University of Maryland
CMSC652 — Complexity Theory
Professor Jonathan Katz

Final Exam

Instructions:

- The completed exam must be turned in by 3:30 on Dec. 19. You may hand it to me in person or (1) email me a pdf; (2) slide it under my door; (3) put it in my CS mailbox on the first floor. In the latter two cases, you should follow up with an email to make sure I received it.
- You may use any results from class (plus course notes) or the Arora-Barak textbook, but no other sources.
- Show your work for partial credit.

1. **(2 points)** What was your favorite thing you learned this semester?

2. **(14 points)** Consider the promise problem

$$\begin{aligned}\Pi_Y &= \{(\varphi,\varphi') : \varphi \in \overline{\mathsf{SAT}}, \varphi' \in \mathsf{SAT}\}\\ \Pi_N &= \{(\varphi,\varphi') : \varphi \in \mathsf{SAT}, \varphi' \in \overline{\mathsf{SAT}}\}.\end{aligned}$$

Show that if this problem is in promise-$\mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.

3. **(30 points)** Language L is in $\mathcal{BP} \cdot \mathcal{NP}$ if it has a "randomized Karp reduction" to 3-SAT; namely, if there is a probabilistic poly-time Turing machine M such that

$$\begin{aligned}x \in L &\Leftrightarrow \Pr[M(x) \in 3\text{-}\mathsf{SAT}] \geq 3/4\\ x \notin L &\Leftrightarrow \Pr[M(x) \in 3\text{-}\mathsf{SAT}] \leq 1/4.\end{aligned}$$

   (a) Sketch a proof that the error probability, above, can be reduced to any inverse polynomial without changing the definition of the class.
   (b) Prove that $\mathcal{BP} \cdot \mathcal{NP} \subseteq \mathcal{NP}_{/\mathsf{poly}}$. (Class $\mathcal{NP}_{/\mathsf{poly}}$ is defined in Exercise 7.7.)
   (c) Prove that $\mathcal{BP} \cdot \mathcal{NP} \subseteq \Sigma_3$.
   (d) Prove that $\mathcal{BP} \cdot \mathcal{NP} = \mathbf{AM}$.

4. **(18 points)** Consider the proof that $\mathsf{co}\mathcal{NP} \subseteq \mathcal{IP}$ from lecture 18. Show that if the verifier chooses (and sends to the prover) all its random coins in advance, than a cheating prover can convince the verifier of a false statement with probability (essentially) 1. (For simplicity, consider the formula $\varphi(x) = x$, which is not in $\overline{\mathsf{SAT}}$.)

5. **(18 points)** Let (Π_Y, Π_N) denote the promise problem given by

$$\begin{aligned}\Pi_Y &= \{\varphi \mid \varphi \text{ is a boolean formula with 8 satisfying assignments}\}\\ \Pi_N &= \{\varphi \mid \varphi \text{ is a boolean formula with no satisfying assignments}\}.\end{aligned}$$

Prove that if (Π_Y, Π_N) is in promise-$\mathcal{RP}$, then $\mathcal{NP} \subseteq \mathcal{RP}$.

6. **(18 points)** In class we showed that parity cannot be computed by polynomial-size, constant-depth circuits composed of NOT gates and (unbounded fan-in) AND and OR gates. Extend this to show that parity cannot be computed by polynomial-size, constant-depth circuits even if we allow unbounded fan-in "mod 3" gates that output 0 iff the sum of their inputs is 0 modulo 3.