Today

- PCP Composition
- Proof of the PCP Theorem.

CS5.330.1 : PCPs
Limits of Approximation Algorithms

Lecture 06 (2023-3-3)

Instructor: Prahladh Harsha

Recap PCP construction via LDT from last lecture.

Parameters of PCP constructed:

$|S^m| \cong n$; $\mathbb{F}$; $d = O(m|S|)$

Randomness $= O(m \log |\mathbb{F}|) = O(\log n)$

Proof length $= O(m |\mathbb{F}|^{2m}) = \text{poly}(n)$

Query Complexity $= O(m|\mathbb{F}|) = \text{polylog}\, n$

Alphabet size $= |\mathbb{F}|$ (ie $\log |\mathbb{F}|$ in bit complexity). $\log\log n$.

Decision Complexity $= \text{poly}(m |\mathbb{F}|)$ $\text{polylog}\, n$.
Contrast $\tilde{O}(m|\mathbb{F}|)$.

Soundness Error $= \frac{9}{10} + O\left(\frac{m|S|}{|\mathbb{F}|}\right)$ — constant.

Parameter Setting: $|S| = O(\log n)$
$m = O(\log n / \log\log n)$

$$S^m = \text{poly}(n) \iff m \log S = O(\log n)$$

$$\frac{m|S|}{|\mathbb{F}|} = \text{small constant} \quad ; \quad |\mathbb{F}| = O(\log^2 n).$$

Thus,

$$NP \subseteq PCP_{1, 9/10}[O(\log n), \text{poly} \log n].$$

[ALMSS]

Above PCP has all desired parameters except for query complexity.

(Furthermore, the PCP can be constructed in poly time given the NP certificate)

But we previously constructed a Hadamard-based PCP

$$SAT \in PCP_{1, 9/10}[O(n^2), 14]$$

Summarizing:

Robust PCP + PCP of proximity = PCP

Composition Theorem:

Assume the following two hold

(a) L has a robust PCP verifier V_{out}

w/ randomness complexity $r_{out}(n)$

query complexity $q_{out}(n)$

decision complexity $d_{out}(n)$

robust soundness error $1-\varepsilon_{out}(n)$

robustness parameter $\rho_{out}(n)$

(b) CKT-VAL (two inputs : explicit i/p C
implicit i/p : x)

has a PCP of proximity verifier V_{in}

w/ randomness complexity $r_{in}(n)$

query complexity $q_{in}(n)$

decision complexity $d_{in}(n)$

proximity parameter $\delta_{in}(n)$

soundness error $1-\varepsilon_{in}(n)$

& (c) $\delta_{in}(d_{out}(n)) < \rho_{out}(n)$

then L has composed PCP V_{comp}

randomness complexity $r_{out}(n) + r_{in}(d_{out}(n))$

query complexity $q_{in}(d_{out}(n))$

soundness error $1 - \varepsilon_{out}(n) \cdot \varepsilon_{in}(d_{out}(n))$

Furthermore

(a) If V_{out} is a PCP of proximity w/ parameter $\delta_{out}(n)$, so is V_{comp} (w/ the same proximity parameter)

(b) If V_{in} has robust soundness w/ robustness parameter $\rho_{in}(n)$, then so does V_{comp} w/ robustness parameter $\rho_{in}(\ell_{out}(n))$.

Part II: Proof of the PCP Theorem

Inner verifier — PCP of Proximity Verifier.

Recall the Hadamard-based PCP construction

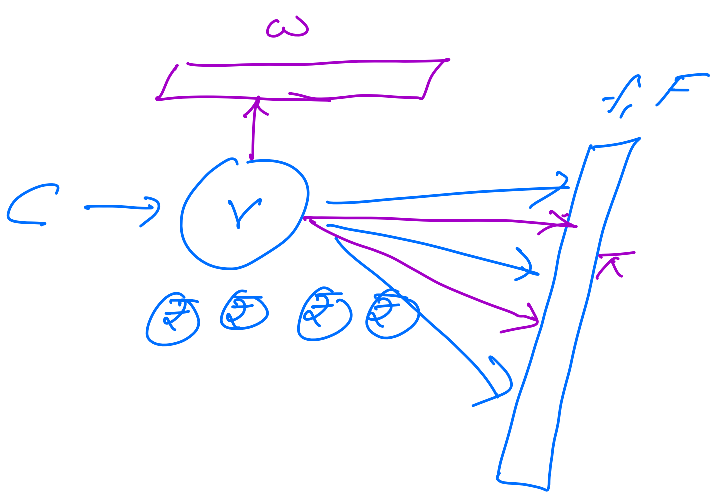
Soundness: $\exists\, \delta_0 \in (0,1)$, $\forall\, \delta \leq \delta_0$

$$\Pr[\mathrm{Ver}^{f,F} \text{ acc}] \geq 1-\delta$$

$$\Downarrow$$

$\exists\, C(z)=1$, s.t. f is δ-close to ℓ_z & F is δ-close to quad_z.

PCP of Proximity for Circuit-Value



If $\Pr[\text{Ver acc}] \geq 1-\delta$
$\Downarrow$
f - δ-close to ℓ_z
(Hadamard encoding of z)
& Z is a satisfying assignment
(i.e., $C(z)=1$)

PCPP Verifier$^{\omega, \pi}(C)$

① Run the Hadamard-based PCP verifier for C.

② Proximity Test
(a) Pick an $i \in [|\omega|]$
(b) Pick $x \in_R \{0,1\}^n$
(c) Accept if $f(x+e_i) - f(x) = \omega_i$.

Soundness: If $\delta(\omega, z) \geq 3\delta$

$\Pr[\text{Proximity Verifier rejects}] \geq \delta.$

Conclusion: $CVal \in PCPP_{1, 9/10}[O(n^2), 20, \frac{1}{100}]$
I.
proximity parameter

Low degree test based PCP:

$$SAT \in PCP_{1, 9/10}[O(\log n), \text{poly}\log n]$$

Qn: (1) Is this PCP robust?

(2) Is it robust even over the binary alphabet?

Recall PCP construction from last lecture

Verifier: (1) Pick ℓ in $\mathbb{F}^m$, ℓ' in $\mathbb{F}^{2m}$

(2) Query $C, Q_1, \ldots Q_m$ on ℓ

& reject if any restriction is not low-degree

(3) Query $P_1 \ldots P_{2m}$ on ℓ'

& reject if any restriction is not low-degree

(4) For each $z \in \ell$, reject if

$$C(C(z)-1)(C(z)-2)(C(z)-3)) \neq \sum_{i=1}^{m} Q_i(z) Z_S(z_i)$$

(5) For each $\underset{(x', y')}{z'} \in \ell'$, reject if

$$E(z') \cdot (\quad) \neq \sum_{i=1}^{2m} P_i(z') Z_S(z_i')$$

(;
(;
( )

For starters, is the LDT robust

i.e. $\delta(f, RM_{\mathbb{F}}(m,d)) \geq \delta$

$$\Downarrow ???$$

$$\Pr_{\ell}\left[\delta(f|_{\ell}, RM_{\mathbb{F}}(1,d)) \geq \delta/8\right] \geq \varepsilon_0 \quad . \qquad \ldots (*)$$

In fact, we have:

$$\left.\begin{array}{l} \delta(f, RM_{\mathbb{F}}(m,d)) \geq \delta \\ \Downarrow \\ \mathbb{E}_{\ell}\left[\delta(f|_{\ell}, RM_{\mathbb{F}}(1,d))\right] \geq \delta/4 \end{array}\right\} \text{provided } \delta \leq \delta_0 = \mathrm{poly}\left(\frac{d}{|\mathbb{F}|}\right)$$

Apply averaging argument to above to get (*)

Robustify the Joint LDT

$Q_1 \ldots Q_m : \mathbb{F}^m \to \mathbb{F}$

Run a LDT on all of them.

Bundle the Q's into one table

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

Standard LDT Soundness Claim

$$\mathbb{E}_{\ell}\left[\delta(f|_\ell, RM_{\mathbb{F}}(1,d))\right] \geq \delta \Rightarrow \delta(f, RM_{\mathbb{F}}(m,d)) \geq 4\delta.$$

What if f - vector of r functions.

$$f^{(r)} : \mathbb{F}^m \to \mathbb{F}^r$$

$$\mathbb{E}_{\ell}\left[\delta(f^{(r)}|_\ell, RM^{r}_{\mathbb{F}}(1,d))\right] \geq \delta.$$

$$\Downarrow$$

$$\delta(f^{(r)}, RM^{(r)}_{\mathbb{F}}(m,d)) \geq 4\delta.$$

Proof works even in this case.

Bundled Proof:

$C : \mathbb{F}^m \to \mathbb{F}^{m+1}$

$P : \mathbb{F}^{2m} \to \mathbb{F}^{2m}$

Verifier: (1) Pick ℓ in $\mathbb{F}^m$, ℓ' in $\mathbb{F}^{2m}$

(2) Query C along ℓ

P along ℓ'

(3) Check $C|_\ell \in RM^{(m+1)}_{\mathbb{F}}(1,d)$

$$P|_{\ell'} \in RM_{\mathbb{F}}^{(2m+1)}(1, d')$$

④ For each $z \in \ell$

$$(C_0(z)-1)(C_0(z)-2)(C_0(z)) = \sum_{j=1}^{m} C_j(z) \cdot Z_j(z_j)$$

⑤ For each $z' \in \ell'$

$$=$$

Conclusion: For every $\rho < 1/4$, $\exists\ \varepsilon_\rho$

II $\quad$ 3COL $\in$ robust$_{1, 1-\varepsilon_\rho}$ $[O(\log n), \text{poly}\log n, \rho]$ ↳ robust res.

Composing Robust PCP from II w/ PCPP from I

$$3COL \in PCP_{1, 0.999}[\underbrace{\text{poly}\log n}, O(1)]$$

exp in poly ≥ 2.

(ie, outer reduction in query complexity is not small enough for composition w/ inner PCPP)

— Need an additional round of composition.

Will construct a LDT-based Robust PCPP.

Add a proximity test to the LDT-based robust PCP (using locally decodability of RM code)

This yield a Robust PCPP for 3CGL-VALUE

An almost identical construction gives a similar robust PCPP for CVal.

ie,

$\underline{\overline{III}}$ $\quad CVAL \in \text{Robust-PCPP}_{1,\, 99/100}\left[O(\log n), \text{polylog}\, n, \tfrac{1}{10}, \tfrac{1}{5}\right]$

$\tfrac{1}{10}$ → proximity

$\tfrac{1}{5}$ → robustness parameter

$$\underset{\underline{II}}{\text{Robust PCP}} + \underset{\underline{\overline{III}}}{\text{Robust PCPP}} + \underset{I}{\text{PCPP}}$$

= PCP for 3COL w/ the following parameter

Randomness Complexity = $O(\log n)$

$$+ O(\log \cdot \operatorname{poly}\log n)$$

$$+ O\left((\operatorname{poly}\log\log n)^2\right)$$

$$= O(\log n)$$

Query $= O(1)$

$\boxtimes$