CMSC 39600 - Lec #16 (Nov 15)

Today

Robustifying

Augment with PCPP

First we'll robustify the LDT.

robust-LDT $(A: \mathbb{F}^m \to \mathbb{F})$

1. Choose random plane ρ

and accept if $A|_\rho$ is a deg d poly.

Claim: $\delta(A, P_{m,d}) \geq \delta \Rightarrow$ ~~Exp$_\rho$ $\{A|_\rho\}$ has~~ e

Expected fractional distance of A from satisfying the rob-LDT $\geq \delta - \epsilon_0$

$\mathbb{E}_\rho[\delta(A|_\rho, P_{2,d})] \geq \delta - \epsilon_0$.

Pf: Create planes oracle $A: S_2^m \to P_{2,d}$

$$A(\rho) = \arg\max_{p \in P_{2,d}} (\delta(A|_\rho, p))$$

Thus, $\delta(A|_\rho, P_{2,d}) = \delta(A|_\rho, A(\rho))$

On the other hand,

$\delta - \epsilon_0 \leq \Pr[\text{rej}] = \Pr[A(\rho)(x) \neq A(x)] = \mathbb{E}_\rho[\delta(A|_\rho, A(\rho))]$

Similarly bundled robust LDT

<u>Prob-PCP Verifier</u> Input: circuit C

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

$P : \mathbb{F}^{3m+3} \to \mathbb{F}^{3m+3}$

1. $\rho' \in_R S_2^m$. Check if $A|_{\rho'} \in P_{2,d}$

2. $\rho \in_R S_2^{3m+3}$, Check if $\forall i \; P_i^6|_\rho \in P_{2,d}$

3. $\forall \; z = (u, v, \omega, a, b, c) \in \rho$
 check if
 $\hat{C}(u, v, \omega, a, b, c)(A(u) - a) \ldots = \sum z_H(z_i) P_i(z)$

As before.

Randomness = $O(\log n)$

Query Complexity = $\text{poly}\log n$.

<u>Soundness Analysis</u>

<u>Claim</u> For ϵ

if A is ϵ-far from any deg mh poly $a : \mathbb{F}^m \to \mathbb{F}$ s.t $a|_{H^m}$ is a sat assign, then expected fraction of input read that needs to be modified $= \Omega(\epsilon - \epsilon_0)$.

ie. w prob $\Omega(\epsilon - \epsilon_0)$ atleast $\Omega(\epsilon - \epsilon_0)$ portion of i/p read needs to be modified.

Augmenting with a PCP of proximity

Case (i) $\delta(A, P_{m,d}) > \epsilon$

In exp, $\epsilon - \epsilon_0$ of the i/p read by Step 1 needs to be changed

ie, In exp, $\frac{\epsilon - \epsilon_0}{5}$ of total i/p

Case (ii) $\delta(P, P^{\odot(3m+3)}_{3m+3,d}) > \epsilon$

Same as above

Case (iii) $\exists\ a \in P_{m,d}$ $\delta(A, a) \leq \epsilon$

$\triangleright$ $P_1, \dots P_m \in P_{m,d}$, $\delta(P, P_1 \odot P_2 \odot \dots \odot P_{3m+3}) \leq \epsilon$.

B - bad set where identity does not hold

$$\frac{|B|}{|\mathbb{F}|^m} > 1 - \frac{d}{9} - 4\epsilon$$

All of $|B \cap \rho|$ needs to be changed

One need $\mathbb{E}[|B \cap \rho|] > (1 - \frac{d}{9} - 4\epsilon) 9^m$

Either $A|_\rho$ or $P|_\rho$ on all of $B \cap \rho$ needs to be changed

$$\left(1 - \frac{d}{9} - 4\epsilon\right)\frac{1}{5} > \frac{\epsilon - \epsilon_0}{5} \quad \text{if} \quad \underbrace{5\epsilon + \frac{d}{9} < 1 + \epsilon_0}.$$

Thus, in expectation $\frac{\epsilon - \epsilon_0}{5}$ fraction of i/p reads needs to be changed

Hence, w/p $\geq \frac{\epsilon - \epsilon_0}{10}$ at least $\frac{\epsilon - \epsilon_0}{10}$ fraction of input needs to be changed.

Augmenting with a PCP of proximity

$a: \mathbb{F}^m \to \mathbb{F}$ contains the assignment to i/p gates

Need to crossverify against $W: [k] \to \{0,1\}$

Rob-PCPP Verifier

1. Run Rob-PCP Verifier
2. Proximity Test
   Choose $i \in_R [k]$. $x \in H^m$ that corresponds w/ i
   Choose a random plane ρ thr i
   & accept if $A|_\rho$ is a low-deg poly
   & $A(x) = W[i]$

Soundness Analysis

Case (i) A is not $2\epsilon_0$-close to any $a \in P_{m,d}$ st $C(a|_{H_m}) = 1$

Then w/prob $\frac{\epsilon_0}{10}$ ~~α~~ $= \Omega(1)$, atleast [Pr[Rob-PCP verif]]

$\frac{\epsilon_0}{10} = \Omega(1)$ of proof oracle read needs to be modified.

Case(ii) A is $2\epsilon_0$-close to a s.t. $C(a/_{H_m}) = 1$

then W is δ-far from $a/_{H_m}$

Hence w/prob