Homework 11
Due Wed May 21, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

22. Recall our definition of the class $\mathsf{IP}_{\varepsilon^-,\varepsilon^+}$: We say that a language $L \subseteq \{0,1\}^*$ is in this class if there is a polynomial-time verifier V that uses a random string r and has the following properties, where P is an arbitrarily powerful prover that interacts with V:

$$x \in L \implies \exists\, P: \Pr_r[P * V \text{ rejects } (x,r)] \le \varepsilon^- ,$$
$$x \notin L \implies \forall\, P: \Pr_r[P * V \text{ accepts } (x,r)] \le \varepsilon^+ .$$

We defined $\mathsf{IP} = \mathsf{IP}_{\frac{1}{3},\frac{1}{3}}$ and remarked that the choice of the constants isn't terribly important, as can be proved by suitable repetition and Chernoff bound analysis. We also remarked that ε^- can be made zero (though not by simple repetition): we shall eventually see a proof of this. Finally, we remarked that ε^+ cannot be made zero because it makes the underlying class boil down to plain old NP.

Justify this last remark. Specifically, prove that $\mathsf{IP}_{\frac{1}{3},0} = \mathsf{NP}$. [2 points]

23. Let p be a prime. This problem involves the group $\mathbb{Z}_p$, consisting of integers $\{1,2,\ldots,p-1\}$ with multiplication performed mod p. At some point you will need to use the fact that every element of $\mathbb{Z}_p$ has a multiplicative inverse mod p (that's what makes it a group).

The *quadratic residuosity problem* asks whether a given integer is a square mod p. The brute force solution is to try out all elements of $\mathbb{Z}_p$ and compute the square of each, but it takes time proportional to p, which is exponential in the input length. But one can give interesting interactive proofs for this problem. To be precise, define the languages

$$\text{QR} = \{\langle p,x\rangle : p \text{ is prime, } x \in \mathbb{Z}_p, \text{ and } \exists\, y \in \mathbb{Z}_p\ (y^2 \equiv x \pmod{p})\} ,$$
$$\text{QNR} = \{\langle p,x\rangle : p \text{ is prime, } x \in \mathbb{Z}_p, \text{ and } \forall\, y \in \mathbb{Z}_p\ (y^2 \not\equiv x \pmod{p})\} .$$

The acronyms denote "quadratic residue" and "quadratic non-residue," respectively.

Prove that both these languages are in IP and that one of these is in fact in NP. [2 points]

Hint: Your protocol for one of the languages should mimic the one we gave in class for NONISO. Suppose $\langle p,x\rangle \in$ QNR and $z \in \mathbb{Z}_P$. What can you say about $xz^2 \bmod p$?

24. In our definition of IP, we allowed the verifier to ask randomly generated questions, but did not allow the prover to give randomly generated answers. Define the class IP' to be similar to IP, except that the prover may also use a random string to compute his answers. The prover's random string is independent of the verifier's. Prove that $\mathsf{IP}' = \mathsf{IP}$. [2 points]