6.841: Advanced Complexity Theory Fall 2012

Lecture 23 — December 4, 2012

Prof. Dana Moshkovitz *Scribe: Ilya Razenshteyn*

1 Overview

In the last lecture we covered Valiant–Vazirani reduction and investigated the complexity of approximate counting.

In this lecture we prove Toda's Theorem: $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

2 Toda's Theorem Statement

One can easily see from the definition of #P that $\mathrm{NP}, \mathrm{coNP} \subseteq \mathrm{P}^{\#\mathrm{P}}$. The question that is naturally to ask is: can we reduce a larger complexity class to #P? In [Tod91] Seinosuke Toda proved the following theorem.

Theorem 1. *It is true that* $\mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$. *Moreover, the reduction queries an oracle from* #P *(say,* #SAT*) only once.*

3 Randomized Reduction

Let us recall the definition of $\oplus$SAT.

Definition 2. *For every Boolean formula* φ *on* n *variables we say that* $\bigoplus_{x \in \{0,1\}^n} \varphi(x)$ *is true iff* $\varphi(x)$ *has an odd number of satisfying assignments. To put it another way,*

$$\bigoplus_{x \in \{0,1\}^n} \varphi(x) \equiv \sum_{x \in \{0,1\}^n} \varphi(x) \pmod 2.$$

The language $\oplus$SAT *consists of all the true formulae of the form* $\bigoplus_{x \in \{0,1\}^n} \varphi(x)$.

In this section we show how to reduce PH to $\oplus$SAT via a randomized reduction. In the next section we present an ingenious idea of Toda that allows us to derandomize the reduction at a cost of switching from $\oplus$SAT to #SAT.

So, our goal in this section is the following theorem.

Theorem 3. *For every* $c \in \mathbb{N}$ *there exists a randomized algorithm that takes a quantified Boolean formula* $\varphi(x)$ *with* n *variables (*x *stands for the set of free variables), and a parameter* m *and outputs a formula* $\bigoplus_y \psi(x, y)$ *such that for every* x

$$\mathbf{Pr}[\varphi(x) = \bigoplus_y \psi(x, y)] \geq 1 - 2^{-m}.$$

The running time of the reduction is $(nm)^{O_c(1)}$.

To prove this theorem we first need to establish some properties of $\bigoplus$-formulae.

3.1 Properties of Parity-Quantified Formulae

Let $\varphi, \psi\colon \{0,1\}^n \to \{0,1\}$ be any Boolean functions. Let us denote $\#(\varphi)$ the number of satisfying assignments of φ. Then, one can easily build formulae $\varphi + \psi$ and $\varphi \cdot \psi$ with $O(n)$ variables such that

- $\#(\varphi + \psi) = \#(\varphi) + \#(\psi)$;
- $\#(\varphi \cdot \psi) = \#(\varphi) \cdot \#(\psi)$.

Using this "arithmetic operations" one can easily show that if $\bigoplus_x \varphi(x)$ and $\bigoplus_y \psi(y)$ are parity-quantified formulae with disjoint sets of variables, then their conjunction, disjunction and negation can be represented as parity-quantified formulae with only a constant blowup in size. This implies, for example, that $\oplus$P is closed under the complement.

3.2 Proof of Theorem 3

W.l.o.g. we can assume that $\varphi(x) = \exists x_1\ \psi(x_1, x)$, where ψ is a quantified formula with $c-1$ levels of alternation (note that x_1 is a set of variables, not a single variable), since $\oplus$SAT is closed under taking negations.

Now we invoke the induction hypothesis and get a formula $\bigoplus_y \tau(x_1, x, y)$ such that for every x_1, x we have

$$\mathbf{Pr}[\bigoplus_y \tau(x_1, x, y) = \psi(x_1, x)] \geq 1 - 2^{-(m+n+10)}.$$

Now by union bound we have that with probability at least $1 - 2^{-(m+10)}$ we have $\bigoplus_y \tau(x_1, x, y) = \psi(x_1, x)$ *for every* x, x_1. In this case we have $\varphi(x) = \exists x_1\ \bigoplus_y \tau(x_1, x, y)$, and it is only left to remove the outer quantifier. For this we use Valiant–Vazirani reduction. Let us first recall it in somewhat "abstract" setting.

Theorem 4. *There is a polynomial-time randomized algorithm that given 1^n produces a Boolean formula $\alpha(x, y)$, where x is a vector of n variables, such that for any function $\beta\colon \{0,1\}^n \to \{0,1\}$ we have*

- *If $\exists x\ \beta(x)$, then*
$$\mathbf{Pr}[\bigoplus_{x,y}(\alpha(x, y) \wedge \beta(x))] \geq \frac{1}{8n};$$
- *If $\neg\exists x\ \beta(x)$, then*
$$\mathbf{Pr}[\bigoplus_{x,y}(\alpha(x, y) \wedge \beta(x))] = 0;$$

We invoke this Theorem N times (we will determine the exact value of N later) and get N formulae $\alpha_1(x_1, z), \alpha_2(x_1, z), \ldots, \alpha_N(x_1, z)$. We build the final formula as follows:

$$\bigvee_{i=1}^{N} \bigoplus_{x_1, z} (\alpha_i(x_1, z) \wedge \bigoplus_{y} \tau(x_1, x, y)). \tag{1}$$

Let us condition of the event that $\bigoplus_y \tau(x_1, x, y) = \psi(x_1, x)$ for every x_1, x. Then we see that with probability at least $(1 - 1/8n)^N$ (1) is equal to $\varphi(x)$. So, if we choose $N = O(nm)$ we can make this probability at least $1 - 2^{-(m+10)}$. Thus, the total probability of failure is at most $2^{-(m+9)} \ll 2^{-m}$.

It is left to observe that we can (and should!) transform (1) to a $\oplus$SAT instance using tricks from Section 3.1.

4 Derandomization

In this section we show how to derandomize Theorem 3 at a cost of switching from $\oplus$SAT to #SAT.

We can think about the reduction from the proof of Theorem 3 as a deterministic one that takes a string of random coins of size R. So, we have a polynomial-time deterministic reduction $f(\varphi(x), r)$ such that

- If $\varphi(x)$, then for at least 0.99 fraction of r's $f(\varphi(x), r) \in \oplus$SAT;
- If $\neg\varphi(x)$, then for at least 0.99 fraction of r's $f(\varphi(x), r) \notin \oplus$SAT.

We want to use a counting oracle to distinguish these two cases. For this we need the following gap-amplification Lemma.

Lemma 5. *There exists a polynomial-time deterministic reduction that given 1^l and a $\oplus$SAT-formula ψ produces a Boolean formula γ such that*

- *If $\psi \in \oplus$SAT, then $\#(\gamma) \equiv -1 \pmod{2^l}$;*
- *If $\psi \notin \oplus$SAT, then $\#(\gamma) \equiv 0 \pmod{2^l}$.*

Let us first show how to finish the proof of Toda's theorem assuming the Lemma. If we denote the reduction in the Lemma by T, then we can consider the following formula:

$$\sum_r T(f(\varphi, r)).$$

If we choose $l > R + 10$, then for $\varphi \in \oplus$SAT and $\varphi \notin$ SAT the ranges of possible values of this formula are disjoint. So, we can compute this sum using an oracle from #P (since T and f are polynomial-time deterministic reductions), and, thus, decide φ.

So, it is left to prove the Lemma. For $l = 1$ there is nothing to prove: we can take the reduction to be the identity. By the inductive hypothesis suppose that $\#(\gamma') \equiv 0$ or $-1 \pmod{2^t}$. We will show

how to switch from 2^t to 2^{2t}. Namely, consider the formula $\gamma = 4\gamma'^3 + 3\gamma'^4$ (here by arithmetic operations we mean the tricks from Section 3.1). It turns out that it gives exactly what we need! If $\#(\gamma') \equiv 0 \pmod{2^t}$, then $\#(\gamma) \equiv 0 \pmod{2^{2t}}$, but if $\#(\gamma') \equiv -1 \pmod{2^t}$, then $\#(\gamma) \equiv -1 \pmod{2^{2t}}$. We repeat this process $O(\log l)$ times, and get the desired formula. It is left to observe that on each step the blow up in size is at most constant, so in total we have polynomial running time.

References

[Tod91] Seinosuke Toda. PP is as Hard as the Polynomial-Time Hierarchy. *SIAM J. Comput.*, 20(5):865–877, 1991.