

4-13 Randomized Algorithms

Hengfeng Wei

hfwei@nju.edu.cn

June 10, 2019





1/2

Definition (*ZPP*: Zero-error Probabilistic Polynomial Time)

$$L \in ZPP$$

$$\iff$$

$\exists A$ (*probabilistic polynomial-time algorithm*):

$$Pr(A(x) = L(x)) \geq \frac{1}{2}$$

$$Prob(A(x) = ?) = 1 - Pr(A(x) = L(x)) \leq \frac{1}{2}$$

Q : Why 1/2?

$$ZPP_\delta : ZPP_{1/3} = ZPP_{1/2} = ZPP_{2/3}$$

$$L \in ZPP_\delta$$

$A^{(k)}$: Repeat A k times independently

Output the non-“?” value if any; Otherwise, output “?”

$$L \in ZPP_\alpha \text{ for some } \alpha$$

$$\Pr\left(A^{(k)}(x) = L(x)\right) = 1 - \Pr\left(A^{(k)}(x) = ?\right) \geq 1 - (1 - \delta)^k$$

$$L \in ZPP_{1-(1-\delta)^k}$$

Definition (*RP*: Randomized Polynomial time (One-Sided Error))

$$L \in RP$$

$$\iff$$

$\exists A$ (*probabilistic polynomial-time algorithm*) :

$$x \in L \implies \Pr(A(x) = 1) \geq \frac{1}{2}$$

$$x \notin L \implies \Pr(A(x) = 0) = 1$$

Q : Why $1/2$?

$$RP_\delta : RP_{1/3} = RP_{1/2} = RP_{2/3}$$

$$L \in RP_\delta$$

$A^{(k)}$: Repeat A k times independently

Accept x iff any of the k runs accepts

$$L \in RP_\alpha \text{ for some } \alpha$$

$$Pr(x \in L \wedge A^{(k)}(x) = 1) = 1 - Pr(x \in L \wedge A^{(k)}(x) = 0) \geq 1 - (1 - \delta)^k$$

$$L \in RP_{1-(1-\delta)^k}$$

Definition (*BPP*: Bounded-error Probabilistic Polynomial time
(Two-Sided Error))

$$L \in BPP$$

$$\Longleftrightarrow$$

$\exists A$ (*probabilistic polynomial-time algorithm*) :

$$\exists \epsilon, 0 < \epsilon \leq 1/2 : Pr(A(x) = L(x)) \geq \frac{1}{2} + \epsilon$$

Q : Why 1/2?

Q : Why ϵ ?

$$L \in BPP_{p \triangleq (\frac{1}{2} + \delta)}$$

$A^{(k)}$: Repeat A k times independently

Output the “majority” ($\# \geq \lceil k/2 \rceil$) value

$$L \in BPP_\alpha \text{ for some } \alpha$$

$$\Pr\left(A^{(k)}(x) = L(x)\right) \geq 1 - \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{t}{i} p^i (1-p)^{k-i} > 1 - \frac{1}{2}(1 - 4\delta^2)^{k/2}$$

$$L \in BPP_{1-\epsilon} \implies k \geq \frac{2 \ln 2\epsilon}{\ln(1 - 4\delta^2)}$$

Definition (*BPP*: Bounded-error Probabilistic Polynomial time (Two-Sided Error))

$$L \in BPP$$

$$\iff$$

$\exists A$ (*probabilistic polynomial-time algorithm*) :

$$\exists \epsilon, 0 < \epsilon \leq 1/2 : Pr(A(x) = L(x)) \geq \frac{1}{2} + \epsilon$$

Q : Why ϵ ?

Q : What about $Pr(A(x) = L(x)) > \frac{1}{2}$?

Q : What about $Pr(A(x) = L(x)) \geq \frac{1}{2} + n^{-c}$ for some constant c ?

$$\Pr(A(x) = L(x)) \geq \frac{1}{2} + n^{-c} \text{ for some constant } c$$

$$L \in BPP_{p \triangleq (\frac{1}{2} + n^{-c})}$$

$A^{(k)}$: Repeat A k times independently

Output the “majority” ($\# \geq \lceil k/2 \rceil$) of x_1, x_2, \dots, x_k

$$L \in BPP_\alpha \text{ for some } \alpha$$

Indicator random variables

$$X_i = \begin{cases} 1, & x_i = L(x) \\ 0, & \text{otherwise} \end{cases}$$

$$X = \sum_{i=1}^k X_i$$

$$\Pr\left(X \geq \frac{1}{2}k\right) \geq \dots$$

$$\forall 0 < \delta < 1 : \Pr\left(X < (1 - \delta)pk\right) < e^{-\frac{\delta^2}{3}pk}$$

$$\text{Fix } \delta = 1 - \frac{1}{2p}$$

$$\Pr\left(X \geq \frac{1}{2}k\right) \geq 1 - e^{-\frac{k}{3n^c}}$$

$$\Pr\left(X \geq \frac{1}{2}k\right) \geq 1 - e^{-\frac{k}{3n^c}}$$

Choose $k = 3n^{c+d}$ for some constant d

$$\Pr\left(X \geq \frac{1}{2}k\right) \geq 1 - e^{-n^d}$$

$$L \in BPP_{1-e^{-n^d}}$$

$$\forall \text{ constant } c, d > 0 : BPP_{\frac{1}{2} + \frac{1}{n^c}} = BPP_{1 - \frac{1}{e^{n^d}}}$$

Definition (*PP*: Probabilistic Polynomial time (Unbounded Error))

$$L \in BPP$$

$$\Longleftrightarrow$$

$\exists A$ (*probabilistic polynomial-time algorithm*) :

$$Pr(A(x) = L(x)) > \frac{1}{2}$$

We want $Pr(A^{(k)}(x) = L(x)) \geq 1 - \delta$

k may be exponential of n

$$Pr(A(x) = L(x)) \geq \frac{1}{2} + \frac{1}{2^{n^c}} \text{ for some constant } c$$

$$P \subseteq ZPP \subseteq RP \subseteq BPP \subseteq PP$$

Exercise 5.2.2.9





Office 302

Mailbox: H016

hfwei@nju.edu.cn