22/9/2015 Russell's course, lec 8.

Derandomization vs. circuits.

worst-case to average-case BF = VW

Derandomization to AG IKW / AM

Shown last time: if there is a size poly(m) $\frac{1}{2} - 1/m$-hard fn f, on $n^{1/3}$ bits, then there is a secure PRG, G s.t. $\{0,1\}^{O(n^2)} \to \{0,1\}^n$, G-BPR BP is hard for size n

f_{wc} : $(m_{wc}, 0)$-hard $\quad f_{wc} \leftarrow = M_{wc} \to$ noisy channel $\to$ $\hat{c}$ $\quad$ error-correcting code: STV

$\downarrow$

f_{ach} : $\{m_{ach}, 1/2 - 1/m_{ach}\}$ $\to$ F_{ae} $1/2 - 1/m_{ae}$: $\hat{G}_{ae}$ $\quad$ (k-degree locally-d ecc)

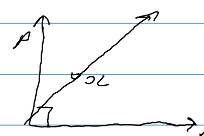
RMS: $f_{wc} = \{x_1, \ldots x_n\} \to \{0,1\}$. Let $p \geq n^2$

$f_{wc}(x_1, \ldots x_n) = \sum_S \alpha_S \prod_{i \in S} x_i$ — unique multilinear extension mod p.

$f_{sh} = f_{wc}$ mod p. $\quad f_{wc} : \mathbb{Z}_p^n \to \mathbb{Z}_p$.

Claim: if C computes f_{sh} on $1 - 1/3n$ fract. of inputs, then $\exists$ C', $|c'| \geq |c|$, which computes f_{wc} on every input.

Let c'' be prob. circ. $\forall x$ $\text{Prob}\left(c''(x) = f_{sh}\right] \geq 2/3$



BF, Lip: random self-reducibility

In high dim, $\bar{y} = \bar{x} + z\bar{a}$ is the line. $f_{sh}(\bar{y}) = \sum_S \alpha_S \prod_{i \in S} (x_i + z\alpha_i) = f(z)$

$f_{sh}(\bar{x}) = f_{\ell}(0)$. If knew $f\ell$ at $\geq 1 \ldots z = n+1$, could interpolate. $\deg(f\ell) = n$

to get $f\ell(0)$: $\quad$ C'': Pick $\bar{a}$ at random. For $z = 1 \ldots z = n+1$, guess that $C(\bar{x} + z\bar{a}) = f\ell(z)$

Interpolate to get $f\ell(z)$ as poly. Output $f\ell(0) = f_{sh}(\bar{x})$

$\text{Prob}\left[c''(x) \neq f_{sh}(x)\right] \leq \text{prob}\left[\exists z, z = 1 \ldots n+1, C(\bar{x} + z\bar{a}) \neq f\ell(z)\right]$

Since $\bar{x} + z\bar{a}$ is a random point, $\leq (n+1)\left(\text{Prob}\left[C(\bar{r}) \neq f_{sh}(\bar{r})\right]\right] \leq 1/3$.

Let C' run C'' poly(n) times and take majority, w/ best values for $\bar{a}$.

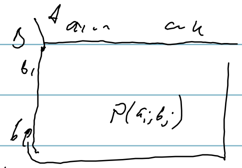
(similar to proving BPP $\subseteq$ P/poly). $\quad$ fsn : (H)

worst-case-hard $\to$ somewhat hard fn $\to$ hard core $\to$ direct product construct - at most as hard as random guessing

Let f_{sh} be an (m, ϵ)-hard problem on $\{0,1\}^{n_{sh}}$. Then $\exists H \subseteq \{0,1\}^{n_{sh}}$, $|H| \geq \Omega(\epsilon \cdot 2^n)$

$\forall c'$, $|c'| \approx m'^{\text{poly}(\delta)}$, $\text{Prob}_{x \in H}\left[c'(x) \neq f_{sh}(x)\right] \geq 1/2 - \delta$.

Von Neumann min-max thm:



Zero-sum game. $P(a_i; b_j)$: payoff that A pays B.

Mixed strategy: dist. over moves. $\max_{\alpha} \min_{b} E_{a \in \alpha}[P_{a,b}] = \min_{\beta} \max_{a} E_{b \in \beta}[P_{a,b}]$

"hard core set game" A: circuit C to try computing f_{sh}. B: $S \subseteq \{0,1\}^n$, $|S| \geq \epsilon \cdot 2^n$, $P_{c,S} = \text{Prob}_{x \in S}\{f_{sh}(x) = C(x)\}$

$- \text{Prob}_{x \in S}\left[f_{sh}(x) \neq C(x)\right]$. If p's-off (for A) is $> \delta$, then A has a dist. of ckts so that

$\forall S$, $|S| \geq \epsilon \cdot 2^n$ this $> \delta$. Let $\hat{S}$: $\{x \mid \text{Prob}_c\left(C(x) = f(x)\right] \leq 1/2 + \delta/2\}$.

Since $\hat{S}$ is not a good move for B, $|\hat{S}| < \epsilon \cdot 2^n$. Let c' be maj. of $\sim n/\delta^2$ circ from C, correct on all

but on set S. XOR: picks $f_{ach}(x_1, \ldots x_k) = f_{sh}(x_1) \oplus \ldots \oplus f_{sh}(x_k)$ - $k \approx n/\epsilon$.

Say $C(x_1 \ldots x_k) = f_{ach}(x_1, \ldots x_k)$ w. prob $1/2 + \delta$. Pick x_i from H w/ prob ϵ^{-k} H.