CMSC 39600 - Lec #13 (Nov 8)

Today
- Original proof of PCP Theorem
- Low degree Testing
  - Raz-Safra

Low degree testing

Fix:

$\mathbb{F}$ - field ($|\mathbb{F}| = q$)

m - dim of space

d - degree (total degree)

$A: \mathbb{F}^m \to \mathbb{F}$

Suppose A is low degree (i.e., d), then how does one check w/o looking at all of A.

(allow errors)

Idea: For any line ℓ (in general affine space S)

$A|_\ell$ (or $A|_S$) is of deg $\le d$ if A is of deg

Lines-~~Point~~ Test

1. Choose a random $\ell \in$ in $\mathbb{F}^m$
2. Query A along ℓ
3. Accept iff A_ℓ is $\leq$ deg d.

Rubinfeld-Sudan.

Convenient to have extra oracle.

Lines oracle

$\forall \ell$, $A(\ell)$ is a univariate deg d poly.

Lines-Point Test

1. Choose a random ℓ in $\mathbb{F}^m$
2. Choose $x \in_R \ell$
3. Query $p \leftarrow A(\ell)$, $v \leftarrow A(x)$
4. Accept iff $p(x) = v$.

Completeness: A is deg d $\Rightarrow$ ~~$\Pr[acc]$~~
$\Rightarrow \exists$ lines $\Pr[acc] = 1$

Soundness A is δ-far from being deg d
$\forall$ lines $\Pr[acc] \leq 1 - 2\delta$

(Contrapositive)

Analysis: Rubinfeld Sudan, AS, ALMSS

axis-// test: BFL, PS.

Raz-

Planes- Point Test

Thm [Raz-Safra]

$\exists \ \epsilon = \epsilon\left(\frac{d}{q}\right)$

Suppose $\exists$ planes oracle P s.t

$$\Pr\left[\text{planes-point}^{A,P}() = \text{acc}\right] \geq \gamma$$

then $\exists$ poly Q of deg $\leq d$

$$\text{agr}(A, Q) \geq \gamma - \epsilon \, m \, \epsilon$$

No reason to stick to planes, can use any affine subspace of dim k $(k \leq m)$

Infact, proof by induction

For $k = 3, 4 \ldots m$

Suppose $\exists$ k-space oracle A_k s.t

$$\Pr_{b,x}\left[A_k(b)(x) = A(x)\right] \geq \gamma$$

$\Downarrow$

$\exists$ $(k+1)$-space oracle A_{k+1} s.t

$$\Pr_{b,x}\left[A_{k+1}(b)(x) = A(x)\right] \geq \gamma - \epsilon$$

Space vs Point to Space vs. Space.

Ex

$$\Pr_{S,x}\left[\mathcal{A}(S)(x) = \mathcal{A}(x)\right] \geq \nu$$

$$\Downarrow$$

$$\Pr_{S_1,S_2,\, a \in S_1 \cap S_2}\left[\mathcal{A}(S_1) = \mathcal{A}(S_2)\right] \geq \nu^2 - \frac{1}{q}$$

Lemma: For any $\mathcal{A}_k$

$\exists\ t \leq 4/\delta$, $Q_1 \ldots Q_t$ poly

$$\Pr_{(S_1,S_2)}\left[(S_1,S_2) \notin E_A \ \vee \ \exists i\ (Q_i = \mathcal{A})(S_1) \wedge (Q_i = \mathcal{A})(S_2)\right] > 1-\delta.$$

Consistency Graph

$V = S_{k-1}^k$ ($k-1$ spaces in F^k)

$E = \{(S_1,S_2) \mid \cancel{\mathcal{A}_{k-1}(S_1) = \mathcal{A}_{k-1}(S_2)}$
$\forall x \in S_1 \cap S_2 : \mathcal{A}_{k-1}(S_1)(x) = \mathcal{A}_{k-1}(S_2)(x)\}$

Consistency - graph is almost transitive

Lemma: If $(\delta_1, \delta_2) \notin E_{A_2}$, then

$$\Pr_{\delta_3}[(\delta_1, \delta_3) \in E \wedge (\delta_2, \delta_3) \in E_A] \leq \frac{d+1}{q}.$$

Pf:

$(\delta_1, \delta_2) \notin E$

$\Rightarrow \exists\, x \in \delta_1 \cap \delta_2$, s.t $A(\delta_1)$ & $A(\delta_2)$ do not agree on x.

Let $a = \delta_1 \cap \delta_2$.

$A(\delta_1)|_a \neq A(\delta_2)|_a$

Random δ_3.

- δ_3 - unlucky (ie, $\delta_3 \cap a \neq \emptyset$)

  $\Pr[\delta_3\text{-unlucky}] \leq \frac{1}{q}$

- δ_3 - does not spot inconsistency

  (ie, $\forall x \in \delta_3 \cap a$, $A_1(\delta_1)(x) = A_2(\delta_2)(x)$

  $\Pr[\delta_3\text{-does not spot} \mid \delta_3\text{-unlucky}] \leq \frac{d}{q}$.

~~$\leq \mathop{E}_{a' \in T} \Pr[$~~