6.841/18.405J: Advanced Complexity Theory	March 13, 2002
Lecture 11	
Lecturer: Dan Spielman	*Scribe: M.T. Hajiaghayi*

In this lecture, we continue the proof of Toda's theorem, by proving some lemmas and theorems whose proofs were missed in the previous lecture. First we remind Toda's theorem.

Theorem 1 (Toda 1988) $PH \subseteq P^{\#P}$.

In the previous lecture, we introduced some interesting operators such as $\exists, \forall, BP$, and $\oplus$. Also, we introduced the steps of the proof. For example, we showed that $\sum_i^P \subseteq BP \cdot \oplus \cdot BP \cdot \oplus \cdots BP \cdot \oplus \cdot P$ (Step 1) and showed very briefly how we can simplify the sequence of operations (Steps 3 and 4). Today first we prove Steps 3 and 4 more precisely. Then we discuss amplifying $BP \cdot \oplus \cdot P$ (Step 2) and finally finish the proof by showing $BP \cdot \oplus \cdot P \subseteq P^{\#P}$ (Step 5).

Claim 2 *For any class C such as P that we can amplify $BP \cdot C$,*

$$\begin{aligned} \oplus \cdot \oplus \cdot C &= \oplus \cdot C \\ BP \cdot BP \cdot C &= BP \cdot C \\ \oplus \cdot BP \cdot C &\subseteq BP \cdot \oplus \cdot C. \end{aligned}$$

Proof

1) Let L be a language in C. Then $x \in \oplus_y \cdot \oplus_z \cdot L(x,y,z)$ means there is an odd number of y's for which there is an odd number of z's such that $(x,y,z) \in L$. It is equivalent to that there is an odd number of (y,z) pairs for which $(x,(y,z)) \in L$.

2) First we amplify class $BP \cdot C$. Let L be a language in C. Then $x \in BP_y \cdot BP_z \cdot L$ means for at least $c(n)$ fraction of y's, where $c(n) \geq s(n) + \frac{1}{poly(n)}$, for at least $1 - \frac{1}{exp(n)}$ fraction of z's, we have $(x,y,z) \in L$. Thus our new $c'(n) \geq (s(n) + \frac{1}{poly(n)})(1 - \frac{1}{exp(n)})$. On the other hand, for $x \notin L$ for at least $1 - s(n)$ fraction of y's, for at most $\frac{1}{exp(n)}$ fractions of z's we accept x. Thus for $s'(n) \leq s(n) + \frac{1}{exp(n)}$ fraction of (y,z) pairs, we accept x. Here we can observe that still $c'(n) \geq s'(n) + \frac{1}{poly'(n)}$.

3) Let L be a language in C. Then $x \in \oplus_y \cdot BP_z \cdot L$ iff there is a polynomial $p_1(n)$ and a language $L' = BP_z \cdot L \in BP \cdot C$ such that $(x,y) \in L'$ for an odd number of y's with length $p_1(|x|)$.

Now, we amplify the error probabilities of the BP operator such that the error is less than $2^{-2p_1(|x|)}$. Then there is a polynomial $p_2(n)$ such that

1. $(x,y) \in L' \rightarrow Pr_{|z|=p_2(|(x,y)|)}[(x,y,z) \in L] > 1 - 2^{-2p_1(|x|)}$
2. $(x,y) \notin L' \rightarrow Pr_{|z|=p_2(|(x,y|)}[(x,y,z) \in L] < 2^{-2p_1(|x|)}$

Using above facts, we observe

$$x \in \oplus_y \cdot BP_z \cdot L \Rightarrow Pr_z[(x,y,z) \in L] > 1 - 2^{-2p_1(|x|)} \text{ for an odd number of } y.$$

$$x \notin \oplus_y \cdot BP_z \cdot L \Rightarrow Pr_z[(x,y,z) \in L] > 1 - 2^{-2p_1(|x|)} \text{ for an even number of } y.$$

In other words for any y, $Pr_z[(x,y,z) \in L$ disagrees with $(x,y) \in L'] < 2^{-2p_1(|x|)}$.
Thus, $Pr_z[(x,y,z) \in L$ disagrees with $(x,y) \in L'$ for all $y] < 2^{-2p_1(|x|)} \cdot 2^{p_1(|x|)} = 2^{-p_1(|x|)}$.
Therefore,

$$x \in \oplus_y \cdot BP_z \cdot L \Rightarrow Pr_z[(x,y,z) \in L \text{ for an odd number of } y] > 1 - 2^{-p_1(|x|)}$$

and

$$x \notin \oplus_y \cdot BP_z \cdot L \Rightarrow Pr_z[(x,y,z) \in L \text{ for an odd number of } y] < 2^{-p_1(|x|)}$$

, as desired. ■

Now, we discuss Step 2 of Toda's proof. To this end, first we need to introduce some machinery, called *arithmetic on NTM*. Let N_1 and N_2 be two NTM's. Let $n_1(x)$ and $n_2(x)$ be the number of accept paths of N_1 and N_2 on an input x. We define two new NTM's $N_+(x, y)$ and $N_*(x, y)$ such that $n_+(x, y) = n_1(x) + n_2(y)$ and $n_*(x) = n_1(x) * n_2(y)$. We can define N_+ on input (x, y) as follows:

1. non-deterministically choose 1 or 2.
2. if 1 then run $N_1(x)$
3. if 2 then run $N_2(y)$

Machine N_* is defined as follows:

1. run $N_1(x)$
2. if **accept**
   (a) run $N_2(y)$
   (b) if **accept** then **accept** else **reject**.
3. else **reject**

Here $TIME(N_+(x, y)) = \max\{TIME(N_1(x)), TIME(N_2(y))\} + 1$ and $TIME(N_*(x, y)) = TIME(N_1(x)) + TIME(N_2(y))$. Now we can observe that using the constructions of N_+ and N_*, for any polynomial family $P_n(a)$ of degree $poly(n)$ with positive coefficients at most $2^{poly(n)}$, we can take any machine N that has $n(x)$ accept states and conform it to a machine $N_P(x)$ that has $P_{|x|}(n(x))$ accept states and has polynomial running time (we can construct the monomials X^i by N_* and the coefficients by N_+).

We can consider NTM's by circuits. Assume we have two circuits $C_1, C_2 (C_i(\cdot) = M_i(w_i, \cdot))$ taking n-bit inputs and accepting n_1 and n_2 inputs respectively. We can observe that circuit C_+ given by $C_+(x, y) = C_1(x) \wedge C_2(x)$ accepts $n_1 \cdot n_2$ inputs and circuit C_* given by $C_*(x, y, b) = (b \wedge C_1(x)) \vee (\bar{b} \wedge C_2(x))$ has $n_1 + n_2$ accepting inputs. In the rest of the lecture, we use the circuit model.

Lemma 3 *We can amplify $BP \cdot \oplus \cdot P$.*

Proof For simplicity, we assume the error is one-sided. Let $L \in BP_y \cdot \oplus_z \cdot P$.

- If $x \in L$ then for all y's, there is an odd number of z's for which $C(x, y, z) = 1$.
- If $x \notin L$ then for at most $1 - \frac{1}{poly(n)}$ fraction of y's there is an odd number of z's for which $C(x, y, z) = 1$.

Now for amplification, choose $y_1, y_2, \cdots, y_m$ at random where m is polynomial in n. Now we can observe that $\Pi_{i=1}^{m}(\#_{z_i} C(x, y_i, z_i) = 1)$ is odd iff $\forall i$, *the number of z_i's for which* $C(x, y_i, z_i) = 1$ is odd. Here we can construct such a polynomial using the concept of arithmetic on NTM introduced above. Here if $x \in L$ then the probability that for all y_i's, we get an odd number of z's is 1. On the other hand, if $x \notin L$ with probability at most $(1 - \frac{1}{poly(n)})^m$ we get an odd number of z's for all y_i's. Now if $m = n \cdot poly(n)$ then the probability is exponentially small in n.

Now we consider a slightly harder case. Again let $L \in BP_y \cdot \oplus_z \cdot P$ such that,

- If $x \in L$ then for at most $1 - \frac{1}{poly(n)}$ fraction of y's, there is an odd number of z's for which $C(x, y, z) = 1$.
- If $x \notin L$ then for every y, there is an even number of z's for which $C(x, y, z) = 1$.

The main idea here is that we complement parities, take product and complement the result. More precisely, we choose $y_1, y_2, \cdots, y_m$ at random where m is polynomial in n. Now we observe $1 + \Pi_{i=1}^{m}(1 + \#_{z_i} C(x, y_i, z_i) = 1)$ is odd iff $\forall i$, *the number of* z_i*'s for which* $C(x, y_i, z_i) = 1$ is even. We can observe that if $x \notin L$ then our error probability is zero and if $x \in L$ the error probability is at most $(1 - \frac{1}{poly(n)})^m$ which is exponentially small in n when $m = n\ poly(n)$.

Strictly speaking, in our above arguments, we need to consider the case where error is *almost one-sided* (e.g. accept with probability $1 - exp(-n)$ vs. $1 - 1/poly(n)$.) However almost nothing changes in the proof. ■

Finally, we prove Step 5 of Toda's proof.

Theorem 4 $BP \cdot \oplus \cdot P \subseteq P^{\#P}$.

Proof Let L be a language in $BP_y \cdot \oplus_z \cdot P$ where $y \in \{0,1\}^m$. First we introduce $P_n(a)$, a family of polynomials, whose degree is $poly(n)$ and whose coefficients are at most $2^{poly(n)}$ satisfying the following properties:

1. $P_n(a) = 0 \mod 2^{2^m}$ if $a = 0 \mod 2$.
2. $P_n(a) = -1 \mod 2^{2^m}$ if $a = 1 \mod 2$.

In fact, P_n can be constructed as follows. Let $h(x) = 3x^4 + 4x^3$. We can easily check that $x = 0 \mod 2^m \rightarrow h(x) = 0 \mod 2^{2m}$ and $x = -1 \mod 2^m \rightarrow h(x) = -1 \mod 2^{2m}$ (just plug in $x = 0$ and $x = -1 + a2^m$ in $h(x)$). Now, we define

$$h^1(x) = h(x)$$
$$h^c(x) = h^{c-1}(h(x))$$

and let $P_n(a) = h^{\lceil \log 2m \rceil}(a)$. We can check that $P_n(a)$ has all aforementioned properties and its degree is polynomial in m, which is also polynomial in n ($|y|$ is polynomial in n). We turn back to the statement of the theorem. Let $L = BP_y \cdot \oplus_z \cdot L'$. Using amplification mentioned in previous lemma, we know

1. if $x \in L$, then $Pr_y[|\{z : L'(x,y,z) = 1\}|\ is\ odd] > 3/4$; and
2. if $x \notin L$, then $Pr_y[|\{z : L(x,y,z) = 1\}|\ is\ odd] < 1/4$.

Thus to decide whether $x \in L$ or not, we only need to distinguish whether $Pr_y[|\{z : L(x,y,z) = 1\}|\ is\ odd]$ is more than $3/4$ or less than $1/4$.

To distinguish these two in $P^{\#P}$, we compute $\sum_y P_n(\sum_z \#C(y,z))$. Now for a fixed y, the value of $P_n(\sum_z \#C(y,z))$ is either 0 or $-1 \mod 2^{2^m}$. Because of the definition of P_n, we can count the number of y's for which the value is -1. Now we can check whether $Pr_y[|\{z : L(x,y,z) = 1\}|\ is\ odd]$ is more than $3/4$ or less than $1/4$ by only one query of $\#P$. Here the expression $P_n(a)$ is a one-variable polynomial, and its degree is polynomial in n. Therefore using the concept of arithmetic on NTM, $P_n(a)$ is computable in polynomial time. ■

The rest of the proof of Toda's theorem is just putting Steps 1–5 together and using a simple induction.