6.S979 Lecture 16

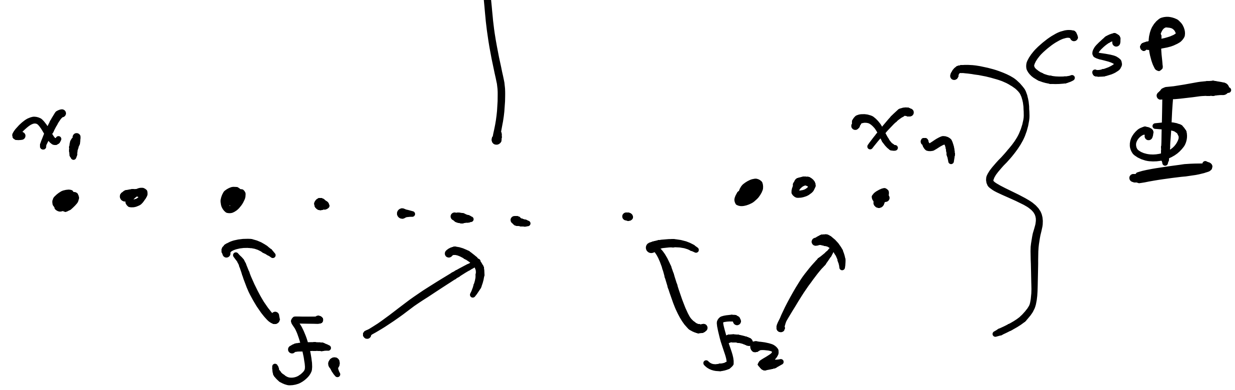
- This Friday OH will be 3-4 pm Eastern

Goal: understand power of MIP

$$NP \subseteq MIP[\log(n)]$$

$$(NEXP = MIP)$$

Clause Var. game



NP-hard: YES: $\omega(\Phi) = 1$.

NO: $\omega(\Phi) \leq 1/2$.

fraction of constraints satisfiable

Idea: "encode" an NP-hard problem (QUADEQ)

$$\Sigma_H(\underset{\in\{0,1\}^n}{\underline{x}}) = \underbrace{\left(\langle x, 0\ldots 0\rangle, \langle x, 0\ldots 01\rangle, \ldots\right)}_{\in\{0,1\}^{2^n}}$$

$$\Sigma(x) = \overbrace{\Sigma_H(x)}, \overbrace{\Sigma_H(x \otimes x)}$$

<u>Last time:</u> Given access to $\underset{\sim}{\Sigma(x)}$ can check whether x satisfies a system of quad. eq. with just 2 queries to $\underset{\sim}{\Sigma(x)}$

YES: x satisfies $\Longrightarrow$ test passes w/ certainty

NO: x doesn't satisfy $\Longrightarrow$ test pass w/ prob $\leq 1/2$

Today: Given $y \in \{0,1\}^{2^n}$, check that y is close to $\mathcal{E}_H(x)$ for some x, using $\underline{3}$ queries to y

- YES: If $y = \mathcal{E}_H(x)$, then test passes w/ certainty
- NO: If y differs from $\mathcal{E}_H(x)$ on at least δ-frac. of positions (for all x), then test succeeds w/ prob. $\leq 1 - \Omega(\delta)$

Note: This looks like self-testing

First: Some notational changes

Think of y as truth table of

$$f : \{0,1\}^n \to \{0,1\}$$

$$\underbrace{(f(0..0),\ f(0...01),\ f(0...10),\ ....)}_{2^n}$$

$$\mathcal{E}_H(x) = (\langle x, 0\ldots0\rangle, \langle x, 0\ldots01\rangle, \langle x, 0\ldots10\rangle, \ldots)$$

$$g_x(a) = \langle x, a\rangle \quad \Leftarrow \text{linear functions } (\text{mod } 2)$$

$\in \{0,1\}^n$

Goal: Given f, is it close to $g_x(\cdot) = \langle x, \cdot\rangle$ for some x

Test [BLR]:

Pick $a, b \in \{0,1\}^n$ at random

Check $f(a) + f(b) = f(a+b)$

- YES: $f(a) = \langle x, a\rangle$

$$f(a) + f(b) = \langle x, a\rangle + \langle x, b\rangle$$
$$= \langle x, a+b\rangle$$
$$= f(a+b) \checkmark$$

- NO: Suppose BLR test passes w/ prob. $1-\varepsilon$

$\Rightarrow \exists x$, f is $O(\varepsilon)$-close to g_x

Notational change #2:

$\{0,1\} \longrightarrow \{1,-1\}$

Instead of f work with $(-1)^f = F$

BLR test: $f(a)+f(b) \stackrel{?}{=} f(a+b)$

$$\underbrace{F(A)}_{\in\{\pm1\}^n} \underbrace{F(B)}_{\in\{\pm1\}^n} \stackrel{?}{=} F(\underbrace{A \circ B}_{\in\{\pm1\}^n})$$

entrywise product

$g_x(a) = \langle x, a\rangle$

$$G_x(A) = (-1)^{\langle x,a\rangle} = \prod_{i:\, x_i=1} A_i$$

$A = (-1)^a$, $A_i = (-1)^{a_i}$

fourier characters

Capital $= \pm 1$, lower case $= \{0,1\}$

Fourier analysis of Boolean functions:

$F: \{\pm 1\}^n \longrightarrow \{\pm 1\}$ $\qquad x_i^2 = 1$

$F(x_1, \ldots, x_n)$

$= \hat{F}_0 + \hat{F}_{\{1\}} x_1 + \hat{F}_{\{2\}} x_2 + \ldots$

$+ \hat{F}_{\{12\}} x_1 x_2 + \ldots + \hat{F}_{\{12\ldots n\}} x_1 x_2 x_3 \ldots x_n$

Fourier decomposition of F

$\hat{F}_S \cdot \prod_{i \in S} x_i$

subset of $\{1, \ldots, n\}$

$$\hat{F}_S = \mathbb{E}_{x \in \{\pm 1\}^n} F(x) \cdot \overbrace{\prod_{i \in S} x_i}^{\chi_S(x)}$$

$$= \mathbb{E}_{x \in \{0,1\}^n} (-1)^{\langle S, x \rangle} F(x)$$

Fourier transform over $\{\pm 1\}^n$ $\qquad \langle F, F \rangle$

$\langle \hat{F}, F \rangle$

$$\sum \hat{F}_S^2 = 1 = \mathop{\mathbb{E}}_{x\in\{\pm1\}^n} F(x)^2$$

$$F(x)^2 = 1$$

Plancherel thm.

$$\langle F, G \rangle := \mathop{\mathbb{E}}_{x\in\{\pm1\}^n} F(x)G(x)$$

orthonormal basis

$$S \neq T \qquad \langle \chi_S, \chi_T \rangle = 0$$

$$\chi_S = \prod_{i\in S} x_i \qquad \chi_T = \prod_{i\in T} x_i$$

Suppose F that passes BLR test w/ prob. $1-\varepsilon$

$$\Longleftrightarrow \Pr_{A,B}\Big[\underbrace{F(A)\cdot F(B)\cdot F(A\circ B)}_{\text{either } 1 \text{ or } -1} = 1\Big] = 1-\varepsilon$$

$$\mathop{\mathbb{E}}_{A,B} F(A)\cdot F(B)\, F(A\circ B) = 1-2\varepsilon$$

$$F(A) = \sum_{S} \hat{F}_S \cdot \chi_S(A)$$

$$\mathop{\mathbb{E}}_{A,B} \sum_{S,T,U} \hat{F}_S \cdot \hat{F}_T \cdot \hat{F}_U \cdot \chi_S(A)\chi_T(B)\, \chi_U(A\circ B)$$

subsets of $\{1,\ldots,n\}$

indicator of S

$(a_1 \ldots a_n)$

$$\chi_S(A) = \prod_{i\in S} \underset{\substack{\| \\ (-1)^{a_i}}}{A_i} = (-1)^{\langle s,a\rangle}$$

$$\mathop{\mathbb{E}}_{a,b} \sum_{s,t,u} \hat{F}_s \cdot \hat{F}_T \cdot \hat{F}_u \cdot (-1)^{\langle s,a\rangle} \cdot (-1)^{\langle t,b\rangle} \cdot (-1)^{\langle u,a+b\rangle}$$

$$= \mathop{\mathbb{E}}_{a,b} \sum_{s,t,u} \hat{F}_S \cdot \hat{F}_T \cdot \hat{F}_u (-1)^{\langle s+u,a\rangle} \cdot (-1)^{\langle t+u,b\rangle}$$

Nonzero iff $s+u=0$
$s=u$

$$= \sum_{s,t,u} \hat{F}_S \cdot \hat{F}_T \cdot \hat{F}_u \left(\mathbb{E}_a (-1)^{\langle s+u, a\rangle} \right) \cdot \left(\mathbb{E}_b (-1)^{\langle t+u, b\rangle} \right)$$

Nonzero iff $t = u$

Recall: if $x \neq 0$, $x \in \{0,1\}^n$, $\Pr_a[\langle x, a\rangle = 0] = 1/2$

$$\mathbb{E}_a (-1)^{\langle x, a\rangle} = 0$$

if $x = 0$, $\langle x, a\rangle = 0$

$$\mathbb{E}_a \underbrace{(-1)^{\langle x, a\rangle}}_{(-1)^0} = 1$$

$$= \sum_u (\hat{f}_u)^3 \geq 1 - 2\varepsilon$$

Recall: $\sum_u (\hat{f}_u)^2 = 1$

Plancherel

$$\sum_u (\hat{F}_u)^3 = \sum_u \underbrace{\hat{F}_u}_{\le \max_u \hat{F}_u} \cdot (\hat{F}_u)^2 \ge 1-2\varepsilon$$

$$\max_u \hat{F}_u \cdot \underbrace{\sum_u (\hat{F}_u)^2}_{=1} \ge \sum_u \hat{F}_u \cdot (\hat{F}_u)^2 \ge 1-2\varepsilon$$

$$\max_u \hat{F}_u \ge 1-2\varepsilon$$

$$\Downarrow$$

$$f = \sum_S \hat{F}_S \chi_S \overset{O(\varepsilon)}{\approx} \hat{F}_{\underbrace{u^*}_{\exists u^*}} \chi_{u^*}$$

$$\approx \chi_{u^*} = \prod_{i \in u^*} x_i = (-1)^{\overbrace{\langle u^*, x\rangle}^{\text{linear function!!!}}}$$

Putting it all together:

CSP looks like this:

Variables $y^{(1)}, y^{(2)}$ $\quad$ Should be $= \mathcal{E}_H(x)\, \mathcal{E}_H(x \otimes x)$

Constraints:

— BLR constraints:

$$y^{(1)}_a + y^{(1)}_b = y^{(1)}_{a+b}$$

$$y^{(2)}_a + y^{(2)}_b = y^{(2)}_{a+b}$$

— "Tensor product" constraint confuse

$$y^{(1)}_a \cdot y^{(1)}_b = y^{(2)}_{a \otimes b + c} \cdot y^{(2)}_c$$

$$y^{(2)}_{a\otimes b} = \langle a \otimes b, x \otimes x \rangle = (\underbrace{\langle a, x \rangle}_{= y^{(1)}_a}) \cdot (\underbrace{\langle b, x \rangle}_{= y^{(1)}_b})$$

$a \otimes b$ not uniformly random

But $\underbrace{a \otimes b + c \text{ is} \quad c \text{ is}}$

to learn $\underline{\underline{f}}(a)$, given $f(a+b)$
$f(b)$

"self-correction",
"interpolation"

— Quad. eq.

$$a x + b x x = c$$

$$y_a^{(1)} + y_b^{(2)} = c$$

$$\downarrow \qquad \downarrow$$

$$y_{a+d}^{(1)} + y_d^{(1)} + y_{b+d'}^{(2)} + y_d^{(2)} = c$$