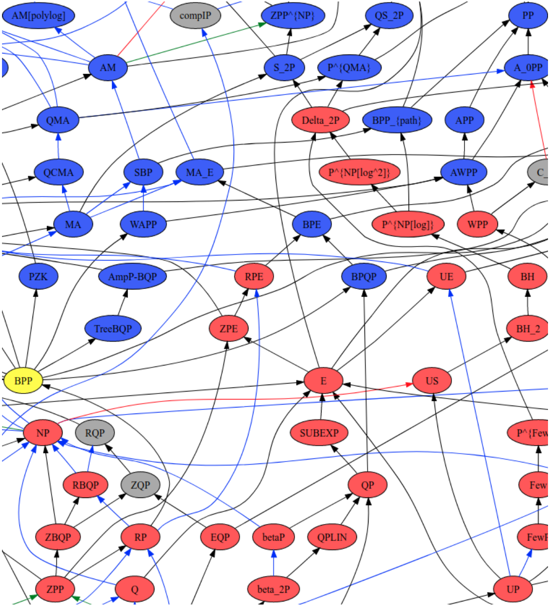
4-13 Randomized Algorithms

Hengfeng Wei

hfwei@nju.edu.cn

June 10, 2019


1/2


AM[polylog]
compIP
ZPP^{NP}
QS_2P
PP
AM
S_2P
P^{QMA}
A_0PP
QMA
Delta_2P
BPP_{path}
APP
QCMA
SBP
MA_E
P^{NP[log^2]}
AWPP
MA
WAPP
BPE
P^{NP[log]}
WPP
PZK
AmpP-BQP
RPE
BPQP
UE
BH
TreeBQP
ZPE
BH_2
BPP
E
US
NP
RQP
SUBEXP
RBQP
ZQP
QP
ZBQP
RP
EQP
betaP
QPLIN
ZPP
Q
beta_2P
UP

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

Definition (ZPP: Zero-error Probabilistic Polynomial Time)

$$L \in ZPP$$

$$\iff$$

$$\exists A \ (\textit{probabilistic polynomial-time algorithm}):$$

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

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

Definition (ZPP: Zero-error Probabilistic Polynomial Time)

$$L \in ZPP$$

$$\iff$$

$$\exists A \; (probabilistic\ polynomial\text{-}time\ algorithm):$$

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

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

Q : Why 1/2?

Definition (ZPP: Zero-error Probabilistic Polynomial Time)

$$L \in ZPP$$

$$\iff$$

$$\exists A \ (\textit{probabilistic polynomial-time algorithm}):$$

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

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

Q : Why 1/2?

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

$$L \in ZPP_{\delta}$$

$$L \in ZPP_\delta$$

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

$L \in ZPP_\delta$

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

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

$L \in ZPP_\delta$

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

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

$L \in ZPP_\alpha$ for some α

$$L \in ZPP_\delta$$

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

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

$L \in ZPP_\alpha$ for some α

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

$$L \in ZPP_\delta$$

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

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

$L \in ZPP_\alpha$ for some α

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

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

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

$$L \in RP$$

$$\iff$$

$$\exists A \; (\textit{probabilistic polynomial-time algorithm}):$$

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

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

Q : Why 1/2?

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

$$L \in RP$$

$$\iff$$

$$\exists A \; (\textit{probabilistic polynomial-time algorithm}):$$

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

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

Q : Why 1/2?

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

$$L \in RP_\delta$$

$$L \in RP_\delta$$

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

$L \in RP_\delta$

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

Accept x iff any of the k runs accepts

$$L \in RP_\delta$$

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

Accept x iff any of the k runs accepts

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

$$L \in RP_\delta$$

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

Accept x iff any of the k runs accepts

$L \in RP_\alpha$ for some α

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

$$L \in RP_\delta$$

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

Accept x iff any of the k runs accepts

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

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

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

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

$$L \in BPP$$

$$\iff$$

$$\exists A \ (probabilistic\ polynomial\text{-}time\ algorithm):$$

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

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

$$L \in BPP$$

$$\Longleftrightarrow$$

$$\exists A \text{ (\textit{probabilistic polynomial-time algorithm})} :$$

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

Q : Why 1/2?

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

$$L \in BPP$$

$$\iff$$

$$\exists A \ (\textit{probabilistic polynomial-time algorithm}):$$

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

Q : Why 1/2? Q : Why ϵ?

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

$$L \in BPP$$

$$\iff$$

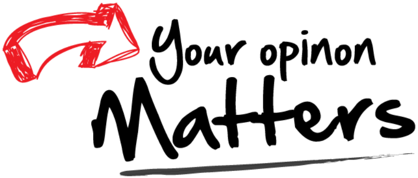
$$\exists A \ (\textit{probabilistic polynomial-time algorithm}):$$

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

Q : Why 1/2? Q : Why ϵ?

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


THANK YOU



Office 302

Mailbox: H016

hfwei@nju.edu.cn