LECTURE 19

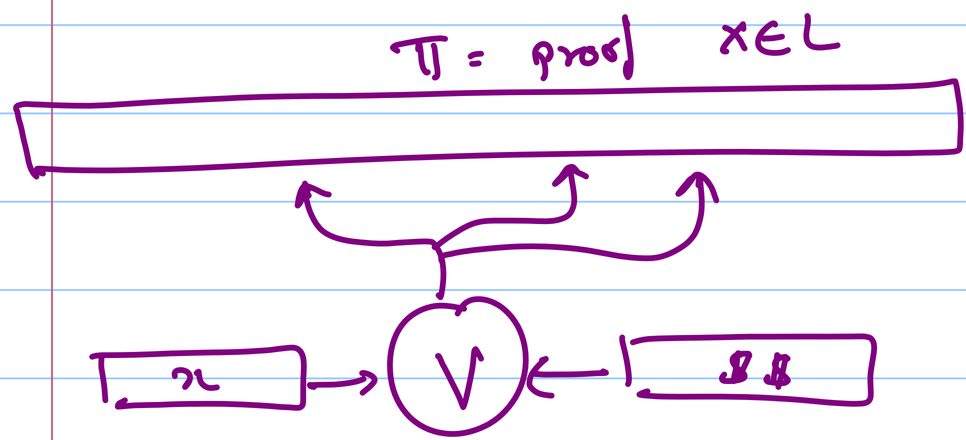
Note Title 4/23/2007

TODAY: PCP's Contd.

- An Exponentially long PCP for Satisfiability.

Review of last lecture: 2 views of PCP

(1)



$$x \in L \Rightarrow \exists \pi \ \Pr[V^{\pi}(x,R)] \geq c(n)$$

$$x \notin L \Rightarrow \forall \pi \ \Pr[V^{\pi}(x,R)] \leq s(n)$$

② $L \leq$ Generalized Graph k-coloring

$x \in L \Rightarrow G_x$ k-colorable

$x \notin L \Rightarrow$ Every k-coloring violates ϵ-fraction of colors.

<u>Today's result:</u> Exponentially long proof verifiable w. $O(1)$ queries.

- Non-trivial in View 1
- Trivial in View 2

<u>Key Ideas:</u> - Arithmetization of SAT

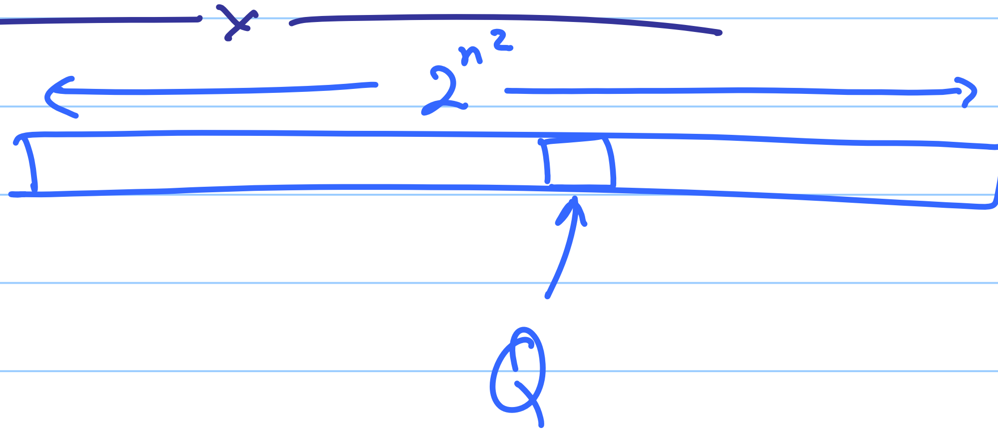
- Nice Properties of Linear functions; (low-degree polynomials).

L = Quadratic SAT

Input = $P_1 \ldots P_m$ m poly of deg 2 in n variables.

Goal: $\exists\, (a_1 \ldots a_n) = \bar{a}$ s.t. $P_1(\bar{a}) = P_2(\bar{a}) \ldots P_m(\bar{a}) = 0$.

PCP: $\Pi =$



$$\Pi[Q] = Q(a) \quad \forall \text{ quadratic function } Q$$

$$\left(\text{so} \quad Q(x_1 \ldots x_n) = \sum_{\substack{1 \le i \le n \\ 1 \le j \le n}} q_{ij}\, x_i x_j + q_0 \right)$$

$$Q \equiv (\{q_{ij}\}, q_0)$$

How to check this proof?

Problem: Π may not equal $\{Q[a]\}_Q$

for any a.

Solution:

Test $\left\{ \begin{array}{l} \text{Will ensure } \underline{\exists\ a} \text{ s.t.} \\ \Pi[Q] = Q(a) \quad \underline{\text{for most } a}. \end{array} \right.$

New Problem: How to test that for $\underline{\text{this}}$ a

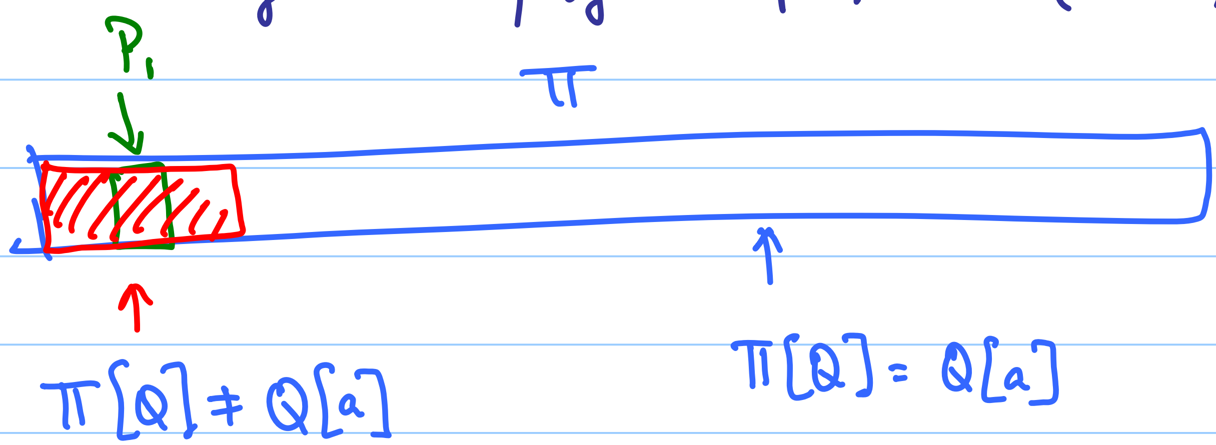
$$P_1(a) = P_2(a) = \cdots P_m(a) = 0 \quad ?$$

New Solution

Will give prob. alg. to check this if Π satisfies Test.

Test(ed) $\Longrightarrow$ Satisfaction test.

- Suppose only one poly P_1. $(m=1)$.



- Can't just read $\pi[P_1]$! maybe wrong.
- But can compute $\tilde{\pi}(P_1)$

$$= \pi[P_1 + Q] - \pi[Q]$$

$$\shortparallel$$

$$(P_1+Q)(a) \quad - \quad Q(a) \quad = \underset{\substack{\uparrow \\ \text{whp.}}}{P_1(a)}$$

Formally: if $\Pr_Q[\pi[Q] \neq Q[a]] \leq \delta$

then $\Pr[\tilde{\pi}(P_1) \neq P_1(a)] \leq 2\delta$

- Many $P_1 \dots P_m$?

  - Can't repeat above for every m!
  - Any way to do $\bigwedge_{j=1}^{m} P_j$ efficiently?

    (algebraically, low-degree ?)

<u>Solution</u>: Pick $\alpha_1 \dots \alpha_m \in_U \{0,1\}$

& check $P_{\bar{\alpha}} = \sum \alpha_j P_j$

if $P_1 \dots P_m = 0$ then so is $P_{\bar{\alpha}}$

if $\exists j \; P_j \neq 0$ then $\Pr_{\bar{\alpha}}[P_\alpha(a) \neq 0] \geq \frac{1}{2}$.

Back to "Test"! How to do it?

Goal: Given $\Pi = \{ \Pi[Q] \}_Q$

Test: $\exists$ a s.t.

$$\Pr_Q \left[\Pi[Q] \neq Q(a) \right] \leq \delta .$$

Idea: Look for structural properties of such a Π & test for them.

Example: $\forall \; Q_1 , Q_2$

$$(Q_1 + Q_2)(a) = Q_1(a) + Q_2(a)$$

Can test this

$$\Pi[Q_1 + Q_2] \stackrel{?}{=} \Pi[Q_1] + \Pi[Q_2] \; ?$$

- $\forall \; Q_1, Q_2$? clearly terrible !
- $O(n^2)$ times ? $O(n)$ times ? $O(1)$ times? (for random Q_1, Q_2).

Remarkable Theorem [BLR]:

$$\Pr_{Q_1, Q_2}\left[\Pi[Q_1] + \Pi[Q_2] = \Pi[Q_1+Q_2]\right]$$

$$= 1-\epsilon > \frac{7}{9}$$

$\Rightarrow \exists\ \tilde{\Pi}$ s.t. $\forall Q_1 Q_2$

$$\tilde{\Pi}[Q_1] + \tilde{\Pi}[Q_2] = \tilde{\Pi}[Q_1+Q_2]$$

& $\Pr_{Q}\left[\Pi[Q] \neq \tilde{\Pi}[Q]\right] \leq 2\epsilon$.

WON'T PROVE THEOREM!

What does $\tilde{\Pi}$ look like?

$\Rightarrow \exists\ y_0, y_{ij}$ s.t.

$\forall\ Q = (\{q_{ij}\}, q_0)$; $\tilde{\Pi}[Q] = \sum q_{ij} y_{ij} + q_0 y_0$

Are we done ?

Still need to test

① $y_{ij} = x_i \cdot x_j \quad \forall i, j$

② $y_0 = 1$

② Easy!

Verify $\bar{1}(a) = 1 \quad (\forall a)$

$\bar{1} = \{\{0\}, 1\}$

$\tilde{\Pi}[\bar{1}] = 1 \approx \Pi[Q + \bar{1}] - \Pi[Q] = 1\,?$

III. Satisfiability of $P_1, \dots P_m$

- $\bar{\alpha} = (\alpha_1 \dots \alpha_m) \longleftarrow$ random ; $Q \leftarrow$ random
- $P_{\bar{\alpha}} = \sum \alpha_j P_j$

$$\pi[Q + P_{\bar{\alpha}}] - \pi[Q] = 0 \ ?$$

Analysis:

1. Makes $14 = O(1)$ queries ;
2. $(\exists a$ s.t. $P_j(a) = 0 \ \forall j)$

   $\Rightarrow \exists \pi, \pi_{lin}$ s.t. $\Pr[\text{verifier}] = 1$

3. $\Pr[\text{Verifier accepts}] \geq .99$

   $\Rightarrow \exists a$ s.t. $P_1(a) = \dots = P_m(a) = 0$

- Continuing optimism ....

Pick random w, v

$$[\; w^T \;] \begin{bmatrix} & & \\ & Y & \\ & & \end{bmatrix} \begin{bmatrix} \\ v \\ \\ \end{bmatrix} = [\; w^T \;] \begin{bmatrix} \\ X \\ \\ \end{bmatrix} [\; X^T \;] \begin{bmatrix} \\ v \\ \\ \end{bmatrix}$$

<u>Claim</u>: if $Y \neq XX^T$ then

$$\Pr_{v,w}\left[w^T Y v \neq w^T X X^T v \right] \geq \frac{1}{4}$$

<u>Proof</u>: Exercise

So how to test ...

$$\underbrace{[\; w^T \;] \begin{bmatrix} & & \\ & Y & \\ & & \end{bmatrix} \begin{bmatrix} \\ v \\ \\ \end{bmatrix}} = [\; w^T \;] \begin{bmatrix} \\ X \\ \\ \end{bmatrix} [\; X^T \;] \begin{bmatrix} \\ v \\ \\ \end{bmatrix}$$

$$\tilde{\Pi}\left[Q_{v,v}\right], \quad Q_{v,v} = \{q_{ij}\}, \quad q_{ij} = v_i w_j .$$

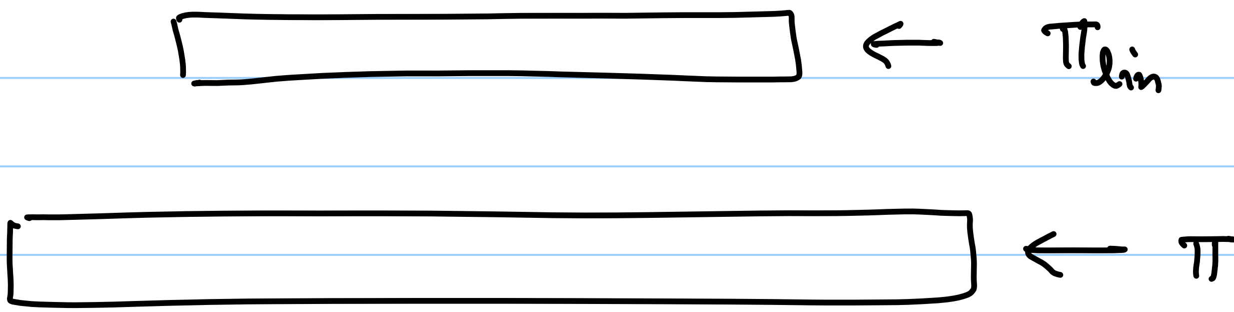
- $w^T X = L_w(a_1 \dots a_n) = \sum w_i a_i$.
- Ask prover to write $L(\bar{a})$ $\forall$ linear function L.
- test by testing

$$\Pi_{lin}[L_1] + \Pi_{lin}[L_2] = \Pi_{lin}[L_1 + L_2].$$

Summary

To prove $\exists\, a$ s.t. $P_1(a) = P_2(a) = \cdots P_m(a) = 0$.

PCP =



(Supposedly $\pi_{lin}[L] = L(a)$ $\leftarrow$ linear L

$\pi[Q] = Q(a)$ $\leftarrow$ quad. Q)

VERIFIER:

I: (linearity of π_{lin})

Pick L_1, L_2 at random & check

$$\pi_{lin}[L_1] + \pi_{lin}[L_2] = \pi_{lin}[L_1 + L_2]$$

II. (Quadraticity of π)

II a: $Q_1, Q_2 \leftarrow$ random

$$\pi[Q_1] + \pi[Q_2] = \pi[Q_1 + Q_2]$$

II b: $L_1, L_2 \leftarrow$ random ; $Q \leftarrow$ random

$$\pi[Q + L_1 \cdot L_2] - \pi[Q] = \pi_{lin}[L_1] \cdot \pi_{lin}[L_2]$$

II c: $Q \leftarrow$ random

$$\pi[Q + \bar{1}] - \pi[Q] = 1$$

III. Satisfiability of $P_1, \ldots, P_m$

- $\bar{\alpha} = (\alpha_1, \ldots, \alpha_m) \longleftarrow$ random ; $Q \leftarrow$ random
- $P_{\bar{\alpha}} = \sum \alpha_j P_j$

$$\pi[Q + P_{\bar{\alpha}}] - \pi[Q] = 0 \; ?$$

Analysis:

1. Makes $14 = O(1)$ queries ;
2. ($\exists a$ s.t. $P_j(a) = 0 \;\forall j$)

   $\Rightarrow \exists \pi, \pi_{lin}$ s.t. $\Pr[\text{verifier}] = 1$

3. $\Pr[\text{Verifier accepts}] \geq .99$

   $\Rightarrow \exists a$ s.t. $P_1(a) = \ldots = P_m(a) = 0$

Conclusions:

- Non-trivial PCPs exist.
- But no use in approximation?
- Turns out protocol has use, though we don't know how to use PCP directly.