Exercises on Randomized Complexity
CSCI 6114 Fall 2023

Joshua A. Grochow

Released: Tuesday November 7, 2023
Due: Monday November 13, 2023

The $\mathsf{BP}\cdot$ complexity class operator is defined as follows; $L \in \mathsf{BP} \cdot \mathcal{C}$ if there is a language $L_V \in \mathcal{C}$ ("$_V$" for "verifier") and a polynomial p such that for all strings x,

$$x \in L \Rightarrow Pr_{r \in \{0,1\}^{p(n)}}[(x,r) \in L_V] \geq 3/4$$
$$x \notin L \Rightarrow Pr_{r \in \{0,1\}^{p(n)}}[(x,r) \in L_V] \leq 1/4$$

Reading before class on Thursday Nov 9

- Köbler, Schöning, and Torán pp. 68–71 on probability amplification.

In-Class Exercises Tuesday

1. Define $\mathsf{BPP} = \mathsf{BP} \cdot \mathsf{P}$.
   (a) Show that $\mathsf{co} \cdot \mathsf{BP} \cdot \mathcal{C} = \mathsf{BP} \cdot \mathsf{co}\mathcal{C}$ for any class $\mathcal{C}$. (Recall: $L^c = \{x \in \Sigma^* : x \notin L\}$ and $\mathsf{co} \cdot \mathcal{C} = \{L : L^c \in \mathcal{C}\}$.)
   (b) Use the preceding to conclude that BPP is closed under complement, that is, $\mathsf{BPP} = \mathsf{coBPP}$.

2. We say that a decision problem A is *(polynomial-time) majority reducible* to a decision problem B, denoted $A \leq^p_{maj} B$, if there is a polynomial-time function $r \in \mathsf{FP}$ such that, for each input x, $r(x)$ outputs a tuple of strings, $r(x) = (y_1, \dots, y_{poly(|x|)})$, and for all strings x,

   $$x \in A \iff \text{More than half of the } y_i \text{ are in } B.$$

   A class $\mathcal{C}$ is *closed under majority reductions* if $B \in \mathcal{C}$ and $A \leq^p_{maj} B$ implies $A \in \mathcal{C}$.
   (a) Show that P is closed under majority reductions.
   (b) Show that NP is closed under majority reductions.

In-Class Exercises Thursday

3. Show that if $\mathcal{C}$ is a class that is closed under majority reductions, then $\mathsf{BP} \cdot \mathsf{BP} \cdot \mathcal{C} = \mathsf{BP} \cdot \mathcal{C}$.

4. (a) (**This one is important!** Gets used all over the place.) Show that if $\mathcal{C}$ is closed under majority reductions, then $\exists \cdot \mathsf{BP} \cdot \mathcal{C} \subseteq \mathsf{BP} \cdot \exists \cdot \mathcal{C}$.

(b) We define the classes $\mathsf{MA} = \exists \cdot \mathsf{BPP}$ and $\mathsf{AM} = \mathsf{BP} \cdot \mathsf{NP}$. Show that $\mathsf{MA} \subseteq \mathsf{AM}$.

(c) Show that $\mathsf{NP} \cup \mathsf{BPP} \subseteq \mathsf{MA}$.

(d) Using complexity class operators and previous parts, show that if $\mathcal{C}$ is closed under majority reductions, then $\forall \cdot \mathsf{BP} \cdot \mathcal{C} \subseteq \mathsf{BP} \cdot \forall \cdot \mathcal{C}$. (That is: *don't* re-do a similar proof to part (a), instead use part (a) directly and some things you know about complexity class operators to prove this result.)

5. Define the "Arthur–Merlin hierarchy" by extending the above, e.g.

$$\mathsf{AMA} = \mathsf{BP} \cdot \mathsf{MA}$$
$$\mathsf{MAM} = \exists \cdot \mathsf{AM},$$

and similarly for more letters. That is, define

$$\mathsf{AM}[k] = \mathsf{BP} \cdot \mathsf{MA}[k-1]$$
$$\mathsf{MA}[k] = \exists \cdot \mathsf{AM}[k-1],$$

with $\mathsf{AM}[1] = \mathsf{AM}$ and $\mathsf{MA}[1] = \mathsf{MA}$.

Show that this hierarchy collapses: for all constant k (independent of input size), $\mathsf{AM}[k] \cup \mathsf{MA}[k] \subseteq \mathsf{AM}$. (Food for thought: what happens if we allow a number of alternations between strong majority and $\exists$ quantifiers that depends on the input size? The answer may surprise you!)

Next week's exercises

6. (a) Show that $\mathsf{AM} \subseteq \Pi_2\mathsf{P}$.

(b) Show that $\mathsf{MA} \subseteq \Sigma_2\mathsf{P} \cap \Pi_2\mathsf{P}$. (Note how much stronger this is than merely $\mathsf{BPP} \subseteq \Sigma_2\mathsf{P} \cap \Pi_2\mathsf{P}$!)

7. (a) Show that if $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{PH} = \mathsf{BPP}$. *Hint:* Use induction, Exercise 4(a), and Exercise 3 to show that $\mathsf{NP} \subseteq \mathsf{BPP} \Rightarrow \mathsf{PH} \subseteq \mathsf{BPP}$.

(b) Show that if $\mathsf{NP} \subseteq \mathsf{coAM}$, then $\mathsf{PH} = \mathsf{AM}$. *Hint:* Similar to previous part, playing around with complexity class operators to show that $\mathsf{NP} \subseteq \mathsf{coAM} \Rightarrow \mathsf{PH} \subseteq \mathsf{coAM}$.

8. Prove that if Graph Isomorphism is NP-complete, then PH collapses to the second level.

Optional Homework Exercises (Side Quest): BPP and oracles

9. (a) Show that BPP is closed under $\leq_T^p$ reductions, that is, that $\mathsf{P}^{\mathsf{BPP}} = \mathsf{BPP}$.

(b) Show that BPP is self-low, that is, $\mathsf{BPP}^{\mathsf{BPP}} = \mathsf{BPP}$.

10. Show that for all classes $\mathcal{C}$, we have $\mathsf{BP} \cdot \mathcal{C} \subseteq \mathsf{BPP}^{\mathcal{C}}$.

11. Show that NP^X is closed under majority reductions for any oracle X. Use the oracle characterization of PH to show immediately that $\Sigma_k\mathsf{P}$ (for all k) and PH are all closed under majority reductions.

12. (a) If L is in BPP, and p is a polynomial, show that $L' = \{(1^n, x_1, \ldots, x_{p(n)}) : x_i \in L \text{ for all } i\}$ is also in BPP.

(b) Show that $\mathsf{NP}^{\mathsf{BPP}} = \mathsf{NP}^{\mathsf{BPP}[1]}$, where the latter means NP with a BPP oracle, but it only queries the oracle once. *Hint:* Use nondeterminism to guess the oracle answers, and use the one query at the end to verify all the guesses at once, using part (a).

(c) Show that $\mathsf{NP}^{\mathsf{BPP}} \subseteq \mathsf{BPP}^{\mathsf{NP}}$. *Hint:* With the previous part of this exercise, this part becomes closely related to Exercise 4.

(d) Use the previous part and the oracle characterization of PH to give an alternative proof that if $\mathsf{NP} \subseteq \mathsf{BPP}$ then $\mathsf{PH} \subseteq \mathsf{BPP}$.

Resources

- Our approach to this material is closest to that in Chapter 2 of Köbler, Schöning, and Torán.

- Arora & Barak Section 8.4.3 covers the result about NP-completeness of GI implying collapse of PH. The rest of their Chapter 8 covers interactive proofs more generally. (Note: they have an exercise to show that $\mathsf{AM} \subseteq \Sigma_3\mathsf{P}$, but in fact we will see it is contained in $\Sigma_2\mathsf{P}$.)

- The result about GI is also covered in Homer & Selman Section 10.5. The rest of Chapter 10 covers probabilistic classes such as BPP (and friends); their Section 12.3 covers Arthur–Merlin games, while the rest of their Chapter 12 covers more general interactive proofs.

- Zachos, S. Probabilistic quantifiers and games, *J. Comput. Syst. Sci.* 36(3):433–451, 1988. doi:10.1016/0022-0000(88)90037-2

- **Warning!** There is another class called "$\exists\mathsf{BPP}$", but it is not the same as $\exists \cdot \mathsf{BPP} = \mathsf{MA}$. See the Complexity Zoo entry for the difference (it has to do with how the randomized machines behave on all witnesses vs how they behave only on the one accepted witness).