CMSC 39600 - Lec #10 (Oct 30)

Today
- Hastad's 3-query PCP
- Hardness of MAX3LIN2
- Long Code

Last Lecture

$\exists \epsilon > 0$ gap-3SAT$_\epsilon$ is NP-hard

$\Downarrow$ Parallel Repetition Theorem

$\forall \epsilon, \exists \Sigma$, gap-LC$_\epsilon$ is NP-hard (label cover)

Why is it useful?

Easier to construct objects over large alphabet
- then reduce

eg Coding
Dinur's Proof.

Today

3-query PCPs for NP.

E3LIN2 Instance. ~~$x_i \oplus x_j \oplus x_k = b_i$~~

$x_1 \ldots x_n$

j^{th} eqn $x_{j_1} \oplus x_{j_2} \oplus x_{j_3} = b_j$

(18-2)

Can always solve exactly

Problem: Find assign that maximizes # of eqns satisfied

Trivial 2 approximation - random assignment

Can't do better.

$gap\text{-}3LIN2_{1-\varepsilon,\ \frac{1}{2}+\delta}$

- YES: $\exists$ assign that satisfies $\geq (1-\varepsilon)$
- NO: $\forall$ assign $\leq (\frac{1}{2}+\delta)$ eqns satisfied.

$gap\text{-}LC^{\Sigma}_{1,\mu} \longrightarrow gap\text{-}3LIN_{1-\varepsilon,\frac{1}{2}+\delta}$

Theorem [Håstad 97]

$\forall\ \varepsilon, \delta > 0$, $gap\text{-}3LIN2_{1-\varepsilon,\ \frac{1}{2}+\delta}$ is NP-hard.

Corollary:

$NP \subseteq PCP_{1-\varepsilon,\frac{1}{2}+\delta}[O(\log n),\ 3]$

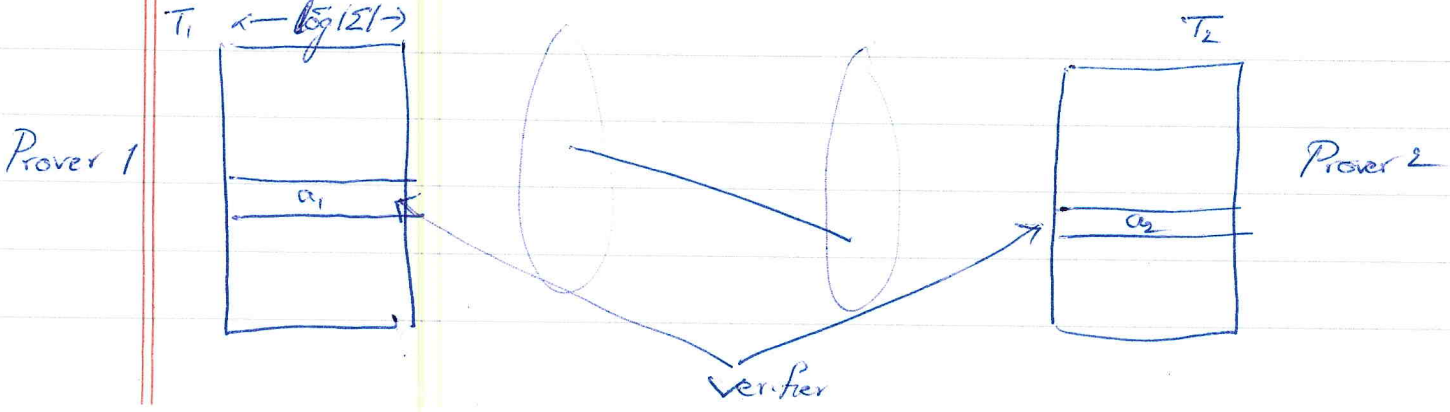
Remark: Im Perfect Completeness

Perfect Completeness achievable

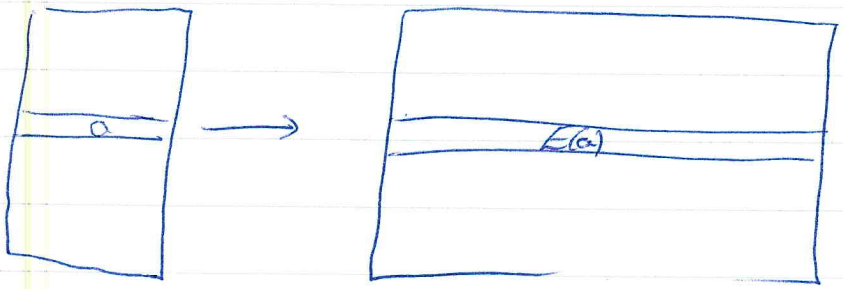
[CLST: $NP \subseteq PCP_{1,\frac{1}{2}+\delta}[O(\log n), 3]$

not using linear eqns:

Label Cover



Encode any $a_1 \neq a_2$ s.t 3 bits suffice



Which encoding?

LONG: $a \longmapsto \langle f(a) \rangle_{f \in \mathcal{F}}$ $\quad (\mathcal{F} = \{f : \{0,1\}^k \to \{0,1\}\})$

$a \in \{0,1\}^k$

$(k = \log|\Sigma|)$

k bits $\longrightarrow$ 2^{2^k} bits

} Long-Code

longest possible encoding (w/o repetition)

Alternate view

$f \longrightarrow T_f$ (truth table of f)

$T_f \in \{0,1\}^{2^k}$

Dictator f_a: $A(a) = x_a$

$a \longmapsto \langle T_f, e_a \rangle$ $\quad e_a \in \{0,1\}^{2^k}$

$= \ell_a(\cdot)$ $\quad \{0 \ldots 1 \ldots 0\}$

WH encoding of the unit vector e_a

[Can use Fourier analysis]

$\forall a \in \{0,1\}^{2^k}$ $\quad$ character f_a: $\chi_a(x) = (-1)^{\langle a, x \rangle}$

$S_a \subseteq \{0,1\}^k$ $\quad \chi_{S_a}(f) = \prod_{a \in S_a} f(a)$

Long Code Testing

$A: \{0,1\}^{2^k} \to \{\pm 1\}$ - Test if long-code.

long code - linear

Can apply BLR-Test

1. Choose $x, y \in_R \{0,1\}^{2^k}$ (ie, $f, g \in_R \mathcal{F}$)
2. $A(x)\,A(y) = A(x+y) = 1$

→ Non-long code fail WH code pass w/p 1 (eg: $f_x()$ for $x \neq e_a$)

Perturbed BLR-Test

$\mu: \{0,1\}^{2^k} \to \{\pm 1\}$

$$\mu(x) = \begin{cases} 1 & \text{w.p } 1-\epsilon/2 \\ -1 & \text{w.p } \epsilon/2 \end{cases} \Bigg] - \epsilon\text{-bias}$$

Perturbed BLR

1. Choose $x, y \in_R \{0,1\}^{2^k}$, μ - ϵ-bias
2. $A(x)\,A(y)\,A(x+y+\mu) = 1$

Completeness: $A = LONG(a) \Rightarrow Pr[\text{Pert-BLR acc}] = 1-\epsilon$.

Soundness

$$P_R[\text{Per-BLR acc}] = \mathop{\mathbb{E}}_{x,y,\mu}\left[\frac{1+A(x)A(y)A(xy\mu)}{2}\right]$$

$$= \frac{1}{2} + \frac{1}{2}\sum_{S,T,U}' \hat{A}_S \hat{A}_T \hat{A}_U \mathop{\mathbb{E}}_{x,y,\mu}\left[\chi_S(x)\chi_T(y)\chi_U(xy)\chi_U(y)\chi_U(\mu)\right]$$

$$= \frac{1}{2} + \frac{1}{2}\sum_{S}' \hat{A}_S^3 \mathop{\mathbb{E}}_{\mu}\left[\chi_S(\mu)\right]$$

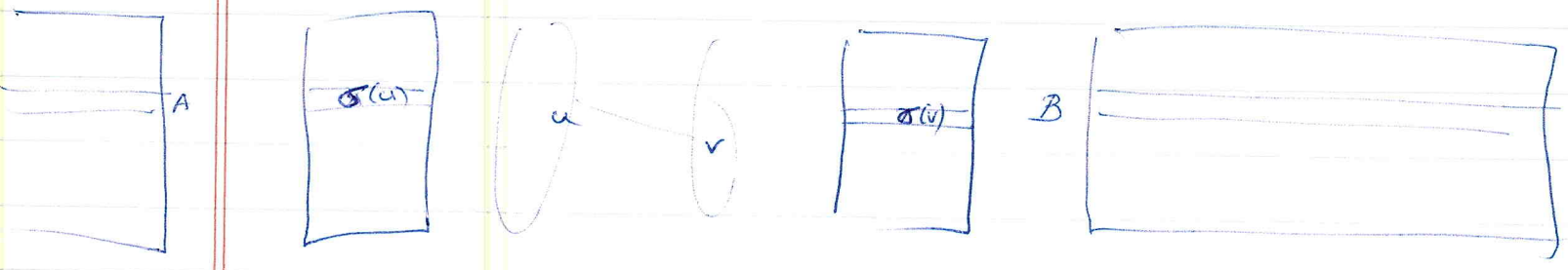
$$\mathop{\mathbb{E}}_{\mu}\left[\chi_S(\mu)\right] = \mathop{\mathbb{E}}_{\mu}\left[\prod_{a\in S}\mu(a)\right] = \prod_{a\in S}\mathop{\mathbb{E}}_{\mu}\left[\mu(a)\right] = (1-\epsilon)^{|S|}$$

$$P_R[\text{acc}] = \frac{1}{2} + \frac{1}{2}\sum_{S}' \hat{A}_S^3 (1-\epsilon)^{|S|}$$

$$\leq \frac{1}{2} + \frac{1}{2}\max_S\left(\hat{A}_S(1-\epsilon)^{|S|}\right) \leq \frac{1}{2} + \frac{1}{2}\max_S \hat{A}_S e^{-\epsilon|S|}$$

$$P_R[\text{acc}] \geq \tfrac{1}{2}+\delta \Rightarrow \exists\, S \text{ s.t. } \hat{A}_S \geq 2\delta$$
$$\geq |S| \quad O\left(\tfrac{1}{\epsilon}\log\tfrac{1}{\delta}\right)$$

Back to original problem



$A := \text{LONG}(\sigma(u))$ $\quad \pi_\epsilon(\sigma(u)) = \sigma(v)$ $\quad B := \text{LONG}(\sigma(v))$

$u, v \in \Sigma' = \{0,1\}^k$

$\pi(\sigma(u)) = \sigma(v)$

1. Choose $f, g \in_R \{0,1\}^{2^k} \mathcal{F}$
2. $A(f)\, A(f)\, B(g)\, A(g \circ \pi) f) = 1.$

$A(x) = x_{\sigma(u)}$

$B(x) = x_{\sigma(v)} = x_{\pi \circ \sigma(v)}$

$A(x \circ \pi) = x \circ \pi$

$A(f) = f(\sigma(u))$

$B(f) = f(\sigma(v)) = f \circ \pi(\sigma(u))$

$A(f \circ \pi) = f \circ \pi(\sigma(u))$

$f(\sigma(u)) = g \circ \pi(\sigma(u))$

---

1. Choose $f, g \in_R \mathcal{F}$, $\mu \in_R \epsilon$-bias
2. Accept if $A(f)\, B(g)\, A(g \circ \pi) f \mu) = 1$

Completeness $\Pr[\text{acc}] = 1 - \frac{\epsilon}{2} > 1 - \epsilon$

Problem: All 1's fools the test.

Assume $A(x) = -A(x)$

1-Folding: $A(x) = -A(-x)$

Claim: $A: \{0,1\}^{2^k} \to \{\pm 1\}$ is 1-folded, then $\hat{A}_\phi = 0$ $\forall$ $|S|$-even

Pf $\hat{A}_\phi = \sum_x A(x) = 0$

$$\pi_2(S) = \{ j \in \{1,\dots,m\} \mid \exists \text{ odd } \# \text{ of } i \text{ s.t. } \pi(i) = j \}$$

$$\chi_S(f \circ \pi) = \chi_{\pi_2(S)}(f)$$

$$\chi_S(f \circ \pi) = \prod_{z \in S} (f \circ \pi)(z) = \prod_{z \in S} f(\pi(z))$$

$$= \prod_{y \in \pi(S)} \left[\prod_{\substack{z \in S \\ \pi(z) = y}} f(z_y) \right] = \prod_{y \in \pi_2(S)} f(y) = \chi_{\pi_2(S)}(f)$$

Soundness:

$$\Pr[\text{acc}] = \mathop{\mathbb{E}}_{u,v,x,y,\mu} \left[\frac{1 + A(f) B(g) A(g \circ \pi) + \mu}{2} \right]$$

$$= \mathop{\mathbb{E}}_{u,v} \left[\frac{1}{2} + \frac{1}{2} \sum_{S,T,U} \hat{A}_S \hat{A}_U \hat{B}_T \mathop{\mathbb{E}}_{f,g,\mu} [\chi_S(f) \chi_T(g) \chi_U(g \circ \pi) \chi_U(f) \chi_U(\mu)] \right]$$

$$= \mathop{\mathbb{E}}_{u,v} \left[\frac{1}{2} + \frac{1}{2} \sum_{S,T} \hat{A}_S^2 \hat{B}_T \mathop{\mathbb{E}}_{g} [\chi_T(g) \chi_U(g \circ \pi)] \mathop{\mathbb{E}}_{\mu} [\chi_S(\mu)] \right]$$

$$= \mathop{\mathbb{E}}_{u,v} \left[\frac{1}{2} + \frac{1}{2} \sum_{S} \hat{A}_S^2 \hat{B}_{\pi_2(S)} (1-\epsilon)^{|S|} \right]$$

Hence —

$$\Pr[\text{acc}] \geq \frac{1}{2} + \delta \Rightarrow \mathop{\mathbb{E}}_{e=(u,v)} \left[\sum_S \hat{A}_S^2 \hat{B}_{\pi_2(S)} (1-\epsilon)^{|S|} \right] \geq 2\delta$$

Hence for at least δ fraction of edges $\sum_S \hat{A}_S^2 \hat{B}_{\pi_2(S)} (1-\epsilon)^{|S|} \geq \delta$

Fix this δ fraction of edges

Decoding an assignment

$a \in L$ — 1. Choose $S \in \{0,1\}^t$ w.p. $\hat{A}_S^2$

2. Set $\sigma(a) \leftarrow S$

3. Set $\sigma(a) = S$.

Similarly for v.

$$\Pr[\pi(\sigma(a)) = \sigma(v)] \geq \sum_{S \neq \phi} \sum_{T \subseteq \pi(S)} \hat{A}_S^2 \hat{B}_T^2 \frac{1}{|S|}$$

$$\geq \sum_S \hat{A}_S^2 \hat{B}_{\pi_2(S)} \frac{1}{|S|}$$

$$\geq \sum_S \left(\hat{A}_S \hat{B}_{\pi_2(S)} \frac{1}{\sqrt{|S|}}\right)^2 \sum \hat{A}_S^2$$

$$\geq \left(\sum_S \hat{A}_S^2 \hat{B}_{\pi_2(S)} \frac{1}{\sqrt{|S|}}\right)^2$$

Prop: $\frac{1}{\sqrt{|S|}} \geq \sqrt{(2\epsilon)^{|S|}} (1-\epsilon)^{|S|}$

Pf: $(2\epsilon|S|)^{-1/2} \geq e^{-\epsilon|S|}$ $\left(\frac{1}{x} \geq e^{-x}\right)$

$\geq (1-\epsilon)^{|S|}$

For each (a,v) in δ-fraction,

$\Pr[(a,v) \text{ is satisfied}] \geq 2\epsilon \left(\sum_S \hat{A}_S^2 \hat{B}_{\pi_2(S)} (1-\epsilon)^{|S|}\right)^2$

$\geq 2\epsilon\delta^2$

Hence $2\epsilon\delta^3$ edges satisfied

$2\epsilon\delta^3 \geq \mu$ — contradicts gap-LC$_{1,\mu}$