Lecture 10

Lecturer: Daniel A. Spielman *Scribe: Cyrus Dolph*

Complexity Class Operators

Toda's theorem relates to some new complexity classes about the hardness of counting. We need to define some operators before outlining the theorem.

Definition 1 *For a polynomial nondeterministic Turing Machine (NTM) M, the function $\# M$ is defined as follows: ($\#M : \Sigma^* \mapsto N$, where $\#M(w)$ is equal to the number of accepting computation paths of M on input w).*

Definition 2 *The $\#$ symbol can also be used as an operator on a complexity class: $\#P$ is equal to the set of functions $\{F : \Sigma^* \mapsto N \mid \exists a$ polynomial time NTM M such that $f(w) = \#M(w)\}$*

Definition 3 *We define $P^{\#P}$ as the set of languages $\{L \mid \exists f \in \#P$ such that $L \in P^f\}$.*

It's clear that $NP \subseteq P^{\#P}$ and also that $coNP \subseteq P^{\#P}$.

Definition 4 *The notion of $\#$ completeness suggests itself immediately. First, it is necessary to define the polynomial-time reducability operator ($\preceq_P$) for functions. We say $g \preceq_P f$ if there exist polynomial time computable functions a and b such that $g(w) = a(f(b(w)))$.*

Definition 5 *Now we are ready to define the property of $\#$ completeness. We say that a function f is $\#$ complete if $f \in \#P$ and $\forall g \in \#P$ $g \preceq_P f$.*

For example, the function $\{\#SAT =$ the number of satisfying assignments to a conjunctive normal formula$\}$ is $\# P$ complete.

Valiant has shown that the matching problem $\{\#MATCHING =$ the number of matchings of a graph[1]$\}$ is also #P complete. Interestingly, $MATCHING \in P$.

Definition 6 *For a complexity class C, we define $\Sigma \cdot C$ as the set of languages $\{L \mid \exists A \in C, f(n) = n^{O(1)}$ such that $w \in L \Leftrightarrow \exists x$, where $|x| = f(|w|)$, such that $(w, x) \in A\}$.*

For example, $\Sigma \cdot P = NP$.

Definition 7 *Likewise, we define $\Pi \cdot C$ as the set of languages $\{L \mid \exists A \in C, f(n) = n^{O(1)}$ such that $w \in L \Leftrightarrow \forall x$, where $|x| = f(|w|)$, such that $(w, x) \in A\}$.*

For example, $\Pi \cdot P = coNP$, $\Sigma \cdot \Pi \cdot P = \Sigma_2 P$.

Definition 8 *For a complexity class C, we define $BP \cdot C$ as the set of languages $\{L \mid \exists A \in C, f(n) = n^{O(1)}$ such that*

$$w \in L \Leftrightarrow \operatorname*{Prob}_{(w,x)\in A} [\ |x| = f(|w|)\ ] \geq \frac{2}{3}$$

$$w \notin L \Leftrightarrow \operatorname*{Prob}_{(x,x)\in A} [\ |x| = f(|w|)\ ] \leq \frac{1}{3}$$

[1] A matching on a graph is a set of pairs of nodes such that each node in the graph is paired with exactly one of its neighbors.

Definition 9 *The parity ($\oplus$) operator is defined in the following manner: A language $L \in \oplus \cdot C$ if $\exists A \in C, f(n) = n^{O(1)}$ such that*

$$w \in L \Leftrightarrow |\{x : |x| = f(|w|), (w, x) \in A\}| \text{ is odd}$$

Accordingly, we write that $L \in \overline{\oplus} \cdot C$ if $\exists A \in C, f(n) = n^{O(1)}$ such that

$$w \in L \Leftrightarrow |\{x : |x| = f(|w|), (w, x) \in A\}| \text{ is even}$$

The operators we have just defined can be chained together in many interesting ways. The complexity classes that can be generated by applying a constant number of these operators are known as the *quantified polynomial classes.*

1 Toda's Theorem

Theorem 10 $\Sigma_k P \subseteq P^{\#P}$

Sketch of Proof

The proof of Toda's theorem will span a couple of lectures. We will begin today by outlining the overall proof and getting to work on the first lemma.

Lemma 11 $\Sigma \cdot P \subseteq BP \cdot \oplus \cdot P$

Actually, we will prove a much stronger result, that

$$(\underbrace{\Sigma \cdot \Pi \cdot \Sigma \cdot \Pi \cdot ...}_{k \text{ times}}) \cdot P \subseteq (BP \cdot \oplus)^k \cdot P$$

Lemma 12 $\oplus \cdot BP \cdot C \subseteq BP \cdot \oplus \cdot C$

where C is any quantified polynomial complexity class. This proof of this lemma is a little tricky.

Lemma 13 $\oplus \cdot \oplus \cdot C = \oplus \cdot C$

The proofs of this and the following lemma are easy.

Lemma 14 $BP \cdot BP \cdot C = BP \cdot C$

Lemma 15 $BP \cdot \oplus \cdot P \subseteq P^{\#P}$

■

Proof of Lemma 1

This is a recap of the proof from last lecture.

We want to build a randomized poly-time reduction of a formula ϕ with the following properties: $\phi \mapsto \phi_1, ..., \phi_{n+1}$ such that

$$\begin{aligned} \phi \in SAT &\Rightarrow \Pr \exists \phi_i \text{ that has exactly one satisfying assignment} > \frac{1}{8} \\ \phi \notin SAT &\Rightarrow \forall i, \phi_i \notin SAT \end{aligned}$$

We construct the reduction by building a family of functions $H_{i,n} : \{0,1\}^n \mapsto \{0,1\}^i$. The reduction chooses at random an $h_i \in H_{i,n}$ where $1 \leq i \leq n+1$, and produces $\phi_1, ..., \phi_{n+1}$ so that

$$\phi_i(x) = true \Leftrightarrow (\phi(t) = true) \wedge (h_i(x) = 0)$$

Claim 16 *Consider the set* $S = \{x \mid \phi(x) = true\}$

If for $|S| > 1$, *we set* $2^{i-2} \leq |S| \leq 2^{i-1}$, *then*

$$\operatorname*{Prob}_{h_i} [\ |S \cap \{x \mid h_i(x) = 0\}| = 1\ ] \geq \frac{1}{8}$$

Proof *of claim:*

for $2^{i-2} \leq |S| \leq 2^{i-1}$, $\operatorname*{Prob}_{h_i} \left[\ \left|S \cap h_i^{-1}(0)\right| = 1\ \right] \geq \frac{1}{8}$

$$\operatorname*{Prob}_{h_i} [\ \exists x \in S \text{ such that } (h(s) = 0) \wedge (\forall y \in S, y \neq x,\ h(y) \neq 0)\ ]$$

because the events in question are disjoint, this probability is equal to:

$$= \sum_{x \in S} \operatorname*{Prob}_{h_i} [\ (h_i(x) = 0) \wedge (\forall y \in S, y \neq x,\ h_i(y) \neq 0)\ ]$$

$$\begin{aligned}
&= \sum_{x \in S} \operatorname*{Prob}_{h_i} [\ h_i(x) = 0\ ] \cdot \operatorname*{Prob}_{h_i} [\ \forall y \in S, y \neq x,\ h_i(y) \neq 0, \text{ given that } h_i(x) = 0\ ] \\
&= \sum_{x \in S} 2^{-i} \left(1 - \operatorname*{Prob}_{h_i} [\ \exists y \in S, y \neq x,\ h_i(y) = 0, \text{ given that } h_i(x) = 0\ ]\right) \\
&\geq \sum_{x \in S} 2^{-i} \left(1 - \sum_{y \in S, y \neq x} \operatorname*{Prob}_{h_i} [\ h_i(y) = 0, \text{ given that } h_i(x) = 0\ ]\right) \\
&\geq |S| \cdot 2^{-i} \cdot \left(1 - (|S| - 1) \cdot 2^{-i}\right) > \frac{1}{8}
\end{aligned}$$

■

Proof *of* $NP \subseteq BP \cdot \oplus \cdot P$: *By the definition of NP,*

$$L \in NP \Longrightarrow \exists A \in P, f(n) = n^{O(1)} \text{ such that } w \in L \Leftrightarrow \exists x, \text{where } x = n^{O(1)}, \text{ such that } (w, x) \in A$$

We construct the language $A' = \{(w, x, h) : (w, x) \in A, \text{and } h(x) = 0\}$ *where* h *contains bits describing a hash function. We have that*

$$\begin{aligned}
w \in L &\Rightarrow \operatorname*{Prob}_{h_1, \ldots, h_{n+1}} [\ \exists i \text{ such that } |\{x : (w, x, h_i) \in A'\}| \text{ is odd}\ ] > \frac{1}{8} \\
w \notin L &\Rightarrow \operatorname*{Prob}_{h_1, \ldots, h_{n+1}} [\ \exists i \text{ such that } |\{x : (w, x, h_i) \in A'\}| \text{ is odd}\ ] = 0
\end{aligned}$$

Now, we create the language A'' *such that*

$$(w, x, h) \in A'' \Leftrightarrow ((x = \overline{0}) \wedge (w, x, h) \notin A') \vee ((x \neq \overline{0}) \wedge (w, x, h) \in A')$$

A'' *has the opposite parity of* A'. *Note that the choice of* $\overline{0}$ *is arbitrary — any element in the range of* x *would suffice to bring about the desired parity flipping property. We have now that*

$$\begin{aligned}
w \in L &\Rightarrow \operatorname*{Prob}_{h_1, \ldots, h_{n+1}} [\ \exists i \text{ such that } |\{x : (w, x, h_i) \in A''\}| \text{ is even}\ ] > \frac{1}{8} \\
w \notin L &\Rightarrow \operatorname*{Prob}_{h_1, \ldots, h_{n+1}} [\ \exists i \text{ such that } |\{x : (w, x, h_i) \in A''\}| \text{ is even}\ ] = 0
\end{aligned}$$

Finally, we construct $B = \{(w, x_1, ..., x_m, h_1, ..., h_m) : (w, x_i, h_i) \in A''$ *for all* $i\}$
For a given $h_i, ..., h_{n+1}$,

$$|\{x_1, ..., x_{n+1} : (w, x_1, ..., x_{n+1}, h_1, ..., h_{n+1}) \in B\}| = \prod_{i=1}^{n+1} |\{x : (w, x, h_i) \in A''\}|$$

Therefore,

$$w \in L \quad \Rightarrow \quad \underset{h_1,\ldots,h_{n+1}}{\text{Prob}} [\ |\{x_1, ..., x_{n+1} : (w, x_1, ..., x_{n+1}, h_1, ..., h_{n+1}) \in B\}| \ \textit{is even}\ ] > \frac{1}{8}$$
$$w \notin L \quad \Rightarrow \quad \underset{h_1,\ldots,h_{n+1}}{\text{Prob}} [\ |\{x_1, ..., x_{n+1} : (w, x_1, ..., x_{n+1}, h_1, ..., h_{n+1}) \in B\}| \ \textit{is even}\ ] = 0$$

To be continued. . .
■

■