18.405J/6.841J: Advanced Complexity Theory Spring 2016

Lecture 16: Exponential Sized PCP

Prof. Dana Moshkovitz *Scribes: Haoran Xu*
Scribe Date: Spring 2015

Overview

In this lecture we will prove a weaker version of the PCP Theorem: $\mathsf{NP} \subseteq \mathsf{PCP}_{1,1-\delta}[\mathsf{poly}(n), O(1)]$ for some constant $\delta > 0$.

Quadratic Equation Problem

From now on, all arithmetic operations are done under $\mathbb{F}_2$.

In the Quadratic Equation Problem (QEP), we are to determine a given system of quadratic equations over variables $x_1, \cdots, x_n$

$$\begin{aligned} e_1(x_1, \cdots, x_n) &= c_1 \\ \vdots \quad &= \vdots \\ e_m(x_1, \cdots, x_n) &= c_m \end{aligned}$$

has a solution. A quadratic polynomial is a polynomial with degree at most 2. Since we have moved the constant term to the right side, from now on, all quadratic functions we are discussing have no constant terms.

It's clear that $\mathsf{QEP} \in \mathsf{NP}$. One can further show that QEP is NP-complete by reducing 3SAT to it: a clause $x_i \vee \neg x_j \vee x_k$ in 3SAT becomes an equation $x_i * (1 - x_j) * x_k = 0$. This is cubic, but we can make it quadratic by introducing in n^2 dummy variables $\{x_{ij}\}$ to represent the value of $x_i x_j$ for all i, j.

Probabilistic Checking of Proofs for QEP

We will prove the weak PCP Theorem by proving $\mathsf{QEP} \in \mathsf{PCP}[\mathsf{poly}(n), O(1)]$.

Define $\mathcal{F}$ to be the set of all quadratic functions $f : \{0,1\}^n \to \{0,1\}$. Any quadratic function p over n variables can be written in form of $\sum P_{ij} x_i x_j$, where P is a $n \times n$ matrix. Note that under $\mathbb{F}_2$, $x_i^2 = x_i$, so the diagonal entries of P represent linear term coefficients. Since any quadratic function over n variables solely depends on its n^2 coefficients, $\mathcal{F}$ contains 2^{n^2} elements.

The proof π is viewed as a function $\pi : \mathcal{F} \to \{0,1\}$. A proof π is valid if there exists some solution $\vec{x}$ of the given QEP instance, such that $\pi(f) = f(\vec{x})$ for all $f \in \mathcal{F}$. That is, the proof π encoded the value of all quadratic polynomials at point $\vec{x}$ where $\vec{x}$ is a solution to the QEP instance. Note that this encoding is very inefficient: its length is exponential with respect to n.

The PCP Verifier

The PCP verifier V will randomly pick one of the three following tests and execute it:

- Linearity Test: pick quadratic function p, q at random, check whether $\pi(p) + \pi(q) = \pi(p + q)$.
- Quadraticity Test: pick linear function l_1, l_2 at random, check whether $\widetilde{\pi}(l_1)\widetilde{\pi}(l_2) = \widetilde{\pi}(l_1 l_2)$.

- Equality Test: pick $r_1, \cdots, r_m \in_{\text{R}} \{0,1\}$, check whether $\widetilde{\pi}(\sum r_k e_k) = \sum r_k c_k$.

where $\widetilde{\pi}(p)$ is defined to be $\pi(p+q)+\pi(q)$, where q is a randomly picked quadratic function. The verfier accepts if the equality in the test holds, and rejects otherwise.

We will prove that V has completeness 1 and soundness $1-\delta$ for some constant $\delta > 0$, that is:

- $A \in \mathsf{QEP} \Leftrightarrow \exists \pi \;\; \Pr[V^{\pi}(A)=1] = 1$
- $A \notin \mathsf{QEP} \Leftrightarrow \forall \pi \;\; \Pr[V^{\pi}(A)=1] \leq 1-\delta$

The completeness part is very easy to check: when $\vec{x}$ is a solution to the QEP instance, it's easy to see that $\pi = \mathcal{F}(\vec{x})$ is linear, and will always pass quadraticity test and equality test.

For the soundness part, it's sufficient to prove that, if V accepts with probability at least $1-\delta$ for some small enough $\delta > 0$, then the QEP instance is satisfiable. Now suppose V accepts with probability at least $1-\delta$ where δ is sufficiently small. Then π passes every test with probability at least $1-3\delta$. We will prove the result by three lemmas.

Lemma 1. If π passes Linearity Test with probability at least $1-3\delta$, then

- π is $O(\delta)$-close to a unique linear function $\widehat{\pi}(p) = P \cdot \widehat{X}$, where $\widehat{X}$ is a $n \times n$ matrix.
- For any p, with probability at least $1-O(\delta)$, $\widetilde{\pi}(p) = \widehat{\pi}(p)$.

Proof. This follows directly from the BLR Test and the Random Self-Reduction Property discussed in last lecture:

Theorem 1. (Soundness of BLR Test) Suppose f is ϵ-far from a linear function, then

$$\Pr_{x,y \text{ u.r.}}[f(x+y) \neq f(x)+f(y)] \geq 2\epsilon/9$$

Theorem 2. (Random Self-Reduction Property) Suppose f is ϵ-far from a linear function where ϵ is sufficiently small, then exists unique linear function $\widehat{f}$ that is ϵ-close from f, and for any x

$$\Pr_{y \text{ u.r.}}[\widehat{f}(x) = f(x+y)+f(y)] \geq 1-2\epsilon$$

□

Lemma 2. If π passes Linearity Test and Quadraticity Test with probability $1-3\delta$, then $\widehat{\pi}(p) = p(x)$ for all p, where x is the column vector defined by $x_i = \widehat{X}_{ii}$.

Proof. It's sufficient to prove that $xx^T = \widehat{X}$, as if it is the case, then $\widehat{\pi}(p) = P \cdot \widehat{X} = \sum P_{ij}\widehat{X}_{ij} = \sum P_{ij}x_i x_j = p(x)$.

We can consider a linear function l as a column vector, in which the i^{th} entry is the coefficient for term x_i. Then

$$\begin{aligned} & \widehat{\pi}(l_1)\widehat{\pi}(l_2) - \widehat{\pi}(l_1 l_2) \\ = \;& (l_1^T x)(x^T l_2) - \sum \widehat{X}_{ij} l_{1i} l_{2j} \\ = \;& l_1^T (xx^T) l_2 - l_1^T \widehat{X} l_2 \\ = \;& l_1^T (xx^T - \widehat{X}) l_2 \end{aligned}$$

Using basic linear algebra knowledge, one can show that if $M = xx^T - \widehat{X} \neq 0$, then for random vector v, w, the probability that $v^T M w \neq 0$ is at least $1/2$. Since with probability $1 - O(\delta)$ both $\widetilde{\pi}(l_1) = \widehat{\pi}(l_1)$ and $\widetilde{\pi}(l_2) = \widehat{\pi}(l_2)$ happens, if $M \neq 0$, then with probability at least $1/2 - O(\delta)$, V will reject, contradicting the assumption that π fails the second test with probability at most 3δ. So $\widehat{X} = xx^T$, as desired. □

Lemma 3. If π passes all three tests with probability at least $1 - 3\delta$, then x is a solution to the QEP instance.

Proof. With probability $1 - O(\delta)$ we have $\widetilde{\pi}(\sum r_k e_k) = \widehat{\pi}(\sum r_k e_k)$, in that case,

$$\begin{aligned}
& \widetilde{\pi}(\sum r_k e_k) = \sum r_k c_k \\
\Rightarrow\ & \sum r_k (E_k \cdot xx^T) = \sum r_k c_k \\
\Rightarrow\ & \sum r_k e_k(x) = \sum r_k c_k \\
\Rightarrow\ & \vec{r} \cdot (\vec{e}(x) - \vec{c}) = 0
\end{aligned}$$

If $\vec{e}(x) \neq \vec{c}$, one can easily show that $\Pr_r[\vec{r} \cdot (\vec{e}(x) - \vec{c}) \neq 0] \geq 1/2$, then V will reject with probability at least $1/2 - O(\delta)$, contradiction. So $\vec{e}(x) = \vec{c}$, and x is a solution to the QEP instance. □

Some More Discussions

The key aspects used in the proof of the weak PCP theorem include locally testable decoding (the linearity test), local-decoding (local position contains global information on x), self-correction (the randomize self-reductibility), and local check of the original instance (the sumcheck used in equality test).

To further reduce the randomness usage to $O(\log n)$ and prove the PCP Theorem, one can encode x by evaluation of low degree polynomials (instead of only quadratic polynomials) defined by x. See Professor Moshkovitz's home page [1] for more information.

As discussed in previous lectures, PCP Theorem implies various results on hardness of approximation. The "Strong PCP Theorem", which stated that $\mathsf{NP} \subseteq \mathsf{PCP}_{1,\epsilon}[O(\log n), 2]_\Sigma$ (Σ is the alphabet, which size depends on $1/\epsilon$), is used to derive optimal inapproximation results.

Next lecture, we will explore the "Parellel Reptition Theorem", a theorem that converts PCP Theorem to Strong PCP Theorem.

References

[1] Professor Moshkovitz's homepage, http://people.csail.mit.edu/dmoshkov/

18.405J / 6.841J Advanced Complexity Theory
Spring 2016