Computational Complexity Theory, Fall 2010 December 8

Lecture 25: PCP based on Linearity Testing

Lecturer: Kristoffer Arnsfelt Hansen Scribe: Allan Rasmussen

Recap from previous Lecture

In the previous lecture we defined the class of languages $\mathbf{PCP}(r(n), q(n))$ to be those languages having a $(c \cdot r(n), d \cdot q(n))$-**PCP** verifier for some $c, d > 0$.

Definition 1 (**PCP** verifier)**.** We say that a language L has a $(r(n), q(n))$-**PCP** verifier if there exists a polynomial-time probabilistic algorithm V satisfying:

Efficiency: Given input x of length n and random access to a proof π, V uses at most $r(n)$ bits of randomness and makes at most $q(n)$ nonadaptive queries to locations of π. Denote by $V^\pi(x)$ the random variable describing the output (1/0 for accept/reject) of the algorithm.

Completeness: If $x \in L$, there exists a proof π, such that V always accepts π as a proof for x; $\Pr[V^\pi(x) = 1] = 1$.

Soundness: If $x \notin L$, V will for any proof π, reject π as a proof for x with probability at least a half; $\Pr[V^\pi(x) = 1] \leq 1/2$.

We also stated the **PCP** theorem;

Theorem 2 (The **PCP** Theorem)**.** $\mathbf{NP} = \mathbf{PCP}(\log n, 1)$.

and proved its equivalence with both

Theorem 3 (**PCP** Theorem: Hardness of approximation view)**.** *There exists $\rho < 1$, such that for every $L \in \mathbf{NP}$, there is a polynomial-time function f mapping strings to 3CNF formulaes, such that*

$$\begin{aligned} x \in L &\Rightarrow \mathrm{val}(f(x)) = 1, \\ x \notin L &\Rightarrow \mathrm{val}(f(x)) < \rho. \end{aligned} \tag{1}$$

and ρ-GAPqCSP being **NP**-hard for some q and $\rho < 1$.

We also reviewed the language QUADEQ. A system of m quadratic equations in n variables over GF(2) is represented by m matrices $A_1, \ldots, A_m$ of size $n \times n$ and a vector $\mathbf{b}$ of size m (all with entries in GF(2)):

$$\mathbf{u}^T A_k \mathbf{u} = b_k, \qquad (k = 1, \ldots, m). \tag{2}$$

The language QUADEQ consists of the satisfiable systems of quadratic equations. By a simple reduction from CIRCUIT-SAT we proved that QUADEQ is **NP**-hard.

Linear Funcitons on $\{0,1\}^n$

Definition 4. A function $f\colon \{0,1\}^n \to \{0,1\}$ is linear if

$$f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y}) \qquad (\mathbf{x},\mathbf{y} \in \{0,1\}^n). \tag{3}$$

Addition on $\{0,1\}$ is modulo 2 and $(\mathbf{x}+\mathbf{y})_i = x_i + y_i$. In other words we regard $\{0,1\} = \mathrm{GF}(2)$ as the field with two elements and $\{0,1\}^n$ as a product vector space. The following lemma is basic linear algebra.

Lemma 5. *The function f is linear if and only if there exists $\mathbf{a} \in \{0,1\}^n$ such that*

$$f(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} \qquad (\mathbf{x} \in \{0,1\}^n). \tag{4}$$

With f given as (4), the truth table of f is actually the Walsh-Hadamard code $\mathrm{WH}(\mathbf{a})$ for $\mathbf{a}$.

Theorem 6 (Linearity Testing)**.** *Assume $f\colon \{0,1\}^n \to \{0,1\}$ satisfies*

$$\Pr_{\mathbf{x},\mathbf{y}}[f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})] \geq \rho \tag{5}$$

for some $\rho > 1/2$. Then there exists $\mathbf{a} \in \{0,1\}^n$ such that

$$\Pr_{\mathbf{x}}[f(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x}] \geq \rho. \tag{6}$$

We may also express the condition (6) by saying that f is ρ-close to a linear function (namely $\mathbf{x} \mapsto \mathbf{a} \cdot \mathbf{x}$). We may use Theorem 6 to **reject functions $f\colon \{0,1\}^n \to \{0,1\}$ that are not ρ-close to a linear function**:

> *Input:* f (as a truth table).
>
> *Operation:* Pick $\mathbf{x},\mathbf{y} \in \{0,1\}^n$ uniformly at random and test whether $f(\mathbf{x}+\mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$. Reject if test fails. Repeat k times.
>
> *Analysis:* If (6) is not satisfied for some a, then (5) is not satisfied, and we reject with probability at least $1 - \rho^k$.

(Notice that functions ρ-close to a linear function very well may be rejected — only truly linear functions are never rejected.) We will use Fourier analysis to prove Theorem 6.

Fourier Analysis on $\{1,-1\}^n$

We define the inner product of two real functions $f, g\colon \{1,-1\}^n \to \mathbb{R}$ by

$$\langle f, g \rangle = \mathrm{E}_{\mathbf{x}}[f(\mathbf{x})g(\mathbf{x})] = 1/2^n \sum_{\mathbf{x} \in \{1,-1\}^n} f(\mathbf{x})g(\mathbf{x}) \tag{7}$$

The **Fourier basis/characters** on $\{1,-1\}^n$ are parametrized by $S \subseteq \{1,\ldots,n\}$;

$$\chi_S(\mathbf{x}) = \prod_{i \in S} x_i \qquad (\mathbf{x} \in \{1,-1\}^n). \tag{8}$$

They satisfy (with $(\mathbf{x} \odot \mathbf{y})_i = x_i y_i$)

$$\chi_S(\mathbf{x} \odot \mathbf{y}) = \chi_S(\mathbf{x})\chi_S(\mathbf{y}) \qquad (\mathbf{x}, \mathbf{y} \in \{1,-1\}^n), \tag{9}$$

and constitute an orthonormal basis:

$$\langle \chi_S, \chi_T \rangle = \mathrm{E}_{\mathbf{x}}[\prod_{i \in S} x_i \cdot \prod_{i \in T} x_i] = \mathrm{E}_{\mathbf{x}}[\prod_{i \in S \Delta T} x_i] = \begin{cases} 1 & S = T, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

Any function $f\colon \{1,-1\}^n \to \mathbb{R}$ may be written as a linear combination $\sum_{S \subseteq \{1,\dots,n\}} \hat{f}(S)\chi_S$ of the characters, where the Fourier coefficient $\hat{f}(T)$ to χ_T is given by

$$\langle f, \chi_T \rangle = \big\langle \sum_S \hat{f}(S)\chi_S, \chi_T \big\rangle = \sum_S \hat{f}(S)\langle \chi_S, \chi_T \rangle = \hat{f}(T). \tag{11}$$

Proposition 7 (Plancherel theorem)**.** *For any $f, g\colon \{1,-1\}^n \to \mathbb{R}$,*

$$\langle f, g \rangle = \sum_S \hat{f}(S)\hat{g}(S). \tag{12}$$

Proof.

$$\begin{aligned} \langle f, g \rangle &= \langle \sum_S \hat{f}(S)\chi_S, \sum_T \hat{g}(T)\chi_T \rangle \\ &= \sum_{S,T} \hat{f}(S)\hat{g}(T)\langle \chi_S, \chi_T \rangle \\ &= \sum_S \hat{f}(S)\hat{g}(S). \end{aligned} \tag{13}$$

□

Corollary 8 (Parseval identity)**.** *For any $f\colon \{1,-1\}^n \to \mathbb{R}$,*

$$\langle f, f \rangle = \sum_S \hat{f}(S)^2. \tag{14}$$

In particular, if $f\colon \{1,-1\}^n \to \{1,-1\}$ we have $\sum_S \hat{f}(S)^2 = 1$. We are now ready to prove Theorem 6. First, if we make the identification $(0,1) \leftrightarrow (1,-1)$, the linear functions are the functions satisfying

$$f(\mathbf{x} \odot \mathbf{y}) = f(\mathbf{x})f(\mathbf{y}) \qquad (\mathbf{x}, \mathbf{y} \in \{1,-1\}^n). \tag{15}$$

The linear functions are precisely the characters/Fourier basis; if f is definded by **a** as in (4) and $S = \{i = 1, \dots, n : a_i = 1\}$, we have

$$f(\mathbf{x}) = \prod_S x_i = \chi_S(\mathbf{x}) \qquad (\mathbf{x} \in \{1,-1\}^n). \tag{16}$$

Also, for any $f, g\colon \{1,-1\}^n \to \{1,-1\}$,

$$\begin{aligned} \langle f, g \rangle &= E_{\mathbf{x}}[f(x)g(x)] \\ &= \Pr_{\mathbf{x}}[f(x)g(x) = 1] - \Pr_x[f(x)g(x) = -1] \\ &= \Pr_{\mathbf{x}}[f(x)g(x) = 1] - (1 - \Pr_x[f(x)g(x) = 1]) \\ &= 2\Pr_{\mathbf{x}}[f(x)g(x) = 1] - 1 \\ &= 2\Pr_{\mathbf{x}}[f(x) = g(x)] - 1. \end{aligned} \tag{17}$$

So f and g being $(1/2+\epsilon)$-close;

$$\Pr_{\mathbf{x}}[f(x) = g(x)] \geq 1/2 + \epsilon, \tag{18}$$

is equivalent to

$$\langle f, g \rangle \geq 2\epsilon. \tag{19}$$

Proof of Theorem 6. Let $1/2 + \epsilon = \rho$. By assumption $\epsilon > 0$ and

$$E_{\mathbf{x},\mathbf{y}}[f(\mathbf{x})f(\mathbf{y})f(\mathbf{x} \odot \mathbf{y})] \geq 2\epsilon. \tag{20}$$

The left-hand side may be rewritten as follows.

$$\begin{aligned} E_{\mathbf{x},\mathbf{y}}[f(\mathbf{x})f(\mathbf{y})f(\mathbf{x} \odot \mathbf{y})] &= E_{\mathbf{x},\mathbf{y}}\big[\sum_S \hat{f}(S)\chi_S(\mathbf{x}) \cdot \sum_T \hat{f}(T)\chi_T(\mathbf{y}) \cdot \sum_U \hat{f}(U)\chi_U(\mathbf{x} \odot \mathbf{y})\big] \\ &= \sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)E_{\mathbf{x},\mathbf{y}}[\chi_S(\mathbf{x})\chi_T(\mathbf{y})\chi_U(\mathbf{x} \odot \mathbf{y})] \\ &= \sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)E_{\mathbf{x},\mathbf{y}}[\chi_S(\mathbf{x})\chi_T(\mathbf{y})\chi_U(\mathbf{x})\chi_U(\mathbf{y})], \end{aligned}$$

and, since $\mathbf{x}$ and $\mathbf{y}$ are choosen independently,

$$\begin{aligned} &= \sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)E_{\mathbf{x}}[\chi_S(\mathbf{x})\chi_U(\mathbf{x})]E_{\mathbf{y}}[\chi_T(\mathbf{y})\chi_U(\mathbf{y})] \\ &= \sum_{S,T,U} \hat{f}(S)\hat{f}(T)\hat{f}(U)\langle\chi_S, \chi_U\rangle\langle\chi_T, \chi_U\rangle \\ &= \sum_S \hat{f}(S)^3. \end{aligned}$$

Since $\epsilon > 0$ we must have $\max_S \hat{f}(S) \geq 0$. Using this for the first inequality;

$$\sum_S \hat{f}(S)^3 \leq \max_S \hat{f}(S) \cdot \sum_S \hat{f}(S)^2 = \max_S \hat{f}(S) = \max_S \langle f, \chi_S \rangle. \tag{21}$$

($\sum_S \hat{f}(S)^2 = 1$; see the remark following Parsevals identity.) Letting S maximize $\langle f, \chi_S \rangle$, we see that $\langle f, \chi_S \rangle \geq 2\epsilon$, implying that f is $(1/2+\epsilon)$-close to the linear function χ_S. □

Exponential-Sized PCP System for NP

We now prove the main result of this lecture.

Theorem 9. NP $\subseteq$ PCP$(\text{poly}(n), 1)$.

Proof. Describing a $(\text{poly}(n), \mathcal{O}(1))$-**PCP** verifier V for the **NP**-hard language QUADEQ will prove the theorem. Let an instance of QUADEQ with m equations and n variables be given by $x = \langle A_1, \ldots, A_m, \mathbf{b}\rangle$ (see (2)). The verifier V will intepret the proof $\pi \in \{0,1\}^{2^n + 2^{n^2}}$ for x as a thruth table for two functions $f\colon \{0,1\}^n \to \{0,1\}$ and $g\colon \{0,1\}^{n^2} \to \{0,1\}$. In a correct proof of x, the functions f and g will be the Walsh-Hadamard encodings $\text{WH}(\mathbf{u})$ and $\text{WH}(\mathbf{u}\mathbf{u}^T)$, and $\mathbf{u} \in \{0,1\}^n$ will satisfy (2). The verification of this is done in three steps.

Step 1: Verify that f and g are linear. That (the truth table for) f is a Walsh-Hadamard code is equivalent to f being linear (same for g). Using the linearity test following Theorem 6, we may with probability 0.9 reject any proof, where f and g are not 0.999-close to respectively

$$\begin{aligned} \tilde{f}(\mathbf{r}) &= \mathbf{u} \cdot \mathbf{r} \qquad (\mathbf{r} \in \{0,1\}^n), \qquad \text{and} \\ \tilde{g}(T) &= W \cdot T \quad \text{(dot product)} \qquad (T \text{ an } n \times n \text{ matrix}), \end{aligned} \tag{22}$$

for some $\mathbf{u} \in \{0,1\}^n$ and $n \times n$ matrix W (with entries in $\{0,1\}$). Notice that in a correct proof f and g will be linear and $\tilde{f} = f$ and $\tilde{g} = g$. We will need to calculate $\tilde{f}$ and $\tilde{g}$ for a constant number C of inputs. Using the random access to f and g, this can be done correctly with probability 0.9 by using the self correction of the Walsh-Hadamard code: To calculate $\tilde{f}(\mathbf{r})$ we pick $\mathbf{r}' \in \{0,1\}^n$ at random and ouput $f(\mathbf{r} + \mathbf{r}') + f(\mathbf{r}')$. With probability at least $1 - 2 \cdot 0.001 = 0.998$ this output is equal to $\tilde{f}(\mathbf{r})$. Repeating the procedure we may amplify the probability of success, so that all C calculations are correct with probability at least 0.9. In a correct proof the calculation of $\tilde{f}$ and $\tilde{g}$ will always be correct.

Step 2: Verify that $W = \mathbf{u}\mathbf{u}^T$. For $\mathbf{r}, \mathbf{s} \in \{0,1\}^n$ we have

$$\begin{aligned} \tilde{g}(\mathbf{r}\mathbf{s}^T) &= W \cdot (\mathbf{r}\mathbf{s}^T) = \mathbf{r}^T W \mathbf{s}, \qquad \text{and} \\ \tilde{f}(\mathbf{r}) f(\mathbf{s}) &= (\mathbf{u} \cdot \mathbf{r})(\mathbf{u} \cdot \mathbf{s}) = \mathbf{r}^T (\mathbf{u}\mathbf{u}^T) \mathbf{s}. \end{aligned} \tag{23}$$

In a correct proof the two lines will be equal for all $\mathbf{r}, \mathbf{s} \in \{0,1\}^n$. Assume now that $W \neq \mathbf{u}\mathbf{u}^T$. With probability at least a half $W\mathbf{s} \neq (\mathbf{u}\mathbf{u}^T)\mathbf{s}$, if we pick $\mathbf{s}$ uniformly at random. And if $W\mathbf{s} \neq (\mathbf{u}\mathbf{u}^T)\mathbf{s}$ for some $\mathbf{s}$, then with probability a half $\mathbf{r}^T W \mathbf{s} \neq \mathbf{r}^T (\mathbf{u}\mathbf{u}^T)\mathbf{s}$, if we pick $\mathbf{r}$ uniformly at random. So testing $\tilde{g}(\mathbf{r}\mathbf{s}^T) = \tilde{f}(\mathbf{r}) f(\mathbf{s})$ with $\mathbf{r}, \mathbf{s}$ picked uniformly at random will reject any proof where $W \neq \mathbf{u}\mathbf{u}^T$ with probability at least a fourth. Repating this test a constant number of times we may reject with probability at least 0.9.

Step 3: Verify that $\mathbf{u}$ satisfies our QUADEQ instance. We have m equations

$$\mathbf{u}^T A_k \mathbf{u} = b_k \qquad (k = 1, \ldots, m). \tag{24}$$

Pick $\mathbf{c} \in \{0,1\}^m$ uniformly at random. Let $A = \sum_{k=1}^m c_k A_k$ and $b = \mathbf{c} \cdot \mathbf{b}$. In a correct proof

$$\mathbf{u}^T A \mathbf{u} = b. \tag{25}$$

If (24) does not hold for some k, we will have $\mathbf{u}^T A \mathbf{u} \neq b$ with probability a half. Since $\mathbf{u}^T A \mathbf{u} = \tilde{g}(A)$ we may test whether (25) holds. Again, by repeating the test a constant number of times we may with probability at least 0.9 reject any proof where (24) does not hold for all k.

It should be clear that the verifier always accepts a correct proof. And if $x \notin$ QUADEQ, the verifier will accept any (necessarily incorrect) proof with probability at at most $4 \cdot 0.1 = 0.4$. The number of queries to π is constant: Altough we repeat tests/calculations, the number of repetitions is independent of the input to V. The verifiers usage of random bits is linear in the input size $|x|$. □