Last Time

- Definition of Hard Core Predicates
- Warm up proofs of Goldreich-Levin Theorem
- Markov, Chebyshev, and Chernoff bounds
Today

- Full proof of the Goldreich Levin Theorem
Today

- Full proof of the Goldreich Levin Theorem
- Scribe notes volunteers?
Recall: Hard Core Predicates

**Definition (Hard Core Predicate)**

A predicate $h : \{0, 1\}^* \to \{0, 1\}$ is a hard-core predicate for $f(\cdot)$ if $h$ is efficiently computable given $x$ and there exists a negligible function $\nu$ s.t. for every non-uniform PPT adversary $A$ and $\forall n \in \mathbb{N}$:

$$\Pr\left[ x \leftarrow \{0, 1\}^n : A(1^n, f(x)) = h(x) \right] \leq \frac{1}{2} + \nu(n).$$
Recall: Goldreich-Levin Theorem

**Theorem (Goldreich-Levin)**

Let $f$ be a OWF (OWP). Define function

$$g(x, r) = (f(x), r)$$

where $|x| = |r|$. Then $g$ is a OWF (OWP) and

$$h(x, r) = \langle x, r \rangle$$

is a hard-core predicate for $g$. 
Assumption: Given $g(x, r) = (f(x), r)$, for every $x$, adversary $A$ outputs $h(x, r)$ with probability $\frac{3}{4} + \varepsilon(n)$ over the choices of $r$.

$$\forall x: \Pr_r[A(f(x), r) = h(x, r)] \geq \frac{3}{4} + \varepsilon(n).$$

Main Idea: Split each query into two queries s.t. each query individually looks random

Inverter $B$:

- Let $a := A(f(x), e_i \oplus r)$ and $b := A(f(x), r)$, for $r \leftarrow \{0, 1\}^n$
- Compute $c := a \oplus b$ as a guess for $x_i^*$
- Repeat many times to get many such $c$ and take majority to get $x_i^*$
- Output $x^* = x_1^* \ldots x_n^*$
Outline of the full proof

- Pairwise Independence
- Getting rid of $x$ in the probabilities:
  \[ \text{GOOD} = \left\{ x : \Pr_r[A(f(x), r) = h(x, r)] \geq \frac{1}{2} + \frac{\varepsilon(n)}{2} \right\} \]
- Hit GOOD with probability $\varepsilon/2$ or more.
- Chebyshev: $\Pr [|X - pm| > \delta m] \leq \frac{1}{4\delta^2 m}$ for $X = \sum_{i=1}^{m} X_i$ for pairwise independent $X_i$’s.
- $(b_1, b_2, b_1 \oplus b_2)$ are pairwise independent
- $(b_1, \ldots b_{\ell}, \oplus_{S_i} b_S)$ are also pairwise independent where $\ell = \ln m$ and $m = n/2\varepsilon^2$.
- $B$ that inverts $f$ for good $x$ with probability more than $1/2$.
- $A$ inverts $f$ using $B$ w/ prob. $\varepsilon/4$ or more.