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

\[ \Pi_Y = \{ (\varphi, \varphi') : \varphi \in \text{SAT}, \varphi' \in \text{SAT} \} \]
\[ \Pi_N = \{ (\varphi, \varphi') : \varphi \in \text{SAT}, \varphi' \in \text{SAT} \}. \]

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

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

\[ x \in L \iff \Pr[M(x) \in 3\text{-SAT}] \geq \frac{3}{4} \]
\[ x \notin L \iff \Pr[M(x) \in 3\text{-SAT}] \leq \frac{1}{4}. \]

(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 \( \text{BPP} \cdot \text{NP} \subseteq \text{NP}/\text{poly} \). (Class \( \text{NP}/\text{poly} \) is defined in Exercise 7.7.)

(c) Prove that \( \text{BPP} \cdot \text{NP} \subseteq \Sigma_3 \).

(d) Prove that \( \text{BPP} \cdot \text{NP} = \text{AM} \).

4. (18 points) Consider the proof that \( \text{coNP} \subseteq \text{IP} \) from lecture 18. Show that if the verifier chooses (and sends to the prover) all its random coins in advance, then 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 \( \overline{\text{SAT}} \).)

5. (18 points) Let \( (\Pi_Y, \Pi_N) \) denote the promise problem given by

\[ \Pi_Y = \{ \varphi \mid \varphi \text{ is a boolean formula with 8 satisfying assignments} \} \]
\[ \Pi_N = \{ \varphi \mid \varphi \text{ is a boolean formula with no satisfying assignments} \}. \]

Prove that if \( (\Pi_Y, \Pi_N) \) 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.