COM S 6810 Theory of Computing — April 23, 2009

Lecture 25: PCP 'Light' Theorem

Instructor: Rafael Pass — *Scribe: Shuang Zhao*

1 Recall from Last Lecture

Theorem 1 (PCP 'light' theorem)**.**

$$\mathsf{NP} \subseteq \mathsf{PCP}(\mathrm{poly}(n), O(1)).$$

This theorem can be proved by showing that the NP-complete problem QUADEQ has a $(\mathrm{poly}(n), O(1))$-PCP verifier.

Let $a_1, a_2, \ldots, a_n \in \{0,1\}$ be a satisfying assignment. The prover is supposed to write down

$$\Pi(\mathbf{v}) := \langle \mathbf{v}, \mathbf{a} \otimes \mathbf{a} \rangle$$

for all $\mathbf{v} \in \{0,1\}^{n^2}$ where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_i \mathbf{x}_i \mathbf{y}_i$.[1]

The verifier checks the proof in three steps:

1. **Linearity Test.** Check that Π is a linear function.
2. **Consistency Test.** Verify that Π encodes $\mathbf{u} \otimes \mathbf{u}$ for some $\mathbf{u} \in \{0,1\}^n$.
3. **Subset Sum Test.** Verify that $\mathbf{u}$ is a satisfying assignment.

We showed in the last lecture that if Π is at distance ϵ from linear, it holds that

$$\Pr_{\mathbf{x},\mathbf{y}}[\, \Pi(\mathbf{x}) + \Pi(\mathbf{y}) \neq \Pi(\mathbf{x} + \mathbf{y}) \,] \geq \epsilon.$$

For all $0 < \epsilon < 1/2$, we can obtain a linearity test rejecting with probability at least $1/2$ every function that is at distance $\geq \epsilon$ from linear (by repeating this test independently). We call such a test a *ϵ-linearity test*.

[1] If $\mathbf{x}, \mathbf{y}$ are two n-dimensional vectors, then $\mathbf{x} \otimes \mathbf{y}$ is defined by

$$\mathbf{x} \otimes \mathbf{y} := (\mathbf{x}_1\mathbf{y}_1, \mathbf{x}_1\mathbf{y}_2, \ldots, \mathbf{x}_1\mathbf{y}_n, \ldots, \mathbf{x}_n\mathbf{y}_1, \mathbf{x}_n\mathbf{y}_2, \ldots, \mathbf{x}_n\mathbf{y}_n).$$

2 Today's Lecture

First we prove the following fact which will be repeatedly used in this lecture:

Lemma 2. *Let* $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$*. If* $\mathbf{x} \neq \mathbf{0}$*, then* $\Pr_{\mathbf{y}}[\, \mathbf{x}^T \mathbf{y} \neq 0 \,] = 1/2$*.*

Proof. Assume without loss of generality that $x_1 = 1$. Then

$$\Pr_{\mathbf{y}}[\, \mathbf{x}^T \mathbf{y} \neq 0 \,] = \frac{1}{2} \Pr_{\mathbf{y}} \left[\sum_{i=2}^{n} x_i y_i = 0 \right] + \frac{1}{2} \Pr_{\mathbf{y}} \left[\sum_{i=2}^{n} x_i y_i \neq 0 \right] = \frac{1}{2}. \qquad \blacksquare$$

Linearity Test. Perform a 0.001-linearity test on $\Pi(\mathbf{v})$. We assume that in the next two steps, Π is at distance 0.001 from a (unique) linear function l. For querying $l(\mathbf{t})$, the verifier picks $\mathbf{r}$ at random and computes $\Pi(\mathbf{r}) + \Pi(\mathbf{r} + \mathbf{t})$. Since only a small number of queries will be used in those steps, according to union bound, it holds that with high probability (at least 0.9 in our proof) $\Pi(\mathbf{r}) + \Pi(\mathbf{r} + \mathbf{t}) = l(\mathbf{t})$ on all these queries.

Consistency Test. If l encodes $\mathbf{u} \otimes \mathbf{u}$, it holds that $\mathbf{u}^T \mathbf{u} = \mathbf{M}$ where

$$\mathbf{u} = (w_{11}, w_{22}, \ldots, w_{nn}) \text{ and } \mathbf{M} = \begin{pmatrix} w_{11} & w_{12} & \ldots & w_{1n} \\ w_{21} & w_{22} & \ldots & w_{2n} \\ & & \ldots & \\ w_{n1} & w_{n2} & \ldots & w_{nn} \end{pmatrix}.$$

Lemma 3. *If* $\mathbf{A}, \mathbf{B}$ *are* $n \times n$ *matrices over* $GF(2)$ *with* $\mathbf{A} \neq \mathbf{B}$*, then*

$$\Pr_{\mathbf{x},\mathbf{y} \in \{0,1\}^n} \left[\, \mathbf{x} A \mathbf{y}^T = \mathbf{x} B \mathbf{y}^T \,\right] \leq \frac{3}{4}.$$

Proof. Let $\mathbf{A}' = \mathbf{A} - \mathbf{B}$. According to Lemma 2, it holds that if $\mathbf{A}' \neq \mathbf{0}$,

$$\Pr_{\mathbf{y}}[\, \mathbf{A}' \mathbf{y}^T \neq \mathbf{0} \,] \geq 1/2 \text{ and } \Pr_{\mathbf{y}}[\, \mathbf{x} \mathbf{A}' \mathbf{y}^T \neq \mathbf{0} \mid \mathbf{A}' \mathbf{y}^T \neq \mathbf{0} \,] \geq 1/2.$$

Therefore, $\Pr_{\mathbf{y}}[\, \mathbf{x} \mathbf{A}' \mathbf{y}^T \neq \mathbf{0} \,] \geq 1/4$, namely $\Pr_{\mathbf{y}}[\, \mathbf{x} \mathbf{A} \mathbf{y}^T = \mathbf{x} \mathbf{B} \mathbf{y}^T \,] \leq 3/4$. $\blacksquare$

To check that $\mathbf{u}^T \mathbf{u} = \mathbf{M}$, we pick $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$ randomly. Then

$$\mathbf{x} \mathbf{M} \mathbf{y}^T = \sum_{i,j \in [n]} x_i y_j w_{ij} = \langle \mathbf{x} \otimes \mathbf{y}, \mathbf{w} \rangle = l(\mathbf{x} \otimes \mathbf{y})$$

and

$$\mathbf{x}(\mathbf{u}^T \mathbf{u}) \mathbf{y}^T = (\mathbf{x} \mathbf{u}^T)(\mathbf{u} \mathbf{y}^T) = \langle \mathbf{x}', \mathbf{w} \rangle \langle \mathbf{y}', \mathbf{w} \rangle = l(\mathbf{x}')\, l(\mathbf{y}')$$

where $\mathbf{x}', \mathbf{y}'$ can be derived from $\mathbf{x}, \mathbf{y}$. By Lemma 3, if $\mathbf{u}^T \mathbf{u} \neq \mathbf{M}$, the consistency test will catch it with probability at least 1/4.

Subset Sum Test. Assume that l encodes $\mathbf{u} \otimes \mathbf{u}$, namely $l(\mathbf{v}) = \langle \mathbf{v}, \mathbf{u} \otimes \mathbf{u} \rangle$. Next we need to check that $\mathbf{A}\mathbf{u}^{(2)} = \mathbf{b}$ where $\mathbf{A}$ is an $m \times n^2$ matrix and $\mathbf{u}^{(2)} = \mathbf{u} \otimes \mathbf{u}$.

Pick random subset $S \subseteq [m]$ and compute

$$f(S) = \hat{\mathbf{S}}^T(\mathbf{A}\mathbf{u}^{(2)} - \mathbf{b}) \;\; \text{where} \;\; \hat{S}_i = \begin{cases} 1 & i \in S \\ 0 & i \notin S \end{cases}.$$

By Lemma 2, $\Pr_S[\, f(S) \neq 0\,] = 1/2$ if $\mathbf{A}\mathbf{u}^{(2)} \neq \mathbf{b}$. And $f(S)$ can be computed by

$$f(S) = \hat{\mathbf{S}}^T(\mathbf{A}\mathbf{u}^{(2)} - \mathbf{b}) = l\big(\,\hat{\mathbf{S}}^T\mathbf{A}\,\big) - \hat{\mathbf{S}}^T\mathbf{b}.$$

Conclusion. The verifier always accepts a correct proof and accepts any incorrect proof with probability at most 0.8. This probability can be reduced to 0.5 by independently repeating this algorithm.