Next question: How do we build $G: \{0,1\}^n \to \{0,1\}^{n+1}$?

- Practice: Heuristic construction
- Theory: Provably from any OWF.

↳ Fundamental concept: HARD-CORE bits. They are bits of info about x that are hard to compute given $y = f(x)$.
It's a predicate $h(x)$ s.t. $h(x) \in \{0,1\}$

is HARD to compute given $f(x)$

(w.p. better than $1/2$).

First: can there be a single h s.t.

h is HARD-CORE $\forall f$ (OWF)?

Impossible! Why? Provable $\hat{f}$ OWF

s.t. h not hard-core for $\hat{f}$!

Fix any h; take f a OWF. Consider:

$$\hat{f}(x) = h(x) \,\|\, f(x).$$

h not hard-core for $\hat{f}$.

$\hat{f}$ is still OWF ?

$$\hat{A} \xleftarrow{\;b \,\|\, y\;} A \xleftarrow{\;y = f(x)\;} \mathcal{C}^{owf}$$

$$b \leftarrow \{0,1\} \qquad\qquad x \leftarrow \mathcal{X}$$

$$\Pr[\hat{A} \text{ wins}] \geq \left(\frac{1}{2} \cdot \Pr[\hat{A}(h(x) \,\|\, y) \text{ wins}] \right)$$

$$\Pr[\hat{A} \text{ wins}] = \Pr[\hat{A}(b,y) \text{ wins} \wedge b = h(x)]$$

$$+ \Pr[\hat{A}(b,y) \text{ wins} \wedge b \neq h(x)]$$

$$\geq \frac{1}{2} \cdot \Pr[\hat{A}(h(x),y) \text{ wins}]$$

$$\geq 1/2 \cdot 1/poly \geq 1/poly .$$

Solution: Swap the quantifiers.

DEF Let $f: \{0,1\}^n \to \{0,1\}^n$ a OWF.
Then h is HARD-CORE for f if:

(i) $\forall$ PPT P

$$\Pr\left[P(y) = h(x) : \begin{array}{l} x \leftarrow \{0,1\}^n \\ y = f(x) \end{array} \right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

(ii)

$\Leftrightarrow$ ALTERNATIVE DEFINITION.

$$(f(x), h(x)) \approx_c (f(x), b)$$

Made with Goodnotes

$x \leftarrow \{0,1\}^n$, $b \leftarrow \{0,1\}$.

Exercise: (NN) $\Rightarrow$ (N)

Also true: (N) $\Rightarrow$ (NN).

Thm. If one-way permutations (OWP) exist $f : \{0,1\}^n \to \{0,1\}^n$, then $\exists$ $G : \{0,1\}^n \to \{0,1\}^{n+1}$ a PRG.

Dim. Trivial: $G(s) = f(s) \| h(s)$

$$G(U_n) \equiv f(U_n) \| h(U_n)$$

$$\approx_c f(U_n) \,\|\, U_1$$

$$\equiv U_{n+1} \qquad \blacksquare$$

THM If OWF $\exists$ const also PRG with $\ell(n) = 1$ const.

All is left is to build h for any given f.

THM (GOLDREICH-LEVIN) Let $f : \{0,1\}^n \to$

$\{0,1\}^n$ be a owf. Then, $g(x, r) = (f(x), r)$ is also owf $g: \{0,1\}^{2n} \to \{0,1\}^{2n}$ with hard-core predicate:

$$h(x, r) = \bigoplus_{i=1}^{n} x_i \cdot r_i .$$

$$= \langle \vec{x}, \vec{r} \rangle \bmod 2$$

Proof notes: If $\exists$ PPT $\mathcal{P}$ for $h(x, r)$, then $\exists$ PPT A breaking g:

In particular A can find x.

Simple cases:

- Assume $\mathcal{P}$ is SUPER GOOD:

$$\forall\ x, r \quad \Pr[\mathcal{P}(y) = h(x, r)] = 1$$

Then A will just run $\mathcal{P}$ on

$$y_1 = (f(x), \vec{e}_1) \qquad \vec{e}_i = (0 \cdots 0 1 0 \cdots) \atop \hookrightarrow i$$

$$y_2 = (f(x), \vec{e}_2)$$

- Second note: Assume that P is VERY GOOD; $\forall x \in \{0,1\}^n$

$$\Pr_r\left[P(f(x), r) = h(x,r) \right] \geq 3/4 + 1/\mathrm{poly}$$

Run P on r random and

$$r \oplus e_i$$

$$x_i = \langle x, r \oplus e_i \rangle \oplus \langle x, r \rangle = \langle x, e_i \rangle$$

Made with Goodnotes

Still you can simplify by relaxing
necessity of many queries.