10/30/12
Russell

$f: \{0,1\}^n \to \{0,1\}$

$\forall$ circuits C of size $S(n)$

$$\underset{x}{\text{Prob}}\left[C(x) = f(x)\right] \le \frac{1}{2} + \frac{1}{S(n)}$$

BFNW: worst case hardness $\Rightarrow$ average case hardness.

$A(x,r)$: $r \in \{0,1\}^T$ uniform at random
T = runtime.

$\mathcal{S} = \{s_1 \cdots s_K\}$.

Good $\left|\underset{i}{\text{Prob}}\left[A(x,s_i)\right] - \underset{r}{\text{Prob}}\, A(x,r)\right| \le \frac{1}{T}$. $(\alpha \le 1/3)$

Equiv $\forall C, |C| = T$,

$$\left|\underset{i}{\text{Prob}}\left(C(s_i)\right) - \underset{r}{\text{Prob}}\, C(r)\right| \le 1/T$$

$\Rightarrow$ Deterministic simulation of A (or C) of time
(Time to construct $\mathcal{S}$) + $K \cdot \text{poly}(T)$.

Yao's Next Bit Test (original construction): $\mathcal{S}$ very efficiently sampleable
- but required a cryptographic assumption.

$\mathcal{S}$ = "(T,ϵ)-pseudorandom".

Q1 Derandomization w/ advice: $BPP \subseteq P/poly$
Q2 Universal graph traversals $\Rightarrow$ derandomization of logspace.

Next bit circuit for $\mathcal{S}$, C, at position i s_i - bit at position i
$C(s_1 \cdots s_{i-1})$ is a "guess" for s_i

$$\text{succ}(C,i) = \underset{s \in \mathcal{S}}{\text{Prob}}\left(C(s_1 \cdots s_{i-1}) = s_i\right) - \frac{1}{2}$$

<u>Yao:</u> Equivalence of (T,ε)-pseudorandom + nonexistence of a small next-bit-circuit

<u>Pf</u> Hybrid argument

$\mathcal{S}_T = \mathcal{S}$, $\mathcal{S}_0 = R$ (randomness)

$\mathcal{S}_i$: Pick $s \in \mathcal{S}$, $r_{i+1}, \dots, r_T \in R$

output $s_1, \dots, s_i, r_{i+1}, \dots, r_T$

<u>Assume:</u> $C(S) - C(R) \geq \varepsilon$ (so not pseudorandom)

$$\left(C(\mathcal{S}_T) - C(\mathcal{S}_{T-1})\right) + \dots + \left(C(\mathcal{S}_1) - C(\mathcal{S}_0)\right) \geq \varepsilon$$

So some $C(\mathcal{S}_i) - C(\mathcal{S}_{i-1}) \geq \varepsilon/T$.

C' - randomized circuit.

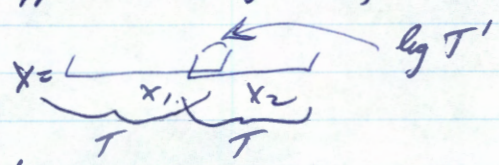
$C' :=$ Pick $r_i \cdots r_T$ at random
If $C(s_1, \dots, s_i, r_i \dots r_T) = T$ output r_i
o/w output $1 - r_i$.

and do the usual calculation. (Hard direction)

Roundabout way to sample n bits:
Use f a hard function
Choose $x_1, \dots x_T \in \{0,1\}^n$
Calculate $f(x_1), \dots, f(x_T) \in \{0,1\}^T$.

Choose $x_1 \; x_T$ - computationally (partially) independent
Knowing any $g_i(x_j)$, $j \neq i$, does not substantially in approximating / guessing $f(x_i)$.

<u>Example</u> $T = 2$



Suppose $C'(x_2, g(x_1)) = f(x_2)$ w/ probability δ.
(1) Fix $T - \lg T'$ bits of $x_1 \setminus x_2$ to maintain the advantage
(2) Recode $g(x_1)$ for T' ways removing values of x_1.
(3) Use C' to approximate $f(x_2)$.

NW construction

m = # of bits to sample; $z_1 \dots z_m$

$A_i \subseteq \{1, \dots m\}$ $|A_i| = n$ $A_i = \{a_{i,1} \dots a_{i,n}\}$

$x_i = z_{a_{i,1}} \dots z_{a_{i,n}} \in \{0,1\}^n$.

$\forall i \neq j$ $|A_i \cap A_j| < \ell$ $(\approx \log T)$.

$\boxed{A_i\text{'s are an } \ell\text{-design}}$

~~Assume~~ Then given $g(x_1) \dots g(x_{i-1})$, still hard to predict $f(x_i)$

Suppose $C'(x_i, g_1(x_1) \dots, g_{i-1}(x_{i-1}))$ predicts $f(x_i)$ w/ prob '$\frac{1}{2}+\varepsilon$'.

(1) Fix bits in $\overline{A_i}$ to maintain the advantage.

(2) For each x_j, $\exists$ at most 2^ℓ possible values available for x_j $j<i$. Give a table of all these values

(3) C simulates G' (a) Look up each x_j in the table.
(b) Feed the info to C'.

Argue as before.

$m << T$ $(m \approx n^2$ or $m = O(n))$

$\ell \lesssim \log T$ (small). ($\ell < m$ of course.)

Let p be prime $n < p < 2n$ (say)

Set $m = p^2$. $m \approx \langle i,j \rangle$ i,j ~~taken mod p~~ $i<n, j<p$

or $m = pn$.

For g a degree $\leq d$, univariate polynomial over $\mathbb{Z}_p$

let $A_g := \{\langle i, g(i) \rangle : i = 1, \dots n\}$.

$|A_g| = n$

$|A_g \cap A_{g'}| \leq \ell$.

Need $T \lesssim p^\ell$ to have enough polynomials

$\ell \approx \frac{\log T}{\log n} << T$.

<u>Theorem (for instance)</u> "Low-end version":

If $\exists f \in EXP$ which is $s(n)$-hard for $s(n) = n^{\omega(1)}$

then $\forall \varepsilon > 0$ $BPP \subseteq DTIME(2^{n^\varepsilon})$.

<u>Pf</u> Let $n = T^\delta$, so f_n is $T^{\omega(1)}$-hard.

Construct $A_1, .. A_T$, $|A_i \cap A_j| \le \frac{\lg T}{\lg n} = \ell = O(1)$,

Let $m = n^2 = T^{2\delta}$.

For all $z_1 .. z_m$, compute $s = f(x_1) .. f(x_T)$

– in total time $2^{n^\delta} \cdot T \cdot 2^m = 2^{T^{2\delta}}$

i.e. subexponential in T.

<u>Theorem</u> "High-end"

If $\exists f \in EXP$, f is $2^{\Omega(n)}$-hard,

then $BPP \subseteq P$.