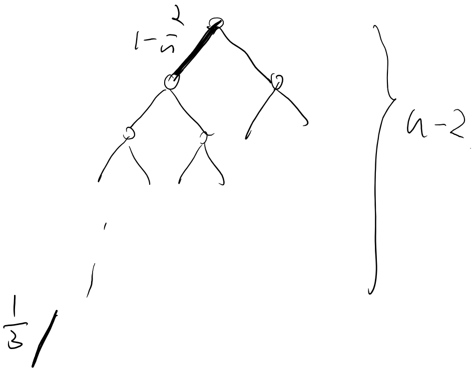
2019 Lec 2

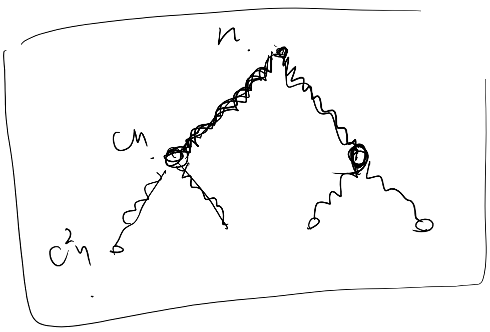
2019年3月14日 18:31

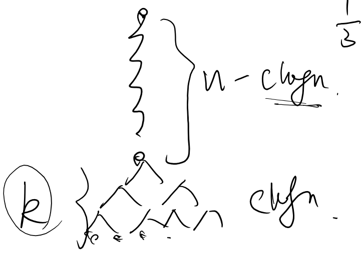
$$\left(1-\frac{2}{n}\right) \times \left(1-\frac{2}{n-1}\right) \times \cdots \times \left(1-\frac{2}{3}\right)$$

$$\frac{3}{5} \times \frac{2}{4} \times \frac{1}{3}$$



$n \longrightarrow m$





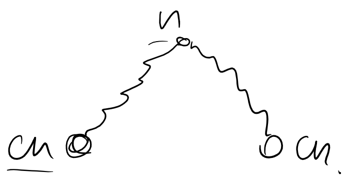
1°. Time complexity.

$$T(n) = O(n^2) + 2T(cn)$$

$$T(n) = O(n^2 \log n)$$

$$n^2 + 2 \cdot (cn)^2 \log cn = n^2 \log n$$

$C = \frac{1}{\sqrt{2}}$



2°. successful probability.

$$P(n) = 1 - (\sim\sim 失败 \quad)^2$$

$$= 1 - \left(1 - P(cn) \cdot P_r(n \to cn \text{ 成功})\right)^2$$

$$= 1 - \left(1 - c^2 P(cn)\right)^2 \qquad C = \frac{1}{\sqrt{2}}$$

$$\geq 1 - \left(1 - \frac{1}{2} P\left(\frac{n}{\sqrt{2}}\right)\right)^2$$

$$\geq \left(1-\frac{2}{n}\right) \cdots \left(1-\frac{2}{cn}\right) \approx c^2$$

$\boxed{1-\frac{2}{n}}$

$RP \subseteq NP$

NP: $\begin{cases} x \in L \Rightarrow \exists y.\ |y| = poly(|x|) & A(x,y) \text{ accepts} \\ x \notin L \Rightarrow \forall y. & A(x,y) \text{ rejects} \end{cases}$

RP: $\begin{cases} x \in L \Rightarrow Pr(B(x) \text{ accept}) \geq \frac{1}{2} \\ x \notin L \Rightarrow Pr(B(x) \text{ accept}) = 0 \end{cases}$

$\forall L \in RP \Rightarrow B$

prove $L \in NP$ construct A. y = random strings

$\boxed{B(x, r)}$ $|r| = poly(|x|)$

$NP \subseteq PP$

$\forall L \in NP \Rightarrow \exists A(x,y)$ $|y| = poly(|x|)$

$Pr(B(x, r))$

random choose r, if $A(x, r)$ accept $\Rightarrow$ $B(x)$ accept

random

if $A(x,r)$ reject $\Rightarrow$ $B(x)$ $\begin{cases} \text{accept} & \frac{1}{2} - \frac{1}{4 \times 2^{poly(x)}} \\ \text{reject} & \frac{1}{2} + \frac{1}{4 \times 2^{poly(x)}} \end{cases}$

$x \in L$ $Pr(B(x) \text{ accept}) = \frac{1}{2^{poly(x)}} + \left(1 - \frac{1}{2^{poly(x)}}\right) \cdot \frac{1}{2} > \frac{1}{2}$

$x \notin L$ $Pr(B(x) \text{ accept}) = \frac{1}{2}$

$\frac{1}{2 \times 2^{poly(x)}}$

$PP \stackrel{?}{=} BPP$

$PP \stackrel{?}{=} BPP$.

$ZPP = RP \cap co\text{-}RP$.

1°. $ZPP \subseteq RP \cap co\text{-}RP$

$\forall L \in ZPP$ ↑ A. prove $L \in RP$. ↑ B.

A: expected running time $= n^c$.

B: run A. until Time n^{c+1}

case 1 A returns before Time n^{c+1} ✓

case 2. A. not return. ——— B return. reject.

$x \notin L$. $Pr(B \text{ accept}) = 0$

$x \in L$ $Pr(B \text{ accept}) = Pr((\text{case 1 happens}) \geq 1 - \frac{1}{n}$.

$$\boxed{\text{Markov Inequality. R.V. } X \geq 0. \quad Pr(X \geq c) \leq \frac{E(X)}{c}}$$

R.V. X: $Time(A)$,

$E(Time(A)) = n^c$.

$Pr(\text{case 1 happens}) = Pr(Time\,A < n^{c+1})$ $2 \cdot n^c$.

$\geq 1 - \frac{E(Time(A))}{n^{c+1}} = 1 - \frac{1}{n}$.

2°. $RP \cap coRP \subseteq ZPP$.

$\forall L \in RP \cap co\text{-}RP$. A_1: RP-Algo. A_3. NP.-

A_2: coRP Algo.

~~construct~~ B (ZPP) → A_1 ← if A_1 accept B accept.

construct B (ZPP)

A_1 ← if A_1 accept B accept.

A_2 ← if A_2 reject B reject

A_3

$E(\text{Time}(B))$ repeat 1 time, B stop with $Pr = \frac{3}{4}$.

$$\leq \frac{4}{3} \times (\text{Time}(A_1) + \text{Time}(A_2) + \text{Time}(A_3))$$

Matrix multiplication verification. $\mathbb{F}_2 = \{0, 1\}$. $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$.

$$A \cdot B \stackrel{?}{=} C.$$

当 $A \cdot B \neq C$. $Pr(ABv = Cv)$

$$= Pr(\underbrace{(AB - C)}_{=D} \cdot v = 0)$$

Assume $d_{11} = 1$

$$\leq Pr(1 \cdot v_1 + d_{12}v_2 + \cdots + d_{1n}v_n = 0)$$

$$= \frac{1}{2}. \qquad \frac{2^{n-1}}{2^n}$$

EQ function.

$f = g$. accept

if $f \neq g$. $Pr(f(x) = g(x))$ $h = f - g$.

$= Pr(h(x) = 0)$ h: $n-1$ 次多项式.

$$\leq \frac{n-1}{p}.$$

set $p = n^2$

communication complexity $= 2\log p = \Theta(\log n)$.

$\Omega(n)$ ← deterministic