Теорема (ADLEMAN)

$BPP \subseteq P/poly$.

Док-во

В классе BPP можно понизить ошибку так, чтобы она была не более $2^{-(n+2)}$. То есть

$$x \in L \Rightarrow P_R[M(x,r)=1] \geq 1 - 2^{-(n+2)}$$

$$x \notin L \Rightarrow P_r[M(x,r)=1] \leq 2^{-(n+2)}.$$

~~x - пло~~ Скажем, что r - плохой для x, если $M(x,r) \neq L(x)$, тогда для $\forall x$ не более $2^{-(n+2)}$ ~~плохих~~ ~~r. Получается~~ $\cdot 2^m$ плохих r. Т.е. всего плохих R не более $2^n \cdot 2^{-(n+2)} \cdot 2^m = \frac{2^m}{4}$, то есть $\exists R'$ хороший для всех. Давайте тогда используем его ~~как~~ ~~совет~~ [illegible] совет, а это и значит, что для L у нас есть схема, то есть $BPP \subseteq P/poly$.

∎

Теорема (Sipser - Gács)

$$BPP \subseteq \Sigma_2^P \cap \Pi_2^P$$

Док-во:

$BPP = coBPP$, поэтому достаточно доказывать $BPP \subseteq \Sigma_2^P$.

$$x \in L \Rightarrow P_2\left[M(x,z)=1\right] \geq 1 - 2^{-n}$$

$$x \notin L \Rightarrow P_2\left[M(x,z)=1\right] \leq 2^{-n}$$

$x \in L$ | $x \notin L$

$$|S_x| \geq 2^m - \frac{2^m}{2^n} \qquad |S_x| \leq \frac{2^m}{2^n}$$

Утв 1 $\forall u_1, u_2, \ldots u_k$, если $|S_x| \leq \frac{2^m}{2^n}$, то $\bigcup (u_i \oplus S_x)$ не покрывает $\{0,1\}^m$

док-во $\left|\bigcup (u_i \oplus S_x)\right| \leq k \cdot \frac{2^m}{2^n} \not\geq 1$ если $k < 2^n$.

Утв 2 $\exists u_1, \ldots u_k$, что $\forall S_x$ т.ч. $|S_x| \geq 2^m - \frac{2^m}{2^n}$

$\exists u_1, \ldots u_k$, что $\bigcup S_x \oplus u_i = \{0,1\}^m$.

док-во Выберем u_i независимо равномерно: тогда $\forall x$ покрывается с вероятностью $1 - 2^{-n}$ одним $u_i + S_x$

$\{0,1\}^m$

$u_i + S_x$ попарно независимы, то есть у

не покрываются с вероятностью не более 2^{-nk}. Всего строк 2^m. То есть наш ожидаемое 2^{m-nk}. Значит если $k=m$, то наше ожидание меньше 1 $\Rightarrow$ $\exists$ нужная матрица.

Получаем

$$x \in L \iff \exists u_1, u_2, \dots u_m \in \{0,1\}^m \ \forall z \in \{0,1\}^m \quad \bigvee_{i=1}^{m} M(x, z \oplus u_i) = 1.$$

Вероятностные сведения

Определение Язык A сводится к языку B с помощью вероятностного полиномиального сведения $A \leq_R B$, если $\exists$ ПМТ M с т. $\forall x \in \{0,1\}^*$:

$$P_z[B(M(x)) = A(x)] \geq \frac{2}{3}.$$

Усв Если $A \leq_R B$ и $B \in BPP$, то $A \in BPP$.

Док-во

$A \to B_1, B_2, \dots B_k$ так чтобы с вероятностью $\frac{9}{10}$ большинство выдавало правильный ответ.

Решим $B_1, \dots B_k$ — с ошибкой не больше $\frac{1}{10k}$

тогда с вероятностью $\frac{9}{10}$ у нас нет ошибки в ответах о $B_1, \dots B_k$ $\Rightarrow$ большинство покажет что с вер не меньше $\frac{8}{10}$ выдали верный ответ.

Определение Класс $BP \cdot NP$

$$BP \cdot NP = \{L : L \leq_R \exists SAT\}$$

Замечание: $\leq_R$ – не транзитивно.

Попарно независимые хэш функции

$\mathcal{H}_{n,k} : \{0,1\}^n \to \{0,1\}^k$

Говорим, что $\mathcal{H}_{n,k}$ попарно независимы если

$\forall \; x, x'$ т.ч $x \neq x' \quad \forall y, y' \in \{0,1\}^k$

$$P_{\substack{h \in \mathcal{H}_{n,k}}} [h(x) = y \wedge h(x') = y] = 2^{-2k}.$$

Теорема (о существовании эффективных ~~попарно~~ попарно неуров. хэш функций)

$\forall n$ положим $\mathcal{H}_{n,n} = \{h_{a,b}\}_{a,b \in GF(2^n)}$

↓ поле из 2^n элементов

$x \to ax+b$

$GF(2^n)$

$\mathcal{H}_{n,n}$ – мн-во попарно нез. хэш функц.

Если могу $\mathcal{H}_{n,k}$, то можно лучше определить.

Док-во упражнение.

Теорема (Валиант – Вазирани)

$\exists$ вероятностный алгоритм f, такой что

$\forall$ булевой формулы φ верно:

$$\varphi \in SAT \Rightarrow P_2[f(\varphi) \in USAT] \geq \frac{1}{8}$$

$$\varphi \notin SAT \Rightarrow P_2[f(\varphi) \in SAT] = 0$$

Лемма (Валиант Вазирани)

$\mathcal{H}_{n,k} : \{0,1\}^n \to \{0,1\}^k$

$S \subseteq \{0,1\}^n$ и $|S| \geq 2^{k-2}$, $|S| \leq 2^{k-1}$.

Тогда $P_{h \in \mathcal{H}_{n,k}}[\exists! x \in S \text{ такое что } h(x) = 0^k] \geq \frac{1}{8}$.

док-во

$\forall x \in S \quad P_2[h(x) = 0^k] = \frac{1}{2^k} = p$

$P_2[h(x) = 0^k \wedge h(x') = 0^k] = p^2$.

Пусть N – это число $x \in S$, таких что $h(x) = 0^k$.

$E(N) = |S|p \in (\frac{1}{4}, \frac{1}{2})$

$$P_2[N \geq 1] \geq \sum_{x \in S} P_2[h(x) = 0^k] - \sum_{x' < x} P_2[h(x) = 0^k \wedge h(x') = 0^k]$$

$$= |S|p - \binom{|S|}{2} p^2$$

$P_2[N \geq 2] \leq \binom{|S|}{2} p^2$.

$P_2[N = 1] = P_2[N \geq 1] - P_2[N \geq 2] \geq |S|p - 2\binom{|S|}{2} p^2 \geq$

$\geq |S|p - |S|^2 p^2 = |S|p(1 - |S|p) \geq \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$

Док-во теоремы

Упорядочим количество решений, точнее в порядке их отрезков их кол-во лежат.

$[1,2]$, $[2,4]$, $[4,8]$ ... они лежат.

Упорядочим с вер не менее $\frac{1}{n}$. После этого возьмем случайное $h \in \mathcal{H}_{n,k}$ и рассмотрим ур-в.

$\exists x\ \varphi(x) \wedge (h(x) = 0^k)$

$h(x) = 0^k$ - можно записать в виде КНФ или h к примеру эффективно вычисляется.

получаем $\exists x\ \varphi(x) \wedge \tau(x, y)$

$\tau(x, y)$ - записывает в КНФ факт того что $h(x) = 0^k$.

□