# 15-251: Great Theoretical Ideas In Computer Science

## Recitation 12

## Don't Share Your Passwords!

Suppose a prime $p$ and a generator $g \in \mathbb{Z}_p^*$ are public, and we have some private password $x$. Further, we make $g^x \pmod p$ public as well. Our goal is to convince an observer that we know $x$, without actually revealing $x$ or other useful information (say, with probability $1/2$). How can this be done?

## Rectangle Definitions

Recall that a rectangle is a set of the form $S \times T$, where $S, T \subseteq \{0,1\}^n$. Show that a set $\mathcal{R} \subseteq \{0,1\}^n \times \{0,1\}^n$ is a rectangle if and only if it has the property that $(x,y) \in \mathcal{R}, (x',y') \in \mathcal{R} \implies (x,y') \in \mathcal{R}, (x',y) \in \mathcal{R}$.

## Coin Flips are Free

Recall the randomized communication complexity model introduced in class. There, the players were allowed to individually flip coins, and make decisions based on the outcomes of those coin flips. We showed that $\mathbf{R}^\epsilon(\text{EQ}) = O(\log n)$, where the error probability $\epsilon = 1/n$. In this question we'll consider a slightly different randomized communication complexity model. In this new model, we'll assume that the players share a public coin. Whenever one of the players flips this coin, the other player automatically sees the outcome of the coin flip (without them communicating any bits). Show that in this model, there is a randomized protocol for EQ of cost $O(1)$ and error probability $1/2^{300}$. What is the exact relationship between the cost and the error probability of your protocol?

## Another Equality Communication

(a) Let $x$ and $y$ be two distinct $n$-bit integers. Let $p$ be a uniformly chosen random prime in the range $2 \le p \le 4n^2$. Obtain an upper bound for $\Pr[x = y \pmod p]$ of the form $1/\text{poly}(n)$ (must decrease as $n$ increases).
Hint: Use Homework 8, Question 5.

(b) Show that $\mathbf{R}^\epsilon(EQ) = O(\log n)$ using a protocol that is different than the one presented in class. What is the error probability of your protocol?