CMSC 39600 - Lec #4 (Oct 4)

Today

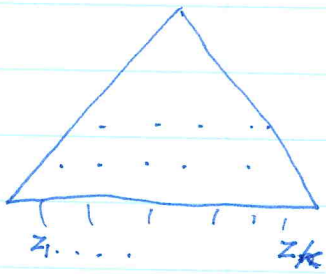
- $NP \subseteq PCP(poly, O(1))$
- PCPs of proximity

Local-Testing ($f(x)+f(y)=f(x+y)$)

- Comp: f is linear $\Rightarrow$ $Pr[\text{Test acc}] = 1$
- Sound: f is δ-far from linear $\Rightarrow$ $Pr[\text{Test acc}] \leq 1-\delta$

Local-Decoding: (z, f; $LD^f(z) = f(x+z) - f(x)$)

- Comp: f is linear $\Rightarrow$ $Pr[LD^f(z) = f(z)] = 1$
- Sound: f is δ-close to linear g $\Rightarrow$ $Pr[LD^f(z) = g(z)] \geq 1-2\delta$.



CIRCUIT-SAT $\in PCP(poly, O(1))$

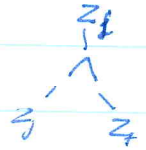
Given C, does there exist ω s.t. $C(\omega) = 1$.

$z_1 \ldots z_k \ldots z_m$ (z_m = output gate) (n-gates)

$\forall$ gates $g(z_{i(g)}, z_{i'(g)}) = z_o$

i

- g is AND $\Rightarrow$ $P_i(z) = z_i - z_j z_k$
- NOT $\Rightarrow$ $P_i(z) = z_i - (1 - z_j)$
- INPUT $\Rightarrow$ $P_i(z) = 0$
- OUTPUT $\Rightarrow$ $P_i(z) = 0$



$\forall$ gates i, $P_i(z) = 0$.

$Quad_x : \{0,1\}^{n^2} \to \{0,1\}$

$$c = \{c_{ij}\}_{i,j=1}^{n} \mapsto \sum_{i,j=1}^{n} c_{ij}\, x_i x_j$$

$$= x^T C x$$

Obs: 1. Can compute any quad fn of x using $quad_x$ (even if x is unknown)

$$p(x) = \sum_{i \neq j} p_{ij}\, x_i x_j + \sum_i p_i x_i + p_{00}$$

$$= quad_x(c) + HW_x(a) + p_{00}$$

$c = \{p_{ij}\}_{i \neq j}$

$a = \{p_i\}$.

---

2. $quad_x$ is linear

Quad Consistency: $f : \{0,1\}^n \to \{0,1\}$, $f' : \{0,1\}^{n^2} \to \{0,1\}$.

1. $y, z \in_R \{0,1\}^n$
2. $f(z) \cdot f(y) = f'(z \otimes y)$ $\quad x \otimes y =$

Based on Freivald's matrix mult. test

Comp: f, f' are such that $f = HW_x$ & $f' = quad_x$
then test acc w/p 1

Sound: f, f' - linear, & $P_R[\text{Quad-consis}(f, f')] \geq 3/4$
then $\exists x$ s.t $f = HW_x$, $f' = quad_x$

Pf:

f is linear $\Rightarrow$ $f = HW_x$ for some x.

f' is linear $\Rightarrow$ $f'(z) = \sum b_{ij} z_{ij}$ for some $\{b_{ij}\}$

Compare B vs $C = xx^T$

If $B \neq C$

then for random z w/p $1/2$.

$Bz \neq Cz$.

then for random y w/p $1/2$

$y^T Bz \neq y^T Cz$.

ie; $f'(y \otimes z) \neq f(y) \cdot f(z)$.

If $B \neq C$, $\Pr[f'(y \otimes z) \neq f(y) \cdot f(z)] \geq 1/4$.

Quad-Corr-Test

$f: \{0,1\}^n \to \{0,1\}$, $f': \{0,1\}^{n^2} \to \{0,1\}$.

1. $y, z \in_R \{0,1\}^n$, $M \in_R \{0,1\}^{n^2}$
2. $f(y) \cdot f(z) = f'(M + yz^T) - f'(M)$

Comp: f, f' s.t. $f = HW_x$ & $f' = quad_x$, then

$\Pr[Q\text{-}C\text{-}T \text{ accepts}] = 1$

Sound: f is ϵ-close to some linear fn g

f' is ϵ-close to some linear fn g'

$\Pr[Q\text{-}C\text{-}T(f,f') \text{ accepts}] \geq \frac{3}{4} + 4\epsilon$

then $\exists\ x$, s.t. $g = HW_x$

$g' = quad_x$

PCP- Verifier for CIRCUIT-SAT

Proof Oracles:

$f: \{0,1\}^n \longrightarrow \{0,1\}$
$f': \{0,1\}^{n^2} \longrightarrow \{0,1\}$

($f = HW_x$ if x is a satisfying assig
$f' = quad_x$)

1. Linearity of f:

$x_1, x_2 \in_R \{0,1\}^n$

$f(x_1) + f(x_2) = f(x_1 + x_2)$

2. Linearity of f'

$M_1, M_2 \in_R \{0,1\}^{n \times n}$

$f'(M_1) + f'(M_2) = f'(M_1 + M_2)$

3. Quad-Consistency of f & f'

$x_1, x_2 \in_R \{0,1\}^n, \quad M \in_R \{0,1\}^{n \times n}$

$f(x_1) f(x_2) = f'(M + x_1 x_2^T) - f'(M)$

4. Circuit Test

Pick $\alpha_1 \ldots \alpha_n \in \{0,1\}$

$P(z) = \sum \alpha_i P_i(z)$

$= c_0 + \sum l_i z_i + \sum_{i,j} Q_{ij} z_i z_j$

Pick $y \in_R \{0,1\}^n, \quad M \in_R \{0,1\}^{n \times n}$

$c_0 + (f(y+l) - f(y)) + (f'(M+Q) - f'(M)) = 0$

---

queries = 4 = O(1)

random coins = $2n + 2n^2 + 2n + n^2 + n + n + n^2$

$= 4(n^2 + n)$

~~Claim: $\exists \varepsilon, s.t.$ $Pr[\text{Verifier}] \geq \varepsilon$, then~~

~~Proof:~~

Claim: $\exists\ \delta_0$, $\forall\ \delta \leq \delta_0$

$Pr[\text{Verifier accepts}] \geq 1-\delta$

$\Downarrow$

f is ~~2~~δ-close to HW_x for some $x = w_0 y$

s.t $C(w) = 1$

Proof: Set $\delta_0 = 1/20$.

By contradiction

If not

- f is δ-far from being linear.

  → Linearity test rejects w/p $\geq \delta$.

- f' is δ-far from being linear

  → Linearity of f' rejects w/p $\geq \delta$

- f is δ-close to g ~~=~~ f' is δ-close to g

  But $\nexists x$, $g = HW_x$, $g' = quad_x$

  → Quad-Corr-Test rejects w/p $\geq \frac{1}{4} - 3\delta \geq \delta$

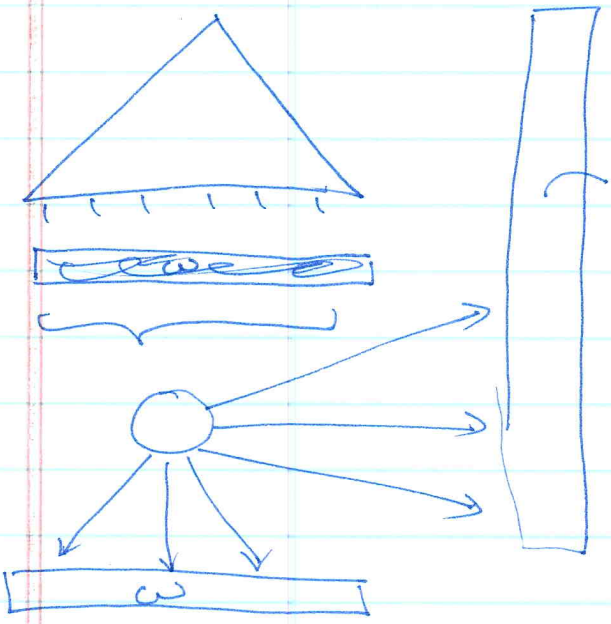
- f is δ-close to HW_x ~~=~~ f' is δ-close to $quad_x$

  $(x = w_0 y)$ But $C(w) \neq 1$

  → Circuit Test rejects w/p $\geq \frac{1}{2} - 4\delta$

  $\geq \delta$.

Actually stronger:



Can check that proof corresponds to a specific ω. (without reading all of ω).

Proximity Test

$j \in_R \{1 \ldots k\}$

$z \in_R \{0,1\}^n$

$\omega_j = f(z + e_j) - f(z)$

~~(f, f')~~ is ~~not~~

Suppose test passes w/p $\geq 1-\delta$

then we can assume

$\exists$ ~~x~~ = ω_{0y} s.t $C(\omega) = 1 \geq$

f is δ-close to HW_x

f' is δ-close to $quad_x$.

~~Now, $\Delta(\omega, \omega') \geq \delta$~~

~~$Pr[$proximity test rej rejects$] \leq 2\delta + \delta$~~

$Pr[\omega_j = f(z+e_j) - f(z)] \geq 1-\delta$ ~~accepts~~

$Pr[\omega_j = WH_x(z+e_j) - WH_x(z)] \geq 1-3\delta.$

$\Rightarrow$ ω is 3δ-close to ω'!