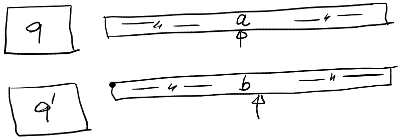
Место для картинки



Вычисления как матрицы
НМТ



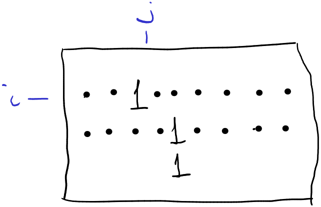
$$A(u,v) = 1 \iff u \xmapsto[M]{1\ \text{шаг}} v$$



$$(q, a) \longmapsto (q', b, \rightarrow)$$

Вычисления как матрицы

ДМТ



одна "1"

$$\sum_j a_{ij} = 1$$

$$i \mapsto j$$

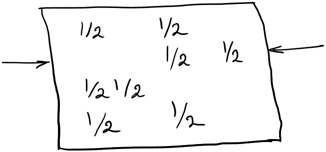
"Эволюция" вектора состояний

$$x = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

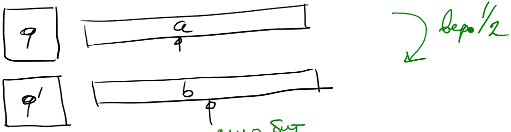
мы здесь

$$x \mapsto Ax \mapsto A^2x \mapsto \dots$$

"Стохастическая матрица"



$$\sum_j a_{ij} = 1$$



Можно думать о "сумме состояний", напр.,

$\frac{1}{2}$ 0000 +

$\frac{1}{2}$ ||||

служ. бит

$$\delta(q, a, 0) = (q', b, \rightarrow)$$
$$\delta(q, a, 1) = (q'', c, \ldots)$$

$$x \mapsto Ax \mapsto A^2 x \mapsto \ldots$$

$$\begin{pmatrix} 0 \\ 1/2 \\ 0 \\ 1/2 \\ 0 \end{pmatrix}$$

мы то ли тут, то ли здесь

BQP

$a_{ij} \in \mathbb{C}$

A унитарная $AA^* = A^*A = E$

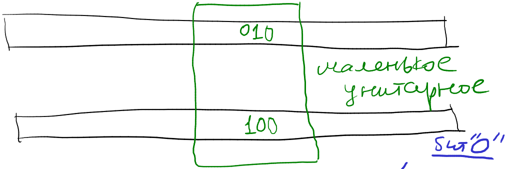
$a^*_{ij} = \overline{a_{ji}}$

Можно обойтись $a_{ij} \in \{0, 1, \pm\frac{3}{5}, \pm\frac{4}{5}\}$

Вместо вероятностей — амплитуды x_i.

Вероятность — $|x_i|^2$.

$$\begin{pmatrix} 1/2 \\ 1/16 \\ -1/16 \\ 0 \end{pmatrix}$$



Смешанное состояние — линейная комбинация чистых (конкретных)

$\sum x_i s_i$ — т.е. с вер. $|x_i|^2$ в s_i

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

1 шаг $\frac{1}{2}$ "0" $\frac{1}{2}$ "1"

2 шага "0"

Квантовые схемы