Computational Complexity — tutorial 10

Probabilistic algorithms 2

Probabilistic complexity classes compared with P:

Class	$\mathbb{P}$[algorithm accepts x] if		**Running time**	**Why is it named so?**
	$x \in L$	$x \notin L$		
P	1	0	polynomial	**P**olynomial
RP	$\geqslant \frac{1}{2}$	0	polynomial	**R**andomized **P**olynomial
co-RP	1	$\leqslant \frac{1}{2}$	polynomial	
BPP	$\geqslant \frac{3}{4}$	$\leqslant \frac{1}{4}$	polynomial	**B**ounded-error **P**robabilistic **P**olynomial
PP	$\geqslant \frac{1}{2}$	$< \frac{1}{2}$	polynomial	**P**robabilistic **P**olynomial
ZPP	1	0	**expected** polynomial	**Z**ero-error **P**robabilistic **P**olynomial

1. Prove the *amplification lemma* for RP: if we replace „$\geqslant \frac{1}{2}$", in the definition of RP with „$\geqslant \varepsilon$" for any constant $0 < \varepsilon < 1$, we'll get exactly the same definition of RP.

In other words: if we run the probabilistic algorithm over and over again, we'll be more and more confident about its answer.

2. Prove the *amplification lemma* for BPP: if we replace „$\geqslant \frac{3}{4}$", „$\leqslant \frac{1}{4}$" in the definition of BPP with „$\geqslant 1-\varepsilon$", „$\leqslant \varepsilon$" for any constant $0 < \varepsilon < \frac{1}{2}$, we'll get exactly the same definition of BPP.

Hint: you can (but don't have to) use a variant of Chernoff bound for Bernoulli variables — for independent variables $X_1, X_2, \ldots, X_n \in \{0,1\}$, $\mu = \mathbb{E}[X_1 + \cdots + X_n]$, $\delta \in (0,1)$:

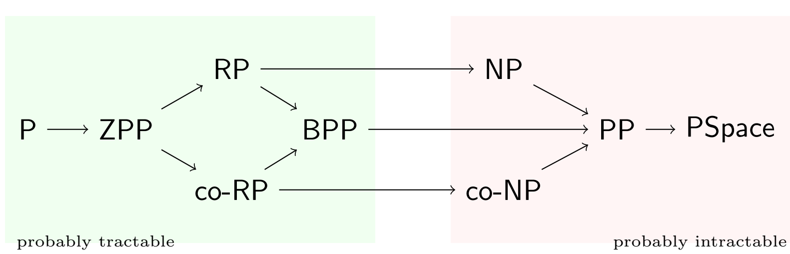
$$\mathbb{P}[X_1 + \cdots + X_n \leqslant (1-\delta)\mu] \;\leqslant\; e^{-\frac{1}{2}\delta^2\mu}.$$

3. As above, but we assume that $\varepsilon = \frac{1}{2} - \frac{1}{n}$ where n is the length of the input.

4. Prove that $\mathsf{RP} \cap \text{co-}\mathsf{RP} = \mathsf{ZPP}$.

5. Prove that $\mathsf{P} \subseteq \mathsf{RP} \subseteq \mathsf{NP} \subseteq \mathsf{PP} \subseteq \mathsf{PSpace}$.

The exercises above can be used to prove the following diagram of inclusions:



6. Prove that RP is closed under union, concatenation and Kleene star.

7. Prove that BPP is closed under union, complementation, concatenation and Kleene star.

8. Prove that $\mathsf{BPP}/\mathsf{Poly} = \mathsf{P}/\mathsf{Poly}$.

Reminder: a decision problem L is in P/Poly *if there is a sequence of polynomial sized strings $w_0, w_1, w_2, w_3, \ldots$ (called* advice*) and a polynomial time algorithm $A(x, w_{|x|})$ deciding if $x \in L$; that is, the algorithm is additionally shown an advice string dependent on the length of x. Note that the sequence $w_0, w_1, w_2, \ldots$ doesn't even have to be computable.*

$\mathsf{BPP}/\mathsf{Poly}$ *is defined analogously, but the algorithm may have $\leqslant \frac{1}{4}$ two-way error.*

$\mathsf{BPP} \subseteq \mathsf{P}/\mathsf{Poly}$ *was proved in the lecture (Adleman's theorem).*

9. *(exam '17)* Assume that there exists a polynomial time deterministic algorithm A which approximates with $\frac{2}{5}$ error the probability that a given circuit C with n inputs accepts a random n-bit input. Formally, given a circuit $C(x_1, \ldots, x_n)$, the algorithm computes a rational number $A(C)$ such that

$$|\mathbb{P}[C(x_1, \ldots, x_n) = 1] - A(C)| \leqslant \frac{2}{5}.$$

Prove that the existence of such an algorithm implies $\mathsf{P} = \mathsf{BPP}$.