18.405J/6.841J Advanced Complexity Theory April 11, 2000

Lecture 18

Lecturer: Dan Spielman *Scribe: Wesley S. Chao*

1 Overview

Today we're going to examine three proofs:

$$\#P \subseteq IP(poly)$$

$$PSPACE \subseteq IP(poly)$$

$$IP(poly) \subseteq PSPACE$$

2 $\#P \subseteq IP(poly)$

It makes sense, first of all, that $P^{\#P} \subseteq IP$. Hence it remains only to prove that

$$\forall f \in \#P, L_f\{(w,c) : f(w) = c\} \subseteq LP$$

We will show that for some $\#P$-hard f, $L_f \subseteq IP$.

Consider Formula-Sum as our f, where the input is an arithmetic formula consisting only of + and * gates, and constants of Z mod p. The output consists of the sums $\Sigma_{x_1 \in \{0,1\}} \ldots \Sigma_{x_n \in \{0,1\}} f(x_1 \ldots x_n)$ mod p, where x_n are variables in the formula. Then $L_{Formula-Sum} \in LP$.

Theorem 1 *Formula-Sum is #P-hard.*

Proof We work from #3SAT. Recall that:
$a \wedge b \rightarrow a \cdot b$
$\neg a \rightarrow 1 - a$
$a \vee b \rightarrow 1 - (1-a)(1-b)$
Using these transformations, we get an arithmetic formula with the same values for $x_1 \ldots x_n \in \{0,1\}$. This formula outputs 1 when true and 0 when false.

To construct this formula, we use IP's, for which $\Sigma_{x_1 \in \{0,1\}} \ldots \Sigma_{x_n \in \{0,1\}} f(x_1 \ldots x_n) = c$ mod P, and we use the fact that for any $\alpha_1 \ldots \alpha_n \in Z$ mod P, we can evaluate $f(\alpha_1 \ldots \alpha_n)$ in polynomial time.

Now we use a sequence of reductions.

Definition 2 *An ϵ-reduction from a language L to a language L' is an IP-protocol that begins with an input w and has as output a verifier, V, that either outputs w' or rejects.*
If $w \in L$, $\exists P$ such that $w' \in L'$.
If $w \notin L$, $\forall P$, $Pr[w' \in L' | V$ does not reject$] < \epsilon$.

If V outputs w', then $w' \in L'$ with probability P.
If V rejects, then $w' \notin L'$ with probability $P - \epsilon$.

Theorem 3 *Say we have ϵ-reductions from $b_n \to b_{(n-1)} \dots b_1 \to b_0$, where $b_0 \in PTime$ and $\epsilon < \frac{1}{3n}$. Then we get an interactive proof for $w_n \in L_n$, by using reductions to produce $w_{n-1} \dots w_0$. V then rejects if $w_0 \notin L_0$. If $w_n \in L_n$, $\exists$ a prover such that V accepts. If $w_n \notin L_n$, $\forall$ provers P, $Pr[V accepts] < \frac{1}{3}$.*

Expanding our definition:

If $w_n \in L_n, \exists$ P $w_{n-1} \in L_{n-1} \dots w_0 \in L_0$ so that V will accept.

If $w_n \notin L_n$, but V does not reject, $w_0 \in L_0$, so $\exists$ a first j such that $w_j \notin L_j$ but $w_{j-1} \in L_{j-1}$, an event that occurs with probability $< \epsilon$. If we choose $\epsilon = \frac{1}{3n}$, the total probability is then equal to $\frac{1}{3}$.

For $L_m = \{(f,c) | f = \text{arithmetic formula of m variables such that } \Sigma_{x_1 \in \{0,1\}} \dots \Sigma_{x_m \in \{0,1\}} f(x_1 \dots x_m) = c \bmod P\}$, an $\epsilon - reduction$ from L_m to L_{m-1} goes as follows:

Let $g(x_m) = \Sigma_{x_1 \in \{0,1\}} \dots \Sigma_{x_{m-1} \in \{0,1\}} f(x_1 \dots x_m)$. Then $g(x_m)$ is a polynomial of degree $\leq size(f)$.

P: sends $q(x_m), a, b$, where q should be g.

V: if $q(0) \neq a$, $q(1) \neq b$, $a + b \neq c$, or $deg(q) > size(f)$, reject.

Choose $\alpha \in \frac{Z}{p}$ at random, which says

$$\Sigma_{x_1 \in \{0,1\}} \dots \Sigma_{x_{m-1} \in \{0,1\}} f(x_1 \dots x_{m-1}, \alpha) = q(\alpha)$$

since formulas only get smaller. Note that $f(x_1 \dots x_{m-1}, \alpha) = w$.

Claim 4 *This is a $\frac{size(f)}{p}$-reduction.*

Proof

Case 1: $w_m \in L_m$.

P sends g(m) = q(m).

g(0) + g(1) = c, so V won't reject.

$\forall \alpha, g(\alpha) = q(\alpha)$, which implies $w_{m-1} \in L_{m-1}$.

Case 2: $w_m \notin L_m$ if $\Sigma \neq c \longleftrightarrow g(0) + g(1) \neq c$.

If V does not reject, then q(0) + q(1) = c.

This implies that $q \neq g$ and $degree(g, q) \leq size(f)$, which in turn implies that $Pr_\alpha[g(\alpha) = q(\alpha)] \leq \frac{size(f)}{p}$.

$(w_{m-1} \in L_{m-1}) \longleftrightarrow (g(\alpha) = q(\alpha))$.

Choose $P > 2^n \cdot n \cdot size(f)$. ■

Theorem 5 *The two-for-one theorem*

Given a function $f(x_1 \dots x_n)$, such that when restricted to any one variable, f is a polynomial of degree $\leq d$, $\exists$ an $\epsilon - reduction$ from assertions like $f(x_1 \dots x_n) \cdot f(y_1 \dots y_n) = c$ to assertions like $f(\alpha_1 \dots \alpha_n) = \beta$.

Proof

Let l(t) $= t \cdot (\frac{1}{1} \dots \frac{1}{n}) + (1-t)(x_1 \dots x_n)$ and g(t) = f(l(t)).

Then g(0) $= f(x_1 \dots x_n)$ and g(1) $= f(\frac{1}{1} \dots \frac{1}{n})$.

The ϵ-reduction is therefore:

P: sends q(t) of degree $\leq$ d

V: rejects if $q(0) \cdot q(1) \neq c$, otherwise choose $\alpha \in \frac{Z}{p}$ at random and says $w' = f(l(\alpha)) = g(\alpha)$. ■

■