PRINCETON UNIVERSITY COS 522: COMPUTATIONAL COMPLEXITY

Lecture 8: Toda's Theorem

Lecturer: *Sanjeev Arora* Scribe:*Arora/Khot*

Toda's Theorem, $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathrm{SAT}}$, came as a big surprise in 1989, since researchers believed that alternation (the feature of the polynomial hierarchy) could not have anything do with the ability of count the number of solutions (a feature of $\#P$).

In this lecture we will use a (yet another) characterization of the class **PH** uniform circuit families, which is left as an exercise.

DEFINITION 1 *Let $\{\mathcal{C}_n\}_{n\geq 1}$ be a circuit family of size $S(n) \geq n$ for input of length n. We say that this is a Direct Connect uniform (DC uniform) family if all the following functions can be computed in deterministic $O(poly(n)log(S(n)))$ time :*

- *$TYPE(n,i)$ = the type (AND, OR, NOT, INPUT, OUTPUT) of gate i in circuit $\mathcal{C}_n$.*
- *$IN(n,i,j) = k$ where k is j^{th} in the ordered list of indices to the gates that feed into gate i, $k = NONE$ if there is no j^{th} gate.*
- *$OUT(n,i,j) = k$ where k is j^{th} in the ordered list of indices to the gates that gate i feeds into, $k = NONE$ if there is no j^{th} gate.*

THEOREM 1
$L \in PH$ iff L can be computed by a DC uniform circuit family $\{\mathcal{C}_n\}$ that

- *uses AND, OR, NOT gates.*
- *has size $2^{n^{O(1)}}$ and constant depth.*
- *gates can have unbounded (exponential) fanin.*
- *the NOT gates appear only at the input level.*

Note that the circuits have exponential size, but they have a succinct representation in terms of a TM which can systematically generate any required portion of the circuit.

We now define a class $\oplus P$ which we use as an intermediate class in the proof of Toda's Theorem.

DEFINITION 2 *A language $L \in \oplus\mathbf{P}$ iff there exists a polynomial time NTM M such that $x \in L$ iff the number of accepting paths of M on input x is odd.*

DEFINITION 3 $\oplus SAT = \{\varphi :$ *boolean formula φ has an odd number of satisfying assignments*$\}$.

A simple modification of the Cook-Levin theorem shows that $\oplus$SAT is complete for $\oplus\mathbf{P}$. The next Theorem is analogous to Theorem 1.

THEOREM 2
$L \in \oplus\mathbf{P}$ iff L can be computed by a DC uniform circuit family $\{\mathcal{D}_n\}$ that

- *uses AND, OR, NOT, XOR gates.*
- *has size $2^{n^{O(1)}}$ and constant depth.*
- *XOR gates can have unbounded (exponential) fanin, but the AND, OR gates have fanin at most $n^{O(1)}$.*
- *NOT gates can appear anywhere in the circuit.*

Now define a randomized reduction between two languages.

DEFINITION 4 *Language A reduces to language B under a randomized polynomial time reduction, denoted $A \leq_r B$, if there exists a deterministic, polynomial time computable function $f : \{0,1\}^* \to \{0,1\}^*$ and a polynomial $p()$ such that*

$$\forall x \in A \qquad \mathbf{Pr}_{y \in \{0,1\}^{p(|x|)}}[f(x,y) \in B] \geq 2/3 \tag{1}$$

$$\forall x \notin A \qquad \mathbf{Pr}_{y \in \{0,1\}^{p(|x|)}}[f(x,y) \in B] \leq 1/3 \tag{2}$$

We prove Toda's Theorem in two steps. First we show that any $L \in \mathbf{PH}$ can be randomly reduced to $\oplus$SAT and then we show that this reduction can be transformed into a (deterministic) reduction to a $\#\mathbf{P}$ problem.

1 Random reduction from PH to $\oplus$SAT

In this section we prove our main lemma that every language in polynomial hierarchy is randomly reducible to $\oplus$SAT.

LEMMA 3
$\forall L \in PH, \quad L \leq_r \oplus SAT.$

We will need the Valiant-Vazirani lemma.

DEFINITION 5 *If $a_1, \ldots, a_k \in GF(2)^N$, then*

$$(a_1, \ldots, a_k)^{\perp} = \left\{ s \in GF(2)^N : \quad s \cdot a_1 = s \cdot a_2 = \ldots = s \cdot a_k = 0 \right\}.$$

Imagine that each vector in $GF(2)^N$ represents an individual, and $S \subseteq GF(2)^N$ is a hobby club. The Valiant Vazirani lemma considers a simple way of picking representatives from S: pick $i \in [0, N]$ randomly and then $a_1, a_2, \ldots, a_i \in GF(2)^N$ randomly and choose the individuals in $S \cap (a_1, \ldots, a_i)^{\perp}$ as the representatives. The lemma shows that this simple method has a probability at least $1/4N$ of yielding a unique representative for the club. The beauty of course is that we not need to know what S is. The proof of the Lemma is left as an exercise. (Note: Below, we only need (3) with the "1"replaced with "is an odd number," which seems a weaker fact but seems no easier to prove.)

LEMMA 4 (VALIANT-VAZIRANI)
If $S \subseteq GF(2)^N$ is nonempty and $i \in \{0, 1, \ldots, N\}$ and $a_1, \ldots, a_i \in GF(2)^N$ are chosen uniformly at random then

$$\mathbf{Pr}[\left| S \cap (a_1, \ldots, a_i)^{\perp} \right| = 1] \geq \frac{1}{4N}. \tag{3}$$

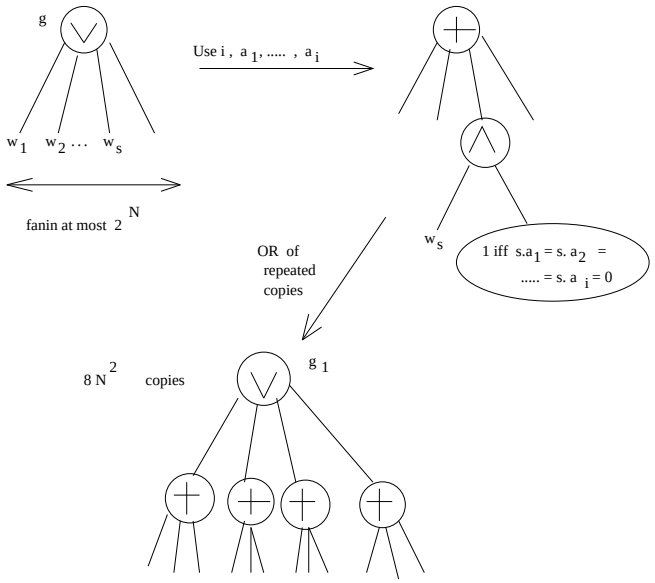

Figure 1: Probabilistic conversion of OR gate to $\oplus$ gate

Now we prove Lemma 3.

PROOF:(Lemma 3) Theorem 1 gives a characterization of L in terms of DC uniform circuit family $\{\mathcal{C}_n\}$. We use a randomized reduction to transform $\{\mathcal{C}_n\}$ into another DC uniform family $\{\mathcal{D}_n\}$ which uses $\oplus$ gates with exponential fanin and AND, OR gates with fanin $n^{O(1)}$. Theorem 2 then shows that the language computed by $\{\mathcal{D}_n\}$ can be expressed as a $\oplus$SAT problem (since $\oplus$SAT is complete for $\oplus\mathbf{P}$).

The reduction will use the Valiant-Vazirani lemma, and the deep fact that 1 is an odd number and 0 is even. Let the size of circuit $\mathcal{C}_n$ be 2^N where $N = n^{O(1)}$. Consider conversion of an OR gate g into XOR gate (Figure 1). The inputs $w_1, w_2, \ldots$ to the gate g can be indexed by strings in $GF(2)^N$. We choose i randomly from $\{0, 1, \ldots, N\}$ and strings $a_1, \ldots, a_i$ randomly from $GF(2)^N$. Then we replace the gate g by an $\oplus$ gate with the same number of inputs, but the input w_s is replced by logical AND of w_s and a predicate p_s which is 1 iff $s \cdot a_1 = \ldots = s \cdot a_i = 0$. (This predicate is computable by a poly(n) size circuit.) We note that if output of gate g is 0, so is output of the $\oplus$ gate. If the output of gate g is 1, there is a nonempty set S of strings s such that $w_s = 1$. With probability $\geq 1/4N$ (over the choice of $i, a_1, \ldots, a_i$, the number of strings $s \in S$ such that $s \in (a_1, \ldots, a_i)^{\perp}$ is odd and the output of $\oplus$ gate is 1. Thus the $\oplus$ gate is equivalent to gate g with probability at least $1/4N$. We can amplify this probability by taking OR of $8N^2$ independent copies of this $\oplus$ gate. The resulting circuit g_1 satisfies,

$$\mathbf{Pr}[g_1(w_1, w_2 \ldots.) \neq g(w_1, w_2, \ldots)] \leq (1 - 1/4N)^{8N^2} \leq e^{-2N}. \tag{4}$$

We apply this transformation to every gate in circuit $\mathcal{C}_n$. (The AND gates are first transformed into OR's using De-Morgan's law.) We use the same random choice of $i, a_1, \ldots, a_i$ for every gate, thus using only $n^{O(1)}$ random bits total. The new circuit $\mathcal{D}_n$ depends on the choice of the random bits. There are only 2^n different inputs for the circuit, and each imposes a set of values $(w_1, w_2, \ldots,$ in the above description) on every gate. Since each gate

transformation fails with probability at most e^{-2N}, we conclude that the old circuit agrees with $\mathcal{C}_n$ on all inputs of lengh n with probability $\geq 1 - 2^n 2^N e^{-2N} \geq 2/3$. It is clear that $\{\mathcal{D}\}_n$ is a DC uniform family satisfying conditions of Theorem 2. As observed before, we can construct a $\oplus$SAT question that decides whether an input is accepted by circuit $\mathcal{D}_n$. □

2 Proof of Toda's Theorem

For $L \in PH$, Lemma 3 gives a reduction $x \to \phi_r$ from input x to a SAT formula ϕ_r using a random string r of length m such that

$$x \in L \Longrightarrow \mathbf{Pr}_r[\phi_r \in \oplus\text{SAT}] \geq 2/3$$

$$x \notin L \Longrightarrow \mathbf{Pr}_r[\phi_r \in \oplus\text{SAT}] \leq 1/3$$

We will construct a $\#\mathbf{P}$ question that counts the number of random strings r such that $\phi_r \in \oplus$SAT. Using a $\#\mathbf{P}$-oracle, we then know the probability $\mathbf{Pr}_r[\phi_r \in \oplus\text{SAT}]$ and we can decide whether $x \in L$, proving Toda's theorem.

We define a transformation of ϕ_r to another SAT formula ϕ_r^* such that

$$\phi_r \in \oplus\text{SAT} \Longrightarrow \#(\phi_r^*) \equiv -1 (mod\ 2^{m+1})$$

$$\phi_r \notin \oplus\text{SAT} \Longrightarrow \#(\phi_r^*) \equiv 0\ (mod\ 2^{m+1}).$$

Here $\#(\psi)$ is the number of satisfying assignments to formula ψ.

Now we construct a NP machine that guesses a random string r, computes ϕ_r and ϕ_r^*, branches out according to an assignment for ϕ_r^* and then checks whether this assignment satisfies ϕ_r^*. Clearly,

$$\begin{aligned} \#accepting\ paths &= \sum_r \#(\phi_r^*) && (5) \\ &\equiv -|\{r|\phi_r \in \oplus\text{SAT}\}|\ (mod\ 2^{m+1}) && (6) \end{aligned}$$

Since there are only 2^m random strings r, the number of accepting paths reduced modulo 2^{m+1} gives the number of random strings r such that $\phi_r \in \oplus$SAT. By definition of $\#\mathbf{P}$, a $\#\mathbf{P}$-oracle can tell the number of accepting paths of this NTM on given input and the proof is complete.

We now give the transformation $\phi \to \phi^*$. For formulas $\varphi(x_1, \ldots, x_n)$ and $\psi(y_1, \ldots, y_m)$, let $\varphi + \psi$ and $\varphi \cdot \psi$ be formulas such that

$$\#(\varphi + \psi) = \#(\varphi) + \#(\psi)$$

$$\#(\varphi \cdot \psi) = \#(\varphi) \cdot \#(\psi)$$

Such formulas can be constructed easily with only constant factor increase in size. One can easily check that

$$\#(\psi) \equiv -1 (mod\ 2^{2^i}) \Longrightarrow \#(4\psi^3 + 3\psi^4) \equiv -1 (mod\ 2^{2^{i+1}})\ and \quad (7)$$

$$\#(\psi) \equiv 0\ (mod\ 2^{2^i}) \Longrightarrow \#(4\psi^3 + 3\psi^4) \equiv 0\ (mod\ 2^{2^{i+1}}). \quad (8)$$

Let $\phi_0 = \phi$ and $\phi_{i+1} = 4\phi_i^3 + 3\phi_i^4$. Let

$$\phi^* = \phi_{\lceil \log(m+1) \rceil}$$

Repeated use of equations 7, 8 shows that if $\#(\phi)$ is odd, $\#(\phi^*) \equiv -1 \ (mod\ 2^{m+1})$ and if $\#(\phi)$ is even, $\#(\phi^*) \equiv 0 \ (mod\ 2^{m+1})$. Also, size of ϕ^* is only polynomially larger than size of ϕ.

3 Open Problems

- What is the exact power of $\oplus$SAT and $\#SAT$?
- What is the complexity of computing approximation to permanent?
- What is the average case complexity of $n \times n$ permanent modulo small prime, say 3 or 5 ? Note that for a prime $p > n$, random self reducibility of permanent implies that if permanent is hard to compute on at least one input then it is hard to compute on $1 - O(p/n)$ fraction of inputs, i.e. hard to compute on average [**?**].

Exercises

§1 Prove Theorems 1 and 2.

§2 Prove the Valiant-Vazirani Lemma.

§3 Describe the constructions of the formulae $\varphi + \psi$ and $\varphi \cdot \psi$ as used in Toda's construction. (Be careful; φ and ψ could have different number of variables.)

§4 Let $f, g : \{0,1\}^* \to \mathbf{N}$ be functions and $c > 1$. We say that f *approximates* g *within a factor* c if for every string x, $g(x) \leq f(x) \leq c \cdot g(x)$. Show that for every $g \in \#\mathbf{P}$ and every $\epsilon > 0$, there is a function in $FP^{\mathbf{\Sigma}_3^p}$ that approximates g within a factor $1 + \epsilon$. (Hint: Use hashing and ideas similar to those in the proof of $\mathbf{BPP} \subseteq \mathbf{PH}$.)