PCPs

Lecture 23

Probabilistically Checkable Proofs

MA Proof

MA[2]

P/M | **V/A**

$$\xrightarrow[\pi]{m}$$

$r \xleftarrow{\$} \{0,1\}^*$

$V(m, r)$

Def: Let $r, q : \mathbb{N} \to \mathbb{N}$ be arbitrary. Then, $L \in PCP(r, q)$ if $\exists$ a probabilistic poly-time (in $|x|$) verifier V such that

(1) $V^{\pi}(x)$ uses $O(r(|x|))$

random bits and reads $O(q(|x|))$ bits of π.

(2) If $x \in L$, then $\exists \pi$ s.t. $\Pr[V^{\pi}(x)=1] = 1$

(3) If $x \notin L$, $\forall \pi^*$ we have $\Pr[V^{\pi^*}(x)=1] < \frac{1}{2}$

Notes

(1) $IP \subseteq PCP(\underbrace{poly(n)}_{\#\text{ random bits}}, \underbrace{poly(n)}_{\#\text{ queries to } \pi})$

$\quad \| $

PSPACE

(2) We can show that $\forall\ |x| = n$,

$|\pi| \leq 2^{r(n)} \cdot q(n)$

$\rightarrow |\pi| = O(2^{|x|})$

(3) V^{π} can adaptively query π; we're only going to look @ non-adaptive verifiers.

- can show that q-query adaptive verifier has a $O(2^{q})$-query non-adaptive verifier.

How Powerful are PCPs?

- Not hard to see that

$$NP = PCP(0, poly(n))$$

Thm (The PCP Theorem):

$$NP = PCP(\log(n), 1)$$

$$\|$$

Lemma: $PCP(\log(n), poly(n)) = NP$

Proof:

- $NP \subseteq PCP(\log(n), poly(n))$

- $PCP(\log(n), \text{poly}(n)) \subseteq NP$

Let $L \in PCP$. Need to give $\forall x \in L$ an NP witness w.

* can't just give some proof Π_x for PCP verifier, $|\Pi_x| \leq 2^{|x|}$

Observe:

- $r(n) = O(\log(n))$

  $\Rightarrow$ # random strings is $\text{poly}(n)$ for PCP V^{Π}

- $q(n) = \text{poly}(n)$

NP-witness: $\{(i, \Pi_i)\}_{i \in S}$

where S is set of all indicies $\hat{V}^{\pi}$ reads over all random choices

$\Rightarrow |S| = poly(n)$

<u>NP verifier</u>: $V(x, \overset{w}{\overbrace{\{(i, \pi_i)\}_{i \in S}}})$

- For all $r \in \{0,1\}^{O(\log(n))}$:
  - Simulate $\underline{\hat{V}^{\pi}}$ w/ randomness r. If $\hat{V}$ queries j, check if pair $(j, \pi_j) \in w$. Reject if not. Else reply with π_j.

So $L \in NP$.

How tight is the PCP theorem?

can you lower this?

$$PCP(\log(n), 1) = NP$$

$$\parallel$$

$$PCP(\log(n), \mathrm{poly}(n))$$

know: If $P \neq NP$ then

$$NP \not\subseteq PCP(o(\log(n)), o(\log(n)))$$

Theorem:

$$PCP(\mathrm{poly}(n), \mathrm{poly}(n))$$

$$\parallel$$

$$PCP(\mathrm{poly}(n), 1) \supseteq NP$$

we'll prove

$$\parallel$$

$$NEXP = MIP = IOP$$

PCP and Inapproximability

max-SAT

n variables
m clauses

Def: Let ϕ be 3CNF and let b be an assignment of ϕ.
Then, we let

$$SAT_b(\phi) := \frac{\#\text{ clauses satisfied by } \phi(b)}{m}$$

$$SAT_b(\phi) = 1 \leftarrow \phi \text{ is satisfiable}$$

$$\text{max-SAT}(\phi) = \max_b SAT_b(\phi)$$

If ϕ is unsatisfiable, can have $\text{max-SAT}(\phi) = 1 - \frac{1}{m}$.

Would like: for fixed const c

$\text{max-SAT}(\phi) < c \longleftrightarrow$

$\phi \in \overline{3SAT}$

tells us this is impossible

Can show: $\forall \phi$,

$\text{max-SAT}(\phi) \geq \frac{7}{8}$

Approximating max-SAT

Def: Let $\rho < 1$. Then, we say

k is a ρ-approximation for ϕ

if

$\rho \cdot \text{max-SAT}(\phi) \leq k \leq \text{max-SAT}(\phi)$

- A Poly-time alg A is a

ρ-approx for 3SAT if $A(\phi)$ always outputs a $\rho(|\phi|)$-approx for ϕ.

Theorem: Let $P \neq NP$ and suppose 3SAT has a c-amplifying reduction. Then there is no c-approx. alg for 3SAT.

Def: Let $c < 1$. A c-amp. 3SAT reduction is a poly-time f s.t.

- If $\phi \in$ 3SAT, then

$f(\phi) \in 3SAT$

- If $\text{max-SAT}(\phi) < 1$ then $\text{max-SAT}(f(\phi)) < c$

Lemma: $NP \subseteq PCP(\log(n), 1)$
$\Longleftrightarrow$ 3SAT has an amplifying reduction f

Other NP-complete problems

- Vertex Cover / Ind set

- **Thm**: If $P \neq NP$, then $\exists\, \rho < 1, \rho' > 1$ s.t.

there is no

- ρ-approx for max-Ind-set
- ρ'-approx for min-vertex-cover.

Thm: There is no $1/2$-approx for Max-Ind-set.

Thm: If $P \neq NP$, then $\forall \rho\, (0,1]$, Max-Ind-SET cannot be ρ-approx in poly-time.

Next Time

$$NP \subseteq PCP(\text{poly}(n), 1)$$

Lecture 23