U.C. Berkeley — CS278: Computational Complexity | Lecture 25
Professor Luca Trevisan | April 20, 2001
Scribe: Chris Harrelson | Last revised June 12, 2001

Lecture 25

Today we will show that $\mathbf{NP} \subseteq \mathbf{PCP}[O(n^2), 112]$, which will finish the proof of the PCP theorem: $\mathbf{NP} = \mathbf{PCP}[p(n), O(1)]$.

1 Picking an NP-complete problem for the reduction

Instead of using 3SAT, we will use a different NP-complete problem for which it is easier to formulate a **PCP** protocol. Here is the problem, called SimultaneousRoots:

> Given m degree-2 polynomials over n variables $x_1, \ldots, x_n$ in $\mathbb{Z}_2$, decide if there are $a_1, \ldots, a_n \in \{0,1\}$ such that
>
> $$\begin{aligned} p_1(a_1, \ldots, a_n) &= 0 \\ &\vdots \\ p_m(a_1, \ldots, a_n) &= 0 \end{aligned}$$
>
> where all operations are mod 2. In other words, find a set of a_i's that are a zero of all of the polynomials.

Claim: this problem is NP-complete.

2 The prover-verifier interaction

The proof provided by the prover has two parts, A and B. Part A has length 2^n and part B has length 2^{n^2}. Hence, one can think of A as a function $A : \{0,1\}^n \to \{0,1\}$ which is specified by listing its value for all of the 2^n different inputs. Similarly, one can think of B as a function $B : \{0,1\}^{n^2} \to \{0,1\}$.

The prover claims to the verifier that

$$A(x_1, \ldots, x_n) = \sum_i x_i a_i$$
$$B(x_{11}, \ldots, x_{nn}) = \sum_{i,j} x_{ij} a_i a_j$$

where $a_1, \ldots, a_n$ are a solution to the instance of SimultaneousRoots in question. This is equivalent to saying that

$$A = \{\vec{a} \cdot \vec{x}^T \ \forall \text{ vectors } \vec{x}\}$$
$$B = \{\vec{a} X \vec{a}^T \ \forall \text{ matrices } X\}$$

Here is the algorithm that the verifier will run to verify that this is in fact the case with good probability:

Repeat 7 times:

1. Pick random $\vec{r}, \vec{s} \in \{0,1\}^n$.
   Reject if $A(\vec{r}) + A(\vec{s}) \neq A(\vec{r} + \vec{s})$.
2. Pick random $\vec{r}, \vec{s} \in \{0,1\}^{n^2}4$.
   Reject if $B(\vec{r}) + B(\vec{s}) \neq B(\vec{r} + \vec{s})$.
3. Pick random $\vec{r}, \vec{s} \in \{0,1\}^n$.
   Reject if $\text{SelfCorrect}(A, r) \cdot \text{SelfCorrect}(A, s) \neq \text{SelfCorrect}(B, \ldots, r_i s_j, \ldots)$.
4. Pick random $\vec{r} \in \{0,1\}^n$. Define $p(x_1, \ldots, x_n)$ to be $\sum_i r_i p_i(x_1, \ldots, x_n)$.
   Let $p(x_1, \ldots, x_n)$ be written for convenience as $c_0 + \sum_i c_i x_i + \sum_{i,j} c_{ij} x_i x_j$.
5. Reject if $c_0 + \text{SelfCorrect}(A, c_1, \ldots, c_n) + \text{SelfCorrect}(B, c_{11}, \ldots, c_{nn}) \neq 0$.

Here we use an auxiliary procedure $\text{SelfCorrect}(A, r_1, \ldots, r_n)$ which picks random $y_1, \ldots, y_n$ and returns $A(\vec{y} + \vec{r}) - A(\vec{y})$.

Each iteration of the loop makes 16 bit queries to the proof: 3 for step 1, 3 for step 2, 6 for step 3, and 4 for step 5. Since there are 7 iterations, there will be a total of $16 \cdot 7 = 112$ bit queries, as required.

3 Proof that the verifier is not fooled

It remains to be proven that if there exists an $A : \{0,1\}^n \to \{0,1\}$ and a $B : \{0,1\}^{n^2} \to \{0,1\}$ such that the verifier accepts with probability > 0.5 on input $p_1, \ldots, p_m$, then $p_1, \ldots, \mathbf{P}_m$ is a YES instance of the SIMULTANEOUSROOTS problem.

Assume for the sake of contradiction that there exists such an A and B, and that this is not a YES instance of the SIMULTANEOUSROOTS problem.

If the verifier accepts after running the whole procedure with probability ≥ 0.5, then it accepts each round with probability at least $0.5^{1/7} > 0.9$. Hence we will assume that it accepts on one iteration with at least this probability in the following lemmas and claims.

CLAIM 1
There is an $\vec{a} \in \{0,1\}^n$ such that A has agreement of > 0.9 with the function $\tilde{A}(x_1, \ldots, x_n) = \sum_i a_i x_i$.

LEMMA 2
(Linearity test): Let $f : \{0,1\}^n \to \{0,1\}$. If $\mathbf{Pr}_{\vec{x},\vec{y}}[f(\vec{x}) + f(\vec{y}) = f(\vec{x} + \vec{y})] = \alpha$, then there is an $\vec{a}$ such that f has agreement at least α with the function $\tilde{f}(x) = \sum_i a_i x_i$.

This lemma was proved in a weaker version by Blum, Luby and Rubinfeld, which was in turn strengthened to this version by Bellare, Håstad, Kiwi and Sudan. Claim 1 follows easily from the lemma and the assumption that step 1 accepts with probability > 0.9.

CLAIM 3
There is a $\vec{b} \in \{0,1\}^{n^2}$ such that B has agreement > 0.9 with the function $\tilde{B}(x_{11}, \ldots, x_{nn}) = \sum_{i,j} b_{ij} x_{ij}$.

This follows from the same lemma and step 2's acceptance with probability > 0.9.

Claim 4
For every $\vec{r} \in \{0,1\}^n$, SelfCorrect$(A, r) = \tilde{A}(\vec{r})$ with probability at least 0.8, and the same is true for B.

Lemma 5
(Self-correction of linear functions): If $f : \{0,1\}^n \to \{0,1\}$ as agreement at least $1-\delta$ with a linear function $\tilde{f}$, then fore every $\vec{x} \in \{0,1\}^n$ the following experiment (i.e. SelfCorrect) gives $\tilde{f}(\vec{x})$ with probability at least $1-2\delta$: pick a random $\vec{y} in \{0,1\}^n$, and return $f(\vec{x}+\vec{y}) - f(\vec{y})$.

Proof: (of Lemma) The first call to f in $f(\vec{x}+\vec{y}) - f(\vec{y})$ is correct with probability at least $1-\delta$, and so is the second. Hence both are correct with probability at least $1-2\delta$. □

Setting $\delta = 0.9$ yields the claim.

Claim 6
If step 3 does not reject, then $b_{ij} = a_i a_j$ for every i, j.

Proof: (of Claim 6) Suppose not. Define $M_1 = (b_{ij})$ and $M_2 = (a_i \cdot a_j)$. Then $M_1 \neq M_2$.

Lemma 7
If $M_1 \neq M_2 \in \{0,1\}^{n^2}$, then by picking random $\vec{r}, \vec{s} \in \{0,1\}^n$, $\vec{r}M_1\vec{s}^T \neq \vec{r}M_2\vec{s}^T$ with probability at least $1/4$.

Proof: (of Lemma) For any $\vec{m_1}, \vec{m_2} \in \{0,1\}^n$ with $\vec{m_1} \neq \vec{m_2}$, $\mathbf{Pr}[\vec{r} \cdot \vec{m_1}^T \neq \vec{r} \cdot \vec{m_2}^T] = 1/2$. This is true because $\sum_i r_i (m_1)_i - \sum_i r_i (m_2)^i = \sum_{i:(m_1)_i \neq (m_2)_i} r_i$, which is 1 with probability 1/2.

This means that $\mathbf{Pr}[\vec{r}M_1 \neq \vec{r}M_2] \geq 1/2$, since M_1 and M_2 must differ in at least one row if they are different. We can now apply the argument above a second time, but this time with the vectors $(\vec{r}M_1) \cdot \vec{y}^T$ and $(\vec{r}M_2) \cdot \vec{y}^T$. Since this second test is independent of the first, their probabilities multiply, giving the desired result. □

Now, with probability at least $1/4$, the $\vec{r}, \vec{s}$ chosen in step 3 are such that $\sum_{i,j} r_i s_j a_i a_j \neq \sum_{i,j} r_i s_j b_i j$. For each such $\vec{r}, \vec{s}$, the test rejects with probability at least $1 - 3(1-0.8) = 0.4$ (all of the calls to SelfCorrect must fail, and there are three of them). Then in total, step 3 rejects with probability at least $1/4(0.4) = 0.1$. This is a contradiction with the assumption of the proof and the fact that if it accepts, it must do it with probability > 0.9. □

Claim 8
If $\vec{a}$ is not a zero of $p_1, \ldots, p_m$, then $\vec{a}$ is not a zero of p with probability at least $1/2$.

Proof: $p(a_1, \ldots, a_n) = \sum_i r_i p_i(a_1, \ldots, a_n)$, which is 0 or 1 with equal probability if at least one of the $p_i(a_1, \ldots, a_n)$ is not zero. □

Claim 9
If $p(a_1, \ldots, a_n) = 1$ then step 5 rejects with probability at least 0.64.

PROOF: Recall that $\tilde{A}(c_1, \ldots, c_n) = \sum_i a_i c_i$ and $\tilde{B}(c_{11}, \ldots, c_{nn}) = \sum_{ij} a_{ij} c_{ij}$. Then with probability at least 0.8^2 (two calls to SelfCorrect; see lemma 5), $c_0 + \sum_i a_i c_i + \sum_{ij} a_{ij} c_{ij} = 1$, since the left hand side of this equation is equal to $p(a_1, \ldots, a_n)$ from step 4, which is equal to 1 by assumption from step 4. $\square$

This means that steps 4 and 5 together fail with probability at $0.64 \cdot 1/2 = 0.32$, which is a contradiction with the assumption that the whole iteration rejects with probability < 0.1. This finishes the proof that this protocol is correct.