CMSC 39600 - Lec #5 (Oct 9)

Today.
- PCPs of proximity
- Proof Composition
- Dinur's Proof

Last Lecture.

Thm: There exists a prob verifier V s.t. on
- explicit input a circuit C
- implicit input an assignment ω
- oracle access to a proof π
- tosses at most $O(n^2)$ coins & makes $O(1)$ queries into (ω, π)

Comp: $C(\omega)=1 \Rightarrow \exists \pi, \Pr[V^{\omega,\pi}(C)=1]=1$

Soundness: $\exists \pi, \Pr[V^{\omega,\pi}(C)=1] \geq 1-\delta \Rightarrow \exists \omega', \delta(\omega,\omega') \leq 3\delta$ & $C(\omega')=1$

or

If $\delta(\omega, SAT(C)) > 3\delta, \Rightarrow \forall \pi, \Pr[V^{\omega,\pi}(C)=1] < 1-\delta$

PCP of proximity

Pair Language L (x,y) - input two parts
- x - explicit part
- y - implicit part.

x, $L_x = \{y \mid (x,y) \in L\}$

eg:- CIRCUIT-VAL = $\{(C, \omega) \mid C(\omega) = 1\}$
(NP-Instance, NP-witness)

Def: PCP of proximity for a pair lang L.
- randomness r
- query comp q
- proximity parameter - δ

Comp: $(x, y) \in L \Rightarrow \exists \pi$,
$$Pr[V^{y,\pi}(x) = 1] = 1$$

Sound: y is δ-far from L_x
$$\Rightarrow \forall \pi, \quad Pr[V^{y,\pi}(x) = 1] < \delta(x)$$

Notation: $L \in PCPP_{1,\delta}[r, q, \delta]$

Thm: $\exists\ \delta_0$,
$$\text{CIRCUIT-VAL} \in PCPP_{1,1-\delta_0}[O(n^2), 17, 38_0]$$

Remark: All parameters measured in terms of explicit i/p.
- Weakening of PCP - only reject those (x, y) where y is δ-far from L_x
- Strongent - only have oracle access to y.

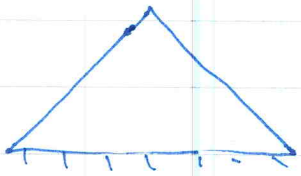
Proof Composition

Want to construct PCPs for NP

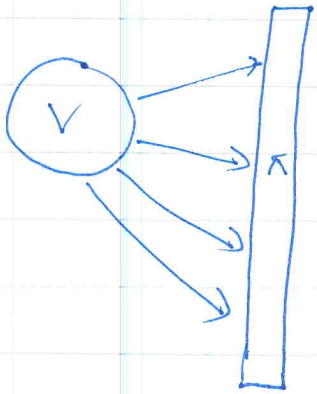
w/ $r = O(\log n)$

$q = O(1)$.

Unfortunately, we can know to construct PCPs w/ large query complexity (when $r = O(\log n)$



Closer look at Verifier's task.



$V(x, R) \longrightarrow (I, D)$

set of indices — Decision ckt.

Need to check

$D(\pi|_I) = 1$?

However, $\pi|_I$ is too long?

Idea: Use PCP to check $D(\pi|_I) = 1$

Proof Composition [Arora + Safra]

However But,

PCP needs to read all its input!!

Use PCP of proximity

Problem: PCPPs distinguish $\begin{cases} D(\pi/_I) = 1 \\ \pi/_I \text{ is } \delta \text{ far from } SAT(D) \end{cases}$

However, need to distinguish between $\begin{cases} D(\pi/_I) = 1 \\ D(\pi/_I) \neq 1 \end{cases}$

Make soundness condition more stringent

(Regular) ~~Robust~~ Soundness:

$$\forall \pi, \quad Pr[D(\pi/_I) = 1] < \delta(|x|)$$

Robust Soundness

$$\forall \pi, \quad Pr[\pi/_I \text{ is } \beta\text{-close from } SAT(D)] < \delta(|x|)$$

PCPP $\rightarrow L \in$ prob-$PCPP_{l,\delta}[n, q, \delta, \rho]$

If PCP $\rightarrow L \in$ prob-$PCP_{l,\delta}[n, q, \rho]$

Composition:

If $\delta_{in} \leq \rho_{out}$:

$L \in \text{rob-PCPP}_{1,1-\varepsilon_{out}}[\kappa_{out}, q_{out}, \delta_{out}, \rho_{out}]$

CIRCUIT-VALUE $\in \text{rob-PCPP}_{1,1-\varepsilon_{in}}[\kappa_{in}, q_{in}, \delta_{in}, \rho_{in}]$

$\Rightarrow L \in \underbrace{\text{rob-PCPP}_{1,1-\varepsilon_{out}\cdot\varepsilon_{in}}[\kappa_{out}+\kappa_{in}, q_{in}, \delta_{out}, \rho_{in}]}_{\text{composed}}$

Pf. Soundness

W/p ε_{out} over R_{OUT}

$\pi_{out}|_{I_{out}}$ is ρ_{OUT}-far from $SAT(D_{out})$

$\Downarrow$

w/p ε_{in} over R_{IN}

$\pi_{IN}|_{I_{IN}}$ is ρ_{IN}-far from from $SAT(D_{IN})$

$\Rightarrow y$ - δ-far from L_x

$\Downarrow$

$\Pr_{R_{OUT}, R_{IN}}[(\pi_{comp}, y)|_{I_{COMP}}$ is ρ_{IN}-far from $SAT(D_{IN})] \geq \varepsilon_{out}\varepsilon_{IN}$

Thus, $L \in \text{rob-PCPP}_{1,1-\varepsilon_0\varepsilon_1}[\kappa_0+\kappa_1, q_1, \delta_0, \rho_{\text{fix}}]$

Outer	Inner	Composed
$\mathcal{R}$-PCPP	$\mathcal{R}$-PCPP	$\mathcal{R}$-PCPP
$\mathcal{R}$-PCP	$\mathcal{R}$-PCPP	$\mathcal{R}$-PCP
$\mathcal{R}$-PCPP	PCPP	~~$\mathcal{R}$~~ PCPP
$\mathcal{R}$-PCP	PCPP	PCP.

Thm $L \in \mathcal{R}\text{-}PCP_{1,1-\delta}[r, q, \rho] \Rightarrow L \in PCP_{1,1-\delta\delta_0}[r + O(q^2), O(1)]$ if $\rho > \delta_0$ //.

Non-Boolean $L \in PCP^{\Sigma}_{1,1-\delta}[r, q]$ $\quad [\Sigma] = [a]$

↓ Robustness

$$\Downarrow$$

$$L \in \mathcal{R}\text{-}PCP_{1,1-\delta}[r, O(aq), O(\tfrac{1}{a})]$$

Parallelization $L \in PCP_{1,1-\varepsilon}[r, q, \rho]$

$$\Downarrow$$

$$L \in PCP^{\Sigma}_{1,1-\varepsilon\rho}[r + \log q, 2] \quad (\Sigma = q$$

$L \in PCP_{1,1-\delta}{}^{\Sigma}[r, q]$ $(|\Sigma| = a) \Rightarrow L \in PCP_{1,1-\delta\delta_0}[r + O(a^2 q^2), O(1)]$

$$\Downarrow$$

$$L \in PCP^{\Sigma}_{1,1-\frac{\delta\delta_0}{O(1)}}[r + O(a^2 q^2) + \log q, 2]$$