

## CS 509: Problem Set 4

### Due October November 17 - Note Extension

**Problem 1:** Suppose that  $(P, V)$  is a perfectly complete interactive proof system for  $L$ , with error  $\frac{1}{4}$ , where  $V$  runs in polynomial time, flipping public coins.

- A. Show that we can replace  $V$  with a verifier  $V'$  such that,
1.  $V'$  runs in polynomial time and logarithmic space, and throws private coins.
  2.  $x \in L$ ,  $(P, V')$  will accept with probability 1.
  3. If  $x \notin L$ ,  $(P, V')$  will reject with non-negligible probability (i.e.,  $1/|x|^{O(1)}$ ).

**Hint:** Look at a random section of the tableau corresponding to  $(P, V)$  on input  $x$

- B. Conclude that there exists a perfectly complete interactive proof system  $(P', V')$  for  $L$ , with error  $\frac{1}{4}$ , where  $V'$  run in polynomial time and logarithmic space (flipping private coins).

**Problem 2:** Recall that a language  $L$  is in RP if there is a probabilistic polynomial-time decision procedure  $D$  such that

- If  $x \in L$ ,  $\Pr[D \text{ accepts } x] \geq \frac{1}{2}$ , and
- If  $x \notin L$ ,  $\Pr[D \text{ accepts } x] = 0$ .

- A. Show that  $\text{RP} \subseteq \text{NP}$ .
- B. (\*) Show that if  $\text{NP} \subseteq \text{BPP}$  then  $\text{NP} = \text{RP}$ .

**Problem 3:** (\*) The solution to Problem 1 requires that the time-space bounded verifier  $V'$  use private coins. Show that if a poly-time, log-space verifier uses only public coins, then the language being accepted is in BPP (probably P suffices).

**Hint:** Show how compute ones optimal strategy and probability of winning given any (known) configuration of the verifier. It is easier if you include the “step count” in the state of the verifier, to make things acyclic.

**Problem 4:** (Sipser, 10.14) Show that the class of nondeterministic polynomial time with a SAT oracle is equal to  $\Sigma_2^{\text{poly}}$ . (In Sipser’s notation, show that  $\text{NP}^{\text{SAT}} = \Sigma_2 P$ .) Note that we showed the analog to this result in the recursion theory part of this course.

**Problem 5:** (\*) (Games against nature) We say that  $L$  has a “game against nature” if there is an Arthur-Merlin proof system  $(P, V)$  for  $L$  such that

- If  $x \in L$  then  $(P, V)$  accepts with probability  $> \frac{1}{2}$ .
- If  $x \notin L$  then  $(\hat{P}, V)$  accepts with probability  $\leq \frac{1}{2}$  for any  $\hat{P}$ .

(That is, we have a proof system in which we do not have a “gap” in the accept and reject probabilities. For this problem, let us assume that  $V$  flips a fixed (polynomial) number of coins. Show that if  $L$  has a game against nature, then  $L \in \text{PSPACE}$ .

**Hint:** Convert to an alternating poly-time game between entities arguing over the probability that  $(P, V)$  accepts on input  $x$ .