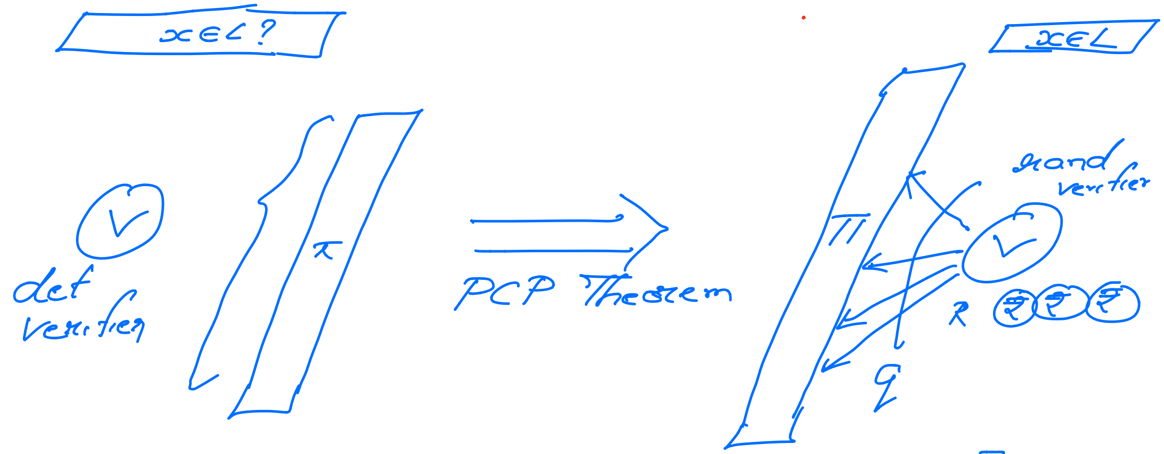
Today

PCPs (lecture 2)

- Inapproximability of Clique
- Exponential sized PCPs

Lecture 26
Computational Complexity (7 May '20)
Instructor: Prahladh Harsha

L



$L \in PCP_{1,\frac{1}{2}}[r, q, m, t, a]$

✓ $\{ r = $ # random coins
$q = $ # queries

Drop
$\{ m \le q \cdot 2^r \} \leftarrow m = $ proof length
$t \le poly \leftarrow t = $ running time of verifier
$a = poly(q) \leftarrow a = $ size of predicate
↳ typical

Today: Application to hardness of approximating Max Clique.

Trivial: $1/n$ - approximation.

gap$_\alpha$-CLIQUE : YES = $\{(G,k) \mid \text{Max-Clique}(G) \ge k\}$
$\alpha \in (0,1)$ (G,k) NO = $\{(G,k) \mid \text{Max-Clique}(G) \le \alpha k\}$

Goal: Does $\exists\, \alpha \in (0,1)$, s.t there is a polytime redn from SAT to gap_α-CLIQUE?

Thm [FGLSS]. If $L \in PCP_{c,s}[r,q,t]$, then there exists a deterministic redn running in time $poly(t \cdot 2^{r+q})$ from L to $gap_{s/c}$-CLIQUE.

PCP Theorem: $SAT \in PCP_{1,1/2}[O(\log n), O(1), t=poly]$

Cor: (PCP Thm + Thm): $SAT \leq_p gap_{1/2}$-CLIQUE.

Proof of FGLSS Thm:

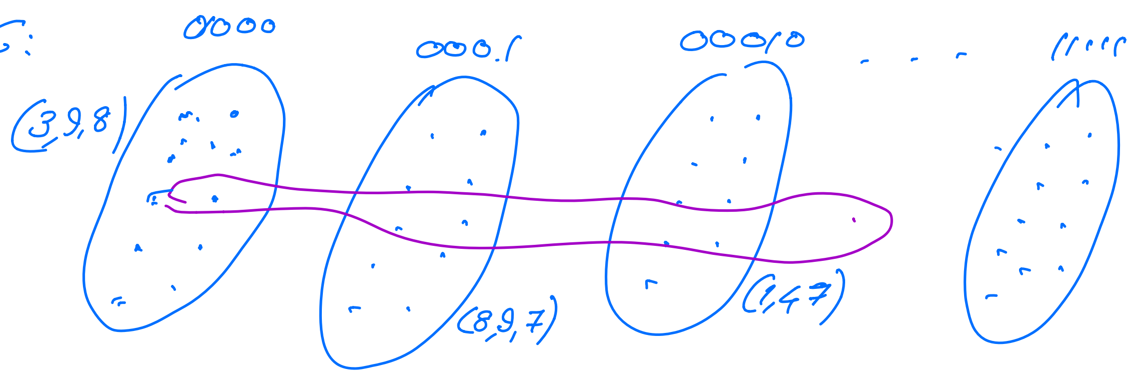
Karp reduction from SAT to Clique:

$L \in PCP_{c,s}[r,q,t]$.

$L \longmapsto gap_{s/c}$-CLIQUE

$x \longmapsto (G,k)$.

G:



$V(G) = 2^r \times 2^q$ = Cloud of each randomness

+ within each cloud, a possible local view of verifier.

2

$E(G) = \{ (R, b_1 .. b_q) \sim (R', b_1', .. b_q') \mid$

Running time of redn poly$(t \cdot 2^{r(n)})$

① $b_1 .. b_q$ & $b_1' .. b_q'$ satisfy the predicate D on rand $r > r'$

② They are consistent $\}$.

G – 2^r-partite graph (There are no edges within a cloud)

$k = c 2^r$; $\alpha = s/c$.

$x \in L \Rightarrow \exists \pi, \Pr_R [V^\pi(x;R) = acc] \geq c$.

$\Rightarrow S \subseteq V(G)$

$S_\pi = \{ (R, \bar{b}) \mid R \in \{0,1\}^r, (Q_R, D) \leftarrow V(x;R)$
$D(\bar{b}) = acc, \ \pi|_Q = \bar{b} \}$.

All vertices in S_π are consistent w/ each other.

Hence, S_π is a clique.

$|S_\pi| \geq c \cdot 2^r$

$(G, c2^r) \in YES(gap_{s/c}\text{-CLIQUE})$

$x \notin L \Rightarrow (G, c2^r) \in NO(gap_{s/c}\text{-CLIQUE})$ $\rightarrow$ need to show

In other words, need to show

$MAXCLIQUE(G) \leq \frac{s}{c} \cdot c 2^r$
$= s \cdot 2^r$

Suppose this is false, ie, $MAXCLIQUE(G) > s \cdot 2^r$

ie, $J > s \cdot 2^r$. random coins + corresponding accepting local views that are completely pairwise consistent

π - proof constructed by extending these local views.

$$\Pr[V^{\pi}(x;R) = acc] > s$$

$\Rightarrow \Leftarrow$ contradiction

$\boxtimes$

Sequential repetition of PCPs:

$$PCP_{1,s}[r,q,t] \subseteq PCP_{1,s^k}[rk, qk, tk]$$

$$SAT \in PCP_{1,1/2}[\log n, 3] \subseteq PCP_{1,1/2^k}[k\log n, 3k]$$

$SAT \leq_p gap_{1/2^k}$-CLIQUE in time $poly(2^{k\log n + 3k})$

Cor: $\forall \alpha \in (0,1)$, gap_{α}-CLIQUE is NP-hard.

Efficient randomness repetition (recycling randomness)

k - different random coins

- pick them from a k-step on a constant degree expander.

- $r + k \cdot \log D$ (D - degree of expander).

$$PCP_{1,s}[r,q,t] \subseteq PCP_{1,s^k}[r+O(k), kq, kt]$$

$SAT \in PCP_{1,1/2}[\log n, 3] \subseteq PCP_{1,1/n}[O(\log n), O(\log n) , poly]$.

Cor: $\exists\, \delta \in (0,1)$; gap_{1/n^δ}-CLIQUE is NP-hard.

Håstad, (recycled queries), Zuckerman

Thm $\forall\, \varepsilon \in (0,1)$, $gap_{1/n^{1-\varepsilon}}$-CLIQUE is NP hard.

(Håstad - randomized redn
Zuckerman - derandomized using extractors).

CLIQUE - amortized query complexity

$\hookrightarrow$ how much does the soundness fall w/ each query.

(In the limit, each additional query halves the soundness)

Next time - bird's eye view of the proof of the PCP Theorem