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

Derandomization vs. circuits.

worst-case to average-case $\exists$ f $\in$ EW

Derandomization to PG IKW / AM

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

f_{wc} : $(m_{wc}, 0)$-hard $\quad f_{wc} \leftarrow = M_{wc}$ — noisy channel → error-correcting code: SJV

$\downarrow$

f_{ach} : $\{m_{ach}, 1/2 - 1/m_{ach}\}$ → F_{ac} $1/2 - 1/m_{ac}$: decoder (majority, locally-decodable ECC)

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

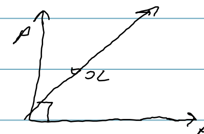
$f_{wc}(x_1, \dots x_n) = \sum_S \alpha_S \prod_{i \in S} x_i$ — unique multilinear expansion mod p.

$f_{sh} = f_{wc} \bmod p$. $\quad f_{wc}: Z_p^n \to Z_p$.

Claim: If C computes f_{sh} on $1 - 1/8n$ fract. of inputs, then $\exists$ C', $|C'| \approx |C|$, which computes f_{wc} on every input.

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

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 know $f\ell$ at $z \neq 1 \dots z = n+1$, could interpolate. $\deg(f\ell) = n$ to get $f\ell(0)$:

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

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

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

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

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

(Similar to proving BPP $\subseteq$ P/poly).

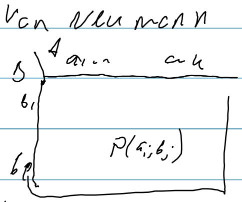
f_{sh}: (HC)

worst-case-hard → somewhat hard fn → hard core → direct product construction, at most as hard as random guessing

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

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

Von Neumann min-max thm:



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

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

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

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

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

Since $\hat{S}$ is not a good move for B, $|\hat{S}| < \varepsilon \cdot 2^n$. Let C' be maj. of $\approx n/\delta^2$ circuits C, correct on all but

dist. of sets S! H: Pick set... $f_{ach}(x_1, \dots x_k) = f_{sh}(x_1) \oplus \dots \oplus f_{sh}(x_k)$ - $k \approx n/\varepsilon$.

See $C(x_1 \dots x_k) = f_{ach}(x_1 \dots x_k)$ w. prob $1/2 + \delta$. Pick x_i from H w. prob ε, $\dots$ $\bar{H}$.