Структурная теория сложности

Эдуард Алексеевич Гирш

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

ПОМИ РАН

9 ноября 2008 г.

Классы RP, BPP, PP

$L \in \mathbf{NP}$, если имеется п.о. п.п. R, такая, 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 RP, BPP, PP

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

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

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

Классы RP, BPP, PP

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

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

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

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

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

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

Классы RP, BPP, PP

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

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

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

$$x \notin L \quad \Rightarrow \quad \frac{|\{w \mid (x,w) \in R\}|}{|\{\text{всех } w\}|} < \frac{1}{3},$$
$$x \in L \quad \Rightarrow \quad \frac{|\{w \mid (x,w) \in R\}|}{|\{\text{всех } w\}|} > \frac{2}{3}.$$

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

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

Понижение вероятности ошибки

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

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

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;

$$\Pr\{\text{ошибок более } k/2\} \leq \qquad .$$

Факт (Chernoff inequality)

$$\Pr\{X > (1+\varepsilon)pk\} < \left(\frac{e^{\varepsilon}}{(1+\varepsilon)^{1+\varepsilon}}\right)^{pk} \leq e^{-\frac{pk\varepsilon^2}{4}},$$

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;

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

Факт (Chernoff inequality)

$$\Pr\{X > (1+\varepsilon)pk\} < \left(\frac{e^{\varepsilon}}{(1+\varepsilon)^{1+\varepsilon}}\right)^{pk} \leq e^{-\frac{pk\varepsilon^2}{4}},$$

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, $p = \frac{1}{3}$, $\varepsilon = \frac{1}{2}$.

BPP $\subset$ P/poly

- "Хорошая" подсказка для входа x не даёт ошибки.
  Можно считать, что их $1 - \frac{1}{4^n}$.
- Подсказку, хорошую для всех $x \in \{0,1\}^n$, можно зашить в схему.
- Покажем, что такая подсказка существует:

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

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

Теорема

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

- 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 подсказки $U = \{0,1\}^{p(n)}$: 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.

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

Теорема

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

- 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 подсказки $U = \{0,1\}^{p(n)}$: 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 $R(x, r \oplus t_i)$.

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

Теорема

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

- 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 подсказки $U = \{0,1\}^{p(n)}$: 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.
- Осталось показать, что это так, т.е. $\exists \{t_i\}_i$. Возьмём их случайно:

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

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

PP versus #P

$f \in \#\mathbf{P}$, если имеется п.о. п.п. R, такая, что $\forall x \in \{0,1\}^*$

$$f(x) = |\{w \mid (x, w) \in R\}|$$

- $\mathbf{P}^{\mathbf{PP}} = \mathbf{P}^{\#\mathbf{P}}$,
- $\mathbf{NP} \subseteq \mathbf{PP}$,
- в определении $\mathbf{PP}$ константу $\frac{1}{2}$ можно заменить на любую полиномиально вычислимую функцию.

$\mathbf{P}^{\mathbf{PP}} \not\subset \mathbf{Size}[n^k]$

Пусть x_0, x_1, ... — входы размера n.
Строим $L \notin \mathbf{Size}[n^k]$:

- Результат на x_0:

$$\neg \underset{C \in \mathbf{Size}[n^k]}{\mathbf{maj}} C(x_0).$$

- Результат на x_1:

$$\neg \underset{\substack{C \in \mathbf{Size}[n^k] \\ C(x_0)=L(x_0)}}{\mathbf{maj}} C(x_1).$$

- Результат на x_2:

$$\neg \underset{\substack{C \in \mathbf{Size}[n^k] \\ C(x_0)=L(x_0) \\ C(x_1)=L(x_1)}}{\mathbf{maj}} C(x_2).$$

- ...

Всего полиномиальное количество шагов, всё в $\mathbf{P}^{\mathbf{PP}}$.

2-раундовые интерактивные доказательства: **MA**, **AM**.

Язык $L \in \mathbf{MA}$, если имеются такие полиномы p и q и полиномиальная ДМТ A, что $\forall x \in \{0,1\}^*$

$$x \in L \implies \exists y \in \{0,1\}^{p(|x|)} : \Pr_{z \in \{0,1\}^{q(|x|)}} \{A(x,y,z) = 1\} = 1,$$

$$x \notin L \implies \forall y \in \{0,1\}^{p(|x|)} : \Pr_{z \in \{0,1\}^{q(|x|)}} \{A(x,y,z) = 1\} < 1/4.$$

Язык $L \in \mathbf{AM}$, если $\langle \ldots \rangle$

$$x \in L \implies \Pr_{z \in \{0,1\}^{q(|x|)}} \{\exists y \in \{0,1\}^{p(|x|)} : A(x,y,z) = 1\} > 3/4$$

$$x \notin L \implies \Pr_{z \in \{0,1\}^{q(|x|)}} \{\exists y \in \{0,1\}^{p(|x|)} : A(x,y,z) = 1\} < 1/4$$

2-раундовые интерактивные доказательства: **MA**, **AM**.

Язык $L \in \mathbf{MA}_2$, если имеются такие полиномы p и q и полиномиальная ДМТ A, что $\forall x \in \{0,1\}^*$

$$x \in L \implies \exists y \in \{0,1\}^{p(|x|)} : \Pr_{z \in \{0,1\}^{q(|x|)}} \{A(x,y,z) = 1\} > 3/4,$$

$$x \notin L \implies \forall y \in \{0,1\}^{p(|x|)} : \Pr_{z \in \{0,1\}^{q(|x|)}} \{A(x,y,z) = 1\} < 1/4.$$

Язык $L \in \mathbf{AM}$, если $\langle \ldots \rangle$

$$x \in L \implies \Pr_{z \in \{0,1\}^{q(|x|)}} \{\exists y \in \{0,1\}^{p(|x|)} : A(x,y,z) = 1\} > 3/4$$

$$x \notin L \implies \Pr_{z \in \{0,1\}^{q(|x|)}} \{\exists y \in \{0,1\}^{p(|x|)} : A(x,y,z) = 1\} < 1/4$$

Пример: неизоморфизм графов

- Мерлин доказывает $G_0 \not\simeq G_1$.
- Артур берёт случайные $i \in \{0, 1\}$ и перестановку вершин π.

- **Первый раунд:** Артур отправляет $\pi(G_i)$.
- **Второй раунд:** Мерлин возвращает i.

- Неизоморфны $\Rightarrow$ может вернуть правильное i.
- Изоморфны $\Rightarrow$ может только угадывать, вер. $\frac{1}{2}$.

Многораундовые интерактивные доказательства: **IP**

Язык $L \in \mathbf{IP}$, если имеются prover (функция) P и verifier (полиномиальная вероятностная MT) V, такие, что $\forall x \in \{0,1\}^*$

$$\begin{aligned} x \in L &\implies & \Pr\{V^P(x) = 1\} = 1, \\ x \notin L &\implies \forall P' & \Pr\{V^{P'}(x) = 1\} < 1/4. \end{aligned}$$

Важный пример: перманент матрицы

#**P**-полная задача

$$\mathbf{perm}\, A = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

- Сведение вниз: $\underline{\mathbf{perm}\, A = a} \iff \sum_{j=1}^{n} a_{1j} \cdot \mathbf{perm}\, A_{1j} = a$.
  - Prover отправляет $d_j = \mathbf{perm}\, A_{1j}$.
  - Verifier проверяет $\sum_j a_{1j} d_j = a$ и рекурсивно проверяет $\underline{\mathbf{perm}\, A_{1j} = d_j}$.
- Объединение двух задач: $\underline{\mathbf{perm}\, B = b}$ и $\underline{\mathbf{perm}\, C = c}$:
  - Prover отправляет коэффициенты $p(x) = \mathbf{perm}(Bx + C(1-x))$.
  - Verifier проверяет $p(0) = c$ и $p(1) = d$ и ...

- Вычисления ведутся над полем размера $\geq n^4$.

Prover достаточно взять из $\mathbf{P}^{\#\mathbf{P}}$.

Важный пример: перманент матрицы

#**P**-полная задача

$$\mathbf{perm}\, A = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

- Сведение вниз: $\underline{\mathbf{perm}\, A = a} \iff \sum_{j=1}^{n} a_{1j} \cdot \mathbf{perm}\, A_{1j} = a$.
  - Prover отправляет $d_j = \mathbf{perm}\, A_{1j}$.
  - Verifier проверяет $\sum_j a_{1j} d_j = a$ и рекурсивно проверяет $\underline{\mathbf{perm}\, A_{1j} = d_j}$.
- Объединение двух задач: $\underline{\mathbf{perm}\, B = b}$ и $\underline{\mathbf{perm}\, C = c}$:
  - Prover отправляет коэффициенты $p(x) = \mathbf{perm}(Bx + C(1-x))$.
  - Verifier проверяет $p(0) = c$ и $p(1) = d$ и ...
  - рекурсивно проверяет $\underline{\mathbf{perm}(Br + C(1-r)) = p(r)}$ для случайного r (ошибка $\leq \dfrac{\deg\left(p(x) - \mathbf{perm}(Bx + C(1-x))\right)}{\text{размер поля}}$).
- Вычисления ведутся над полем размера $\geq n^4$.

Prover достаточно взять из $\mathbf{P}^{\#\mathbf{P}}$.

$\mathbf{PP} \not\subseteq \mathbf{Size}[n^k]$

$\mathbf{PP} \subseteq \mathbf{Size}[n^k] \subseteq \mathbf{P/poly} \quad \Rightarrow \quad \mathbf{P}^{\mathbf{PP}} \subseteq \mathbf{MA} \subseteq \mathbf{PP}$, но $\mathbf{P}^{\mathbf{PP}} \not\subseteq \mathbf{Size}[n^k]$.

$\mathbf{PP} \not\subseteq \mathbf{Size}[n^k]$

$\mathbf{PP} \subseteq \mathbf{Size}[n^k] \subseteq \mathbf{P/poly} \quad \Rightarrow \quad \mathbf{P}^{\mathbf{PP}} \overset{?}{\subseteq} \mathbf{MA} \subseteq \mathbf{PP}$, но $\mathbf{P}^{\mathbf{PP}} \not\subseteq \mathbf{Size}[n^k]$.

Лемма

$\mathbf{PP} \subseteq \mathbf{P/poly} \Rightarrow \mathbf{P}^{\mathbf{PP}} \subseteq \mathbf{MA}$.

- Для $\mathbf{P}^{\mathbf{PP}}$ есть протокол (который для $\#\mathbf{P}$).
- Verifier (Артур) будет моделировать этот протокол сам, для Provera (из $\mathbf{P}^{\mathbf{PP}}$) есть схемы (даст Мерлин).

$\mathbf{PP} \not\subseteq \mathbf{Size}[n^k]$

$\mathbf{PP} \subseteq \mathbf{Size}[n^k] \subseteq \mathbf{P/poly} \quad \Rightarrow \quad \mathbf{P}^{\mathbf{PP}} \subseteq \mathbf{MA} \overset{?}{\subseteq} \mathbf{PP}$, но $\mathbf{P}^{\mathbf{PP}} \not\subseteq \mathbf{Size}[n^k]$.

Лемма

$\mathbf{MA} \subseteq \mathbf{PP}$.

Пусть $L \in \mathbf{MA}$, длина док-ва Мерлина $p(n)$, вероятность ошибки $4^{-p(n)}$ (аналогично **BPP** при помощи неравенства Чернова):

$$x \in L \implies \exists y \in \{0,1\}^{p(|x|)} : \Pr_{z \in \{0,1\}^{q(|x|)}} \{M(x,y,z) = 1\} > 1 - 4^{-p(|x|)}$$

$$x \notin L \implies \forall y \in \{0,1\}^{p(|x|)} : \Pr_{z \in \{0,1\}^{q(|x|)}} \{M(x,y,z) = 1\} < 4^{-p(|x|)}$$

В отсутствие Мерлина будем выбирать его док-во y случайно:

$$x \in L \implies \Pr_{(y,z)} \{M(x,y,z) = 1\} > 2^{-p(|x|)} \cdot (1 - 4^{-p(|x|)}) > 4^{-p(|x|)}$$

$$x \notin L \implies \Pr_{(y,z)} \{M(x,y,z) = 1\} < 4^{-p(|x|)}$$