2019 Lec 6

2019年4月18日 13:54

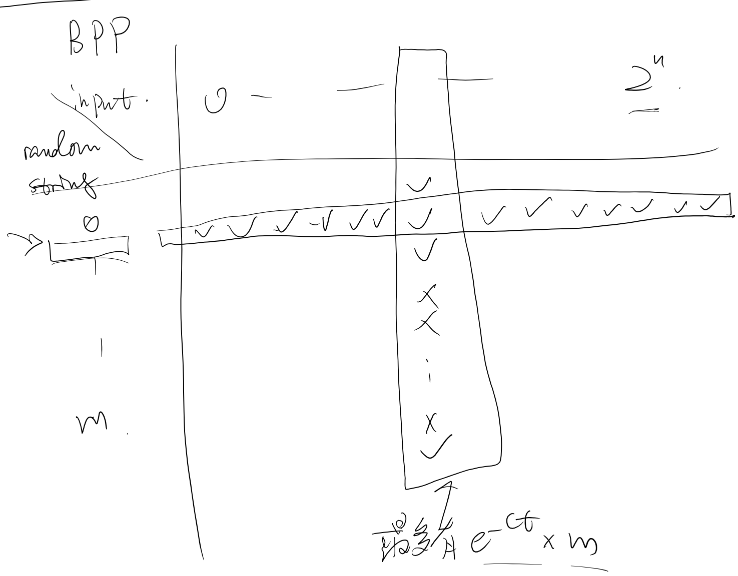
$\boxed{1\sim1}\ \boxed{2--2}\ \boxed{3-3}\ x-x\ 5-5\ \boxed{6}$

叶或多1

$$\frac{6}{5}-1=0.2\text{步}$$

$$\left(\frac{6}{5}-1\right)\times 5+1=2$$

$$\left(\frac{n}{n-1}-1\right)\times n-1+1=2$$



$$e^{-ct}=e^{-n^2}$$

$$\#\text{“}x\text{”}\leq e^{-n^2}\times m\times 2^n$$

$$<m$$

~~BPP~~ $\stackrel{?}{=}$ P

BPP = P

$\forall n$ $\exists$ 多项式时间算法

Probability Amplication.

$Z_p=\{0,1,2,\ldots,p-1\}$

$r,\ r'$:

$$\boxed{\begin{aligned} r_1&=r+r' \quad (\mathrm{mod}\ p)\\ r_2&=r+2r'\\ r_3&=r+3r'\\ &\ \vdots\\ r_t&=r+tr' \end{aligned}}$$

$A(r_1)=0$

$A(r_2)=0$

$\vdots$

$A(r_t)=0$

true answer: $=1$

$$\Pr\Big(\underbrace{\sum_{i=1}^{t} A(r_i)=0}_{=X}\Big) \le \Pr\Big(|X - E(X)| \ge \frac{t}{2}\Big) \le \frac{\mathrm{Var}(X)}{(E(X))^2} = \frac{\mathrm{Var}(X)}{(\frac{t}{2})^2} \approx \Theta\left(\frac{1}{t}\right).$$

$$E(X) = \sum_{i=1}^{t} E(A(r_i)) = \frac{t}{2}.$$

$$\mathrm{Var}(X) = \mathrm{Var}\Big(\sum_{i=1}^{t} A(r_i)\Big) = \sum_{i=1}^{t} \underbrace{\mathrm{Var}(A(r_i))}_{c \cdot t} + \boxed{\sum_{i,j} \mathrm{Cov}(A(r_i), A(r_j))}_{=0}.$$

$r_i = r + i \cdot r' \pmod p$ $\qquad r, \quad r+r'$

$r_j = r + j \cdot r' \pmod p$

$$\Pr(r_i = a,\ r_j = b) = \Pr(r_i = a) \cdot \Pr(r_j = b) = \frac{1}{p^2}$$

$$= \frac{\#\ 方程 \begin{cases} r + ir' \equiv a \\ r + jr' \equiv b \end{cases} 解的个数}{p^2}$$

$x_1, x_2, \ldots, x_n$ $\qquad$ d 维 $\to$ k 维

$\langle x_i, u_1 \rangle \quad \langle x_i, u_2 \rangle \quad \ldots \quad \langle x_i, u_k \rangle$

d 维

PID.

$$Q(x_1, \ldots, x_n) = x_1^k Q_k(x_2, \ldots, x_n) + x_1^{k-1} Q_{k-1}(x_2, \ldots, x_n) + \cdots + Q_0(x_2, \ldots, x_n)$$

$$Q_k(x_2, \ldots, x_n) \not\equiv 0 \qquad Q_k: \text{degree} \le d-k.$$

case 1: $\Pr(\overbrace{Q_k(r_2, \ldots, r_n) = 0}^{A}) \le \dfrac{d-k}{|S|}$. $\qquad P(A) \le \dfrac{d-k}{|S|}$

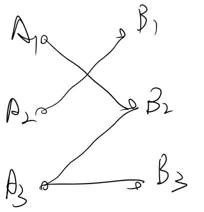
case 2: $\Pr\Big(\overbrace{\underbrace{Q(r_1, \ldots, r_n)}_{f(x_1)} = 0}^{B} \,\Big|\, \overbrace{Q_k(r_2, \ldots, r_n) \not\equiv 0}^{\bar{A}}\Big) \le \dfrac{k}{|S|}$. $\qquad \Pr(B \mid \bar{A}) \le \dfrac{k}{|S|}$

$f(x_1)$ $\qquad\qquad \le \frac{k}{|S|}$

$\Pr(Q(r_1,\dots,r_n)=0)$

$$\Pr(B) = \Pr(B,A) + \Pr(B,\bar{A})$$
$$\qquad \le \Pr(A) \qquad\qquad \le \Pr(B\mid\bar{A})$$

Perfect matching.



$$M=\begin{pmatrix} 0 & x_{12} & 0 \\ x_{21} & 0 & 0 \\ 0 & x_{32} & x_{33} \end{pmatrix}$$

$\exists$ perfect matching

$\Longleftrightarrow$ $\boxed{\det(M)}$ 非零多项式.

$$\det(M) = \sum_{\pi} (-1)^{\pi} \boxed{\prod_{i=1}^{n} M_{i\pi(i)}}$$

$$\mathrm{perf}(M) = \sum_{\pi} \prod_{i=1}^{n} M_{i\pi(i)} \qquad = \mathrm{perm}(M).$$

perfect matching

$$\det(M) = M_{11} M_{22} M_{33} + M_{12} M_{23} M_{31} + M_{13} M_{21} M_{32}$$
$$\quad - M_{11} M_{23} M_{32} - M_{12} M_{21} M_{33} - M_{13} M_{22} M_{31}$$
$$= - x_{12} x_{21} x_{33}$$

3SAT.

$x_1 \vee \bar{x}_2 \vee x_3 \longrightarrow 1-(1-x_1)x_2(1-x_3)$

$\deg f \le 3m$

$x_1=0,\ x_2=1,\ x_3=0 \qquad f(x_1,\dots,x_n) = (1-\cdots)\ (1-\cdots)$

$$\forall\, x_1,\dots,x_n \in \{0,1\} \quad f(x_1,\dots,x_n)=0.$$

$$\Longleftrightarrow \boxed{\sum_{x_1\in\{0,1\}} \sum_{x_2\in\{0,1\}} \cdots \sum_{x_n\in\{0,1\}} f(x_1,\dots,x_n)} = 0 \qquad \mathbb{Z}_p.$$

$$= h_0(x_1,\dots,x_n)$$

$$h_1(x_1) = h_1(x_1,\dots,x_n) \triangleq \sum_{x_2\cdots x_n} f(x_1,\dots,x_n) \qquad h_1(0)+h_1(1)=h_0.$$

$h_2(x_1,x_2) = h_2(x_1,\cdots,x_n) \triangleq \sum_{x_3\cdots x_n} f(x_1,\cdots,x_n)$ $\qquad$ $\underline{h_2(x_1,0)+h_2(x_1,1)=h_1(x_1)}$

$\vdots$

$h_n(x_1,\cdots,x_n) = f(x_1,\cdots,x_n)$.

Merlin $\qquad$ Arthur.

$\deg(h_1)\le 3m$.

$h_1(x_1) \longrightarrow$ $\qquad$ check $h_1(0)+h_1(1)=0$?

$\longleftarrow$ random r_1

$\deg(h_2(x_1,x_2))\le 3m$

$h_2(r_1,x_2) \longrightarrow$ $\qquad$ check $h_2(r_1,0)+h_2(r_1,1)=\boxed{h_1(r_1)}$

$\longleftarrow$ random r_2

$h_3(r_1,r_2,x_3) \longrightarrow$ $\qquad$ check $h_3(r_1,r_2,0)+h_3(r_1,r_2,1)=h_2(r_1,r_2)$

$\vdots$

$\longleftarrow$ random r_{n-1}

$h_n(r_1,r_2,\cdots,r_{n-1},x_n) \longrightarrow$ $\qquad$ check $h_n(r_1,\cdots,r_{n-1},0)+h_n(r_1,\cdots,r_{n-1},1)$
$= h_{n-1}(r_1,\cdots,r_{n-1})$.

check $\boxed{h_n(r_1,\cdots,r_{n-1},x_n)}$ $\swarrow$ PID.
$= f(r_1,\cdots,r_{n-1},x_n)$

$(1-\square x_n)(1-\square(1-x_n))(\quad)$

$h_1(x_1) \ne \sum_{x_2\cdots x_n} f(x_1,\cdots,x_n)$ $\qquad$ $h_1(1)+h_1(0)\ne 0$

case 1: $h_2(r_1,x_2) = \sum_{x_3,\cdots,x_n} f(r_1,x_2,x_3,\cdots,x_n)$

$h_2(r_1,0)+h_2(r_1,1)=h_1(r_1)$ ✓ $\qquad$ $\le \left(\frac{d}{|S|}\right.$

$h_2(x_1,0)+h_2(x_1,1) \ne h_1(x_1)$

当 case 1 没发生.

$h_2(r_1,0)+h_2(r_1,1)\ne h_1(r_1)$

$h_2(r_1,x_2) \ne \sum_{x_3\cdots x_n} f(r_1,x_2,\cdots,x_n)$

case 3. $h_3(r_1, r_2, x_3) \equiv \sum_{x_4 \cdots x_n} f(r_1, r_2, x_3, \cdots, x_n)$

$h_3(r_1, r_2, 0) + h_3(r_1, r_2, 1) = h_2(r_1, r_2)$

$h_3(r_1, x_2, 0) + h_3(r_1, x_2, 1) \not\equiv h_2(r_1, x_2)$

$\frac{d}{|S|}$

case n. $h_n(r_1, \cdots, r_{n-1}, x_n) \equiv f(r_1, r_2, \cdots, r_{n-1}, x_n)$

$h_n(\quad) + h_n(\quad) = h_{n-1}(\quad)$

case n+1. $h_n(r_1, \cdots, r_{n-1}, x_n) \not\equiv f(r_1, \cdots, r_{n-1}, x_n)$ PID

$\frac{d}{|S|}$

cheating probability

$\approx \Theta\left(n \times \frac{d}{|S|}\right)$ $d \le 3m$.

EQ function:

Alice $(x_1, \cdots, x_n) = a$ Bob $(y_1, \cdots, y_n) = b$

$0 \sim 2^n - 1$

random pick prime p.

Alice send $(a \bmod p, p)$ to Bob

$a \bmod p = b \bmod p$. $p \mid a-b$

质因数 $\le n$.

$\Pr(\text{error probability}) \le \dfrac{n}{\frac{n^3}{3\ln n}}$

$1 \sim N$

$N = n^3$

质数 in $\{1 \cdots N\}$

$\approx \frac{N}{\ln N} = o(N)$.

$p: 1 \sim n^3$

communication complexity $= C \log n$,

communication complexity $= \underline{C \lg n}$,