Hardness vs Randomness

Thm: If SAT requires $2^{\Omega(n)}$ sized circuits $\Longrightarrow$ BPP = P

Digesting the assumption

A1. $\exists A \in E$ s.t. computing $A_n = A \cap \{0,1\}^n$ require ckts of size $2^{\Omega(n)}$ $\forall n \geq n_0$

A2. $\exists A \in E$ size 2^{n^ε}

(H^*) $\exists A \in E$ s.t. $corr(A_n, C_n) \leq 2^{-\varepsilon n}$

$\forall C_n$ ckts of size $2^{\varepsilon n}$

$\Pr_{x \in \{0,1\}^n}[C(x) = A_n(x)] \leq \frac{1}{2} + 2^{-\varepsilon n}$

[IW '97] $(H1) \Longrightarrow (H^*)$

worst-case to avg case.

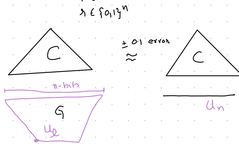
[NW'94] $H^* \Longrightarrow BPP = P$ (today)

Uniformly picking SAT inputs ??

def^n: A PRG of seed length $s = \ell(n)$ is a (family of) functions $(G_\ell)_\ell$ uniformly computable in time $2^{O(\ell)}$ s.t. for all $n \geq n_0$, and all ckts

$C : \{0,1\}^n \to \{0,1\}$ of size $\leq n^3$

$\Pr_{s \in \{0,1\}^t}[C(G(s)) \text{ accepts}] \overset{\pm .01}{\approx} \Pr_{x \in \{0,1\}^n}[C(x) \text{ accepts}]$



AB def^n $\in E$.

We say $G : \{0,1\}^s \to \{0,1\}^n$ is an $S(\ell)$ prg if

- $|G(z)| = S(|z|)$ ~ size?
- $\forall z \in \{0,1\}^s$ the distb^n $G(U_\ell)$ is $(S^3(\ell), .01)$ pseudorandom.

* A distb^n R over $\{0,1\}^n$ is (S, ε) pseudorandom if for circuits of size $\leq S$

$\left| \Pr[C(R) = 1] - \Pr[C(U_m) = 1] \right| < \varepsilon$

↳ uniform distb^n

Lem: $S(\ell)$ - prg $\Longrightarrow$ $BPTIME(S(\ell(n))) \subseteq DTIME(2^{c\ell(n)})$.

Pf: $L \in BPTIME(S(\ell(n)))$

$\exists$ algorithm A on $\{0,1\}^n$ runs in time $O(S(\ell(n)))$ time

$\Pr_{r \in_R \{0,1\}^m}[A(x, r) = L(x)] \geq 2/3$

$m \leq S(\ell(n))$. Replace truly random strings with PRG.

Pick random $z \in \{0,1\}^{\ell(n)}$, run A the prob of $\Pr_{r \in_R \{0,1\}^m}[A(x, G(z)) = L(x)] \geq 2/3 - .01$

Repeat + Take Majority

Con: $2^{\varepsilon \ell}$ PRG $\Longrightarrow$ BPP = P.

Suppose this is false and $\exists$ x (1.0)

$\Pr_z[A(x, G(z)) = L(x)] < 2/3 - 0.1$

Then $\exists$ a distinguisher for our PRG.

This circuit has size $O(S(\ell(n))^2) \leq S(\ell(n))^3$

$n \geq n_0$

Combinatorial Designs

A family of sets $\{S_1, S_2, \ldots, S_m\}$ is said to be an (ℓ, k, r) design if

1. $S_i \subseteq [\ell]$
2. $|S_i| = k$
3. $|S_i \cap S_j| < r \quad i \neq j$

Lemma: Let $c \geq 2$ (say $= 2$) and $\ell = k^c$, $r \leq k$ ⇝ power of 2. and $r \leq k$

$\Downarrow$

(ℓ, k, r) - design $\{S_1, S_2, \ldots, S_m\}$ for $m \leq k^{(c-1)r}$ in time poly(m).

k = power of 2. $\quad k \equiv \mathbb{F}_k$ identify

and $[\ell] \equiv (\mathbb{F}_k \times \mathbb{F}_k)$

For each univariate polynomial

$$P(x) \in (\mathbb{F}_k[x])_{<r}$$

$$S_p = \{(i, P(i)) : i \in \mathbb{F}_k\}$$

Note, k^r such polynomials, we get k^r subset of $\mathbb{F}_k \times \mathbb{F}_k$. Furthermore, since any two poly only agree at r or more places

$\Rightarrow |S_p \cap S_q| < r$ for $p \neq q$.

Lemma (20.15) $f: \{0,1\}^n \to \{0,1\}$ s.t.

$H_{avg}(f) > 2^{2d} \Rightarrow NW_I^f(U_\ell)$ is $(H_{avg}(f), 1/10)$-pseudo random

---

$I \equiv (\ell, n, d)$ design with $n > d$

$\ell > \frac{10n^2}{d}$

$2^{d/10}$ subsets.

$NW_I^f(U_\ell)$ is $(S/10, Y_{10})$-PRG $S = H_{avg}(f)$

it suffices to prove for every $i \in [2^{d/10}]$ there doesn't exist an $S/2$ circuit C

s.t.

$$\Pr_{\substack{z \sim U_\ell \\ R = NW_I^f(z)}}\left[C(R_1, \ldots, R_{i-1}) = R_i\right] \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}$$

↑ suppose this holds

By def^n of NW_I^f

$$\Pr_{\substack{z \sim U_\ell \\ R = NW_I^f(z)}}\left[C(f(z_{I_1}), \ldots, f(z_{I_{i-1}})) \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}} = f(z_{I_i})\right]$$

Focus on $z_{I_i} := z_1$.

$z_2 = z_1^C \equiv [\ell] \setminus z_1$

$z_1 z_2^{z_2} \cdots z_1 z_2^{z_2}$

$$\Pr_{\substack{z \sim U_\ell \\ R = NW_I^f(z)}}\left[C(f(z_{I_1}), \ldots, f(z_{I_{i-1}})) \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}} = f(z_{I_i}) \; (z_1)\right]$$

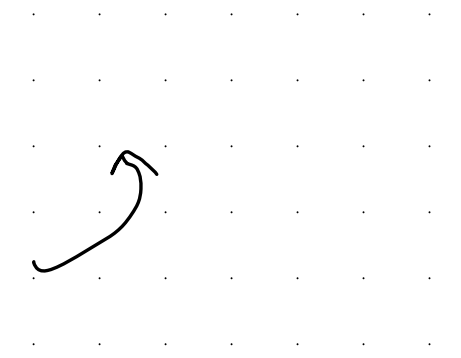
$\Rightarrow$ By averaging principal,

Since, $|I_j \cap I_i| \leq d \quad j \neq i$

$z_1 \longmapsto f_j(z_1, z_2)$ depends on d coordinates of z_1

$\Rightarrow$ each computed by $O(2^d \cdot d)$ size ckt.

$\Rightarrow$ There exist B of size $S/2 + 2^d \cdot d \cdot 2^{d/10}$



$$WSP \geq \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}} > \frac{1}{2} + \frac{1}{S}.$$

$\Rightarrow\Leftarrow$

$H^{avg}(f) > 2^{2d}$

Putting it all together

Thm: $f \in DTIME(2^{O(n)}) \equiv E$

if $H_{worst}(f) \geq 2^{\varepsilon n} \Rightarrow BPP = P$

Pf sketch:

PRG motivation from complexity "intuition" theoretic

$\ell(n) << n$

PRG $G: \{0,1\}^\ell \to \{0,1\}^n$

s.t. $\forall\, x \in \{0,1\}^n$

(*) $\Pr_{x \in \{0,1\}^n}[M(x,1^n) \text{ accepts}] \overset{\pm 0.1}{\approx} \Pr_{s \in \{0,1\}^\ell}[M(x, G(1^\ell)) \text{ accepts}]$

pseudorandom gen that fools M on all x.

M a TM

- Det-time complexity 2^ℓ time (G) · Time of M

(*) fails

$\exists\, x \in \{0,1\}^n \equiv$ non-uniform circuit distinguisher

fools $M_x(r)$ is a distinguisher beating G.

Circuit, we might not know x

Circuit complexity via Naive Cook-Levin thm $O(n^2)$

- By padding all pTM run in linear time for showing BPP = P

Def^n A PRG of seed length $\ell(n)$

- ▷ is uniformly computable in $2^{O(\ell)}$ time.
- ▷ s.t. for all $n \geq n_0$ and all ckts $C: \{0,1\}^n \to \{0,1\}$ of size $\leq n^3$.

$$\Pr_{x \in \{0,1\}^\ell}[C(G(x)) \text{ acc}] \overset{\pm 0.1}{\approx} \Pr_{r \in \{0,1\}^n}[C(r) \text{ accepts}]$$

PRG of [A+B] book

- A distb R over $\{0,1\}^m$ is (S,ε) pseudorandom if

$\Pr_R[C(R) \text{ accpts}] \overset{\pm\varepsilon}{\approx} \Pr_{U_m}[C(U_m) \text{ accepts}]$

No x in the picture. C ckt of size S.

- G is $S(\ell)$ PRG if
  - ▷ $|G(z)| = S(|z|)$ → size param for that string
  - ▷ $G(U_\ell)$ is $S'(\ell)$ Pseudorandom.

Average-case Hardness

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

$\Pr_{x \in \{0,1\}^n}[C(x) = f(x)] < \frac{1}{2} + \frac{1}{S}$ for all size S ckts.

---

distinguisher $\Rightarrow$ Next bit predictor

$$\Pr_{\text{accpts}}[A(G(U_\ell))] - \Pr_{\text{accepts}}[A(U_n)] \geq \varepsilon$$

$$\Rightarrow \Pr[B(y_1, \ldots, y_{i-1}) = y_i] \geqslant \frac{1}{2} + \frac{\varepsilon}{n}$$

$\exists\, B$ predictor algo

$\overline{y} = C_{G_1(U_\ell)}, \ldots, C_{G_n(U_\ell)}$

Yao XOR lemma : Hybrid plus averaging.

Contrapositive:

No predictor $\Rightarrow$ No distinguisher distribution is pseudorandom

next bit

Thm:

$$\Pr_{\substack{i \in [n] \\ r \in R}}[C(r_1, \ldots, r_{i-1}) = r_i] \leq \frac{1}{2} + \frac{\varepsilon}{n}$$

$\Rightarrow$ size $2S$ ckts C on $[n]$

$\Rightarrow$ Y is (S,ε) pseudorandom

Warm up: For $G(z) = z \circ f(z)$ and $\text{Hard}_S(f) \geq n^4$, we have $(\ell+1)$-PRG.

Apply thm at $i = \ell+1$

If we can predict next bit here

$$\Pr_{s,\, r = G(U_\ell)}[C(r_1, \ldots, r_\ell) = r_{\ell+1}] > \frac{1}{2} + \frac{1}{2S(\ell+1)}$$

↓ ckt of size $2(\ell+1)^3$

⇓

$$\Pr_{z \in \{0,1\}^\ell}[C(z) = f(z)] > \frac{1}{2} + \frac{1}{2S(\ell+1)} > \frac{1}{2} + \frac{1}{S^4}$$

Thus f is not avg-case hard.

Thm:

On Worst-case hardness to Avg-case hardness.

Imagine Truth tables as codewords

Good codes [locally-List decodable codes]