Toda's Theorem

Adrian She

June 2021

Abstract

The relationship between counting problems (#**P** problems) and other problems was not known until the discovery of Toda's theorem, for which Toda received the 1998 Gödel Prize. The theorem states that every problem in the polynomial hierarchy can be solved by a polynomial time algorithm with a #**P** oracle. We will sketch the proof of the theorem and outline an application of it to the study of quantum supremacy conjectures.

1 Counting Problems

A counting problem is the problem of computing a function $f : \{0,1\}^* \to \mathbb{N}$ given some input to f. A large number of counting problems belong to the class #**P** .

Definition 1. A function $f : \{0,1\}^* \to \mathbb{N}$ is a function in #**P** if there is a polynomial time computable predicate $M(x, y)$ and a polynomial $p(x)$ with

$$f(x) = |y \in \{0,1\}^{p(|x|)} : M(x, y) = 1|.$$

In other words, the function f counts the number of accepting paths of a non-deterministic polynomial time Turing machine, or equivalently the number of certificates that a polynomial time verifier accepts for a given input x.

A function f is #**P**-hard if every function in #**P** can be computed with a polynomial time algorithm with oracle access to f. Furthermore, a function is #**P**-complete if it is in #**P** and also #**P**-hard.

Examples of #**P**-complete functions include:

- $\#SAT$: Given a propositional Boolean formula $\phi(x_1, \ldots, x_n)$, determine the number of satisfying assignments it has. It is also straightforward to define counting analogues of other **NP**-complete problems such as Hamiltonian cycle, graph colouring etc.
- If M is an $n \times n$ matrix, define its permanent to be

$$\text{Perm}(M) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} M_{i,\sigma(i)}$$

  where S_n is the set of all permutations of n elements. Valiant proved that the permanent is #**P** -complete by reduction from $\#SAT$.

  In particular, if M is a 0-1 matrix, $\text{Perm}(M)$ counts the number of perfect matchings in a bipartite graph G_M whose biadjacency matrix is M. This example suggests that counting problems can be harder than decision problems, as existence of a perfect matching can be decided in polynomial time whereas no subexponential time algorithm is currently known for (exactly) computing the permanent of a matrix.

2 Toda's Theorem

The power of counting was an open problem in theoretical computer science in the 1980s and 1990s. To be more precise, let $\mathbf{P}^{\#\mathbf{P}}$ be the set of problems solvable with polynomial time algorithms assuming access to a $\#SAT$ oracle. It is immediate that **NP** $\subseteq \mathbf{P}^{\#\mathbf{P}}$ and that **coNP** $\subseteq \mathbf{P}^{\#\mathbf{P}}$ as one can decide

existence of a solution by querying the oracle. Furthermore, $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{PSPACE}$ since each $\#SAT$ query can be evaluated using a polynomial amount of memory. However, there remained a huge gap between these upper and lower bounds until the discovery of Toda's theorem [Tod91].

Theorem 1 (Toda's Theorem)**.** $\mathbf{PH} \subseteq \boldsymbol{P}^{\#\mathbf{P}}$ *. In other words, any problem in the polynomial hierarchy has a polynomial time reduction to $\#SAT$. Furthermore, the reduction only uses one query to the $\#SAT$ oracle.*

This was quite surprising at the time, as this seemed to imply that counting is a more powerful resource than originally thought.

The proof proceeds in two main steps and we will summarize the proofs given in [AB09, Chapter 17], also presented in [Mos12]. First, we provide a randomized reduction from **PH** to a related problem $\oplus SAT$. Finally, we will derandomize the reduction to show that **PH** can be reduced to $\#SAT$.

2.1 Step 1: Randomized Reduction to $\oplus SAT$

Definition 2 (The Parity Quantifier)**.** Given a Boolean formula φ, we say that $\oplus\varphi$ is true if and only if φ has an odd number of satisfying assignments. $\oplus SAT$ is the set of all formulas with an odd number of satisfying assignments.

The first step of Toda's theorem is the following reduction.

Theorem 2. *Let $m \geq 1$. There is a polynomial time randomized reduction A that takes a quantified Boolean formulas φ with at most c alternating quantifiers and n variables as input, with the property that*

- *If φ is true, then* $\Pr[A(\varphi) \in \oplus SAT] \geq 1 - 2^{-m}$
- *If φ is false, then* $\Pr[A(\varphi) \in \oplus SAT] \leq 2^{-m}$.

The reduction runs in time $(nm)^{O(c)}$.

Before we prove the theorem, we firstly observe the following properties about the parity quantifier. Given Boolean formula φ let $\#\varphi$ denote the number of satisfying assignments it has. Given two Boolean formulas $\varphi_1(x_1, \ldots, x_n), \varphi_2(y_1, \ldots, y_m)$, there are formulas $\varphi_1 \cdot \varphi_2$ and $\varphi_1 + \varphi_2$ satisfying $\#(\varphi_1 \cdot \varphi_2) = \#(\varphi_1)\#(\varphi_2)$ and $\#(\varphi_1 + \varphi_2) = \#(\varphi_1) + \#(\varphi_2)$. In particular, one can take $\varphi_1 \cdot \varphi_2 = \varphi_1(x) \wedge \varphi_2(y)$, and

$$\varphi_1 + \varphi_2 = (z_{n+1} \wedge \varphi_1(z_1, \ldots, z_n)) \vee (\overline{z_{n+1}} \wedge \overline{z_n} \wedge \ldots \overline{z_{m+1}} \wedge \varphi_2(z_1, \ldots, z_m))$$

assuming $n \geq m$. In particular, this observation implies that given formulas $\oplus\varphi_1, \oplus\varphi_2$, one can find a formula ψ for which $\oplus\psi$ is logically equivalent to each of $(\oplus\varphi_1) \wedge (\oplus\varphi_2), (\oplus\varphi_1) \vee (\oplus\varphi_2)$, and $\neg(\oplus\varphi_1)$. For instance, $(\oplus\varphi_1) \wedge (\oplus\varphi_2)$ is logically equivalent to $\oplus(\varphi_1 \cdot \varphi_2)$ and the addition $\varphi_1 + \varphi_2$ is used for the other two cases. We prove the main theorem by combining this observation about $\oplus SAT$ with the Valiant-Vazirani reduction.

Theorem 3 (Valiant-Vazirani Reduction)**.** *Let $\beta : \{0,1\}^n \to \{0,1\}$ be a Boolean function. There is a randomized reduction running in poly(n) time that produces a formula $\alpha(x, y)$ with the property that*

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

The Valiant-Vazirani reduction combined with the properties of $\oplus SAT$ and induction, can be used to show that the claimed reduction exists.

Proof of Theorem 2 assuming Theorem 3. We will proceed by induction on the number of quantifiers c in φ, and may assume that $\varphi = \exists\, x\, \beta(x)$ and β has at most $c - 1$ quantifiers. Otherwise, we can apply the reduction to the negation $\neg\varphi$ since we observed that we can always find a formula ψ for which $\oplus\psi$ is equivalent to $\neg(\oplus\varphi)$. The case $c = 1$ is covered by the Valiant-Vazirani reduction and Chernoff bounds.

Now assuming by induction that β can be converted into a $\oplus SAT$ formula $\oplus\tau(y)$ correctly, one can apply the Valiant-Vazirani reduction K times to conclude that the formula

$$\alpha = \bigvee_{i=1}^{K} (\oplus\alpha_i(x, y) \wedge \oplus\tau(y))$$

has the property if $\exists x\,(\beta(x) = 1)$, that

$$\Pr[\bigvee_{i=1}^{K}(\oplus\alpha_i(x,y) \wedge \oplus\tau(y)) = 1] \geq 1 - (1 - \frac{1}{8n})^K \geq 1 - \exp(-\frac{K}{8n}),$$

which can be made arbitarily close to 1 by choosing $K = O(nm)$. Otherwise, in the case where $\beta(x)$ is not satisfiable, $\Pr[\bigvee_{i=1}^{K}(\oplus\alpha_i(x,y) \wedge \oplus\tau(y)) = 1] = 0$. By the previous observations about logical properties of $\oplus SAT$ formulas, α can be converted into a $\oplus SAT$ formula. Since we can argue similarly that the failure probability of the induction hypothesis can be made arbitrarily small, this completes the proof of the theorem. □

Now it remains to prove that the Valiant-Vazirani reduction is correct. We provide the statement of the Valiant-Vazirani reduction here. The reduction works as follows.

- Choose uniformly at random an index $i \in \{1, \ldots, n\}$ and random Boolean vectors $v_1, \ldots, v_{i+1} \in \{0,1\}^n$.
- Let $\alpha(x,y)$ be the Boolean formula $\alpha(x,y) = \phi_{v_1} \wedge \cdots \wedge \phi_{v_{i+1}}$ where $\phi_{v_j}(x,y)$ is a Boolean formula that satisfied if and only if the dot product satisfies $v_j \cdot x = 0$. Output $\alpha(x,y) \wedge \beta(x)$.

The correctness of the Valiant-Vazirani reduction follows from the following lemma.

Lemma 1. *If $S \subseteq \{0,1\}^n$ is non-empty, then given vectors $v_1, \ldots, v_{n+1}$, we have*

$$\Pr[\exists i \in \{1, \ldots, n\} \quad |S \cap \langle v_1, \ldots, v_{i+1}\rangle^{\perp}| = 1] \geq \frac{1}{8},$$

where $\langle v_1, \ldots, v_{i+1}\rangle^{\perp} = \{x \in \{0,1\}^n : v_j \cdot x = 0$ for all $j = 1, \ldots, i+1\}$.

In particular, if β was satisfiable, the Valiant-Vazirani reduction produces a formula with a unique (and hence an odd number of) satisfying assignments with probability at least $\frac{1}{8n}$ as claimed, since with probability at least $\frac{1}{n}$ the index chosen in the reduction matches the index in the lemma.

We will defer the proof of the lemma to the Appendix.

2.2 Step 2: Derandomization Step

Now we will derandomize the previous reduction, at the expense of replacing $\oplus SAT$ with $\#SAT$. The following lemma is straightforward to prove.

Lemma 2. *If $a \equiv -1 \mod N$ then $4a^3 + 3a^4 \equiv -1 \mod N^2$. Otherwise, if $a \equiv 0 \mod N$ then $4a^3 + 3a^4 \equiv 0 \mod N^2$.*

The lemma implies the following corollary since we can build a formula φ' with $4\#(\varphi)^3 + 3\#(\varphi)^4$ satisfying assignments given any formula φ.

Corollary 1. *There is a reduction from Boolean formulas φ to φ' with the property that $\varphi \in \oplus SAT$ if and only if $\#(\varphi') \equiv -1 \pmod{2^l}$, which runs in time poly(l).*

Now we can derandomize the reduction presented in Step 1 to conclude the proof of Toda's theorem.

Proof of Theorem 1. We view the randomized reduction in Step 1 as a deterministic reduction $A(\varphi, r)$ that produces a formula φ_r depending some string of random bits $r \in \{0,1\}^R$. Assume that the reduction succeeds with probability at least $\frac{3}{4}$. Now apply the reduction in Corollary 1 to φ_r with $l = R + 2$ to produce some formula φ'_r. If φ was true then $\#(\varphi'_r) \equiv -1 \pmod{2^{R+2}}$ with probability at least $\frac{3}{4}$, and otherwise $\#(\varphi'_r) \equiv -1 \pmod{2^{R+2}}$ with probability at most $\frac{1}{4}$. This observation implies that the sum

$$s = \sum_{r \in \{0,1\}^R} \#(\varphi'_r)$$

lies in the range $[-2^R, -\frac{3}{4}2^R] \pmod{2^{R+2}}$ when φ is true and lies in the range $[-\frac{1}{4}2^R, 0] \pmod{2^{R+2}}$ when φ is false. These ranges are disjoint so computing s is sufficient to decide satisfiability of φ.

One can compute the sum s with a $\#SAT$ oracle. All of our reductions are polynomial time, so there is a polynomial sized circuit $\mathcal{C}_\varphi$ that computes if z is satisfying assignment of ϕ'_r given r, z as input. Thus, given a formula φ, we can construct the circuit $\mathcal{C}_\varphi$ in polynomial time and convert it into a Boolean formula using the Cook-Levin construction. A single $\#SAT$ oracle query can then be used to compute the sum s, as by construction s is the number of inputs that satisfy the circuit $\mathcal{C}_\varphi$. This completes the proof that any problem in **PH** can be reduced in polynomial time to $\#SAT$, and thus $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}}$. □

3 Application to Quantum Supremacy Conjectures

A recent application of Toda's theorem is to the study of quantum supremacy conjectures. A generally agreed upon definition of a problem that display quantum supremacy is any problem that (1) can be solved using a quantum device being built with current technology, and (2) no (classical) randomized polynomial time algorithm exists for the problem, assuming that the polynomial hierarchy does not collapse.

Examples of experiments in the past few years that claim to have achieved quantum supremacy include Google's random circuit sampling experiment [AAB+19], and a boson sampling experiment done by the University of Science and Technology in China [ZWD+20]. In these problems, a quantum circuit produces some distribution $\mathcal{D}_C$ over strings that a quantum device would ideally be able to reproduce with small error. On the other hand, one would like to argue that any randomized classical algorithm has no hope of sampling from $\mathcal{D}_C$ with small error. The typical outline of such an argument proceeds in the following steps, which is done in [AA11] for the case of boson sampling experiments.

1. Argue that approximating the output probabilities in $\mathcal{D}_C$ is a $\#\mathbf{P}$-hard problem.
2. Argue that if there was a randomized polynomial time algorithm to approximately sample from $\mathcal{D}_C$, then one can approximate the output probabilities of $\mathcal{D}_C$ using a $\mathbf{BPP^{NP}}$ algorithm. This step typically uses the Stockmeyer's approximate counting algorithm.
3. Using Toda's theorem, $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}}$. However, if we assume a randomized polynomial time exists for our problem, then (1) and (2) imply we can solve a $\#\mathbf{P}$-hard problem in $\mathbf{BPP^{NP}}$. Therefore, $\mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{BPP^{NP}}$, which implies that the polynomial hierarchy collapses to the third level, since $\mathbf{BPP}$ is in the 2nd level of the polynomial hierarchy (Sipser-Lautemann theorem).

Step (1) is currently the least understood but perhaps provides the most interesting research directions. In particular in the case of boson sampling, there are interesting conjectures concerning the behaviour of the permanent $\mathrm{Perm}(X)$ for a matrix X where X has identically and independently distributed Gaussian entries, which have been proposed in [AA11] and imply that estimating boson sampling probabilities is $\#\mathbf{P}$-hard. There seems to have been a lot of progress made in studying these conjectures in recent years and there seem to be remain many interesting open questions to investigate.

References

[AA11] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 333–342, 2011.

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[AB09] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[Bea04] Paul Beame. Toda's theorem, April 2004. `https://users.cs.duke.edu/~reif/courses/complectures/Beame/lect07.pdf`.

[Mos12] Dana Moshkovitz. Toda's theorem, Fall 2012. `https://ocw.mit.edu/courses/mathematics/18-405j-advanced-complexity-theory-spring-2016/lecture-notes/MIT18_405JS16_Todas.pdf`.

[Tod91] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[ZWD+20] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

A Proof of Lemma 1

We follow the proof given in Paul Beame's notes [Bea04]. The lemma follows immediately from the following lemmas.

Lemma 3. *Let $S \subseteq \{0,1\}^n$ be a non-empty set and $v_1, \ldots, v_{n+1}$ be vectors in $\{0,1\}^n$. Then:*

1. *If $0^n \in S$, $\Pr[|S \cap \langle v_1, \ldots, v_{n+1}\rangle^\perp| = 1] > \frac{1}{2}$.*
2. *If $0^n \notin S$ and $2^{i-1} \leq |S| \leq 2^i$, then $\Pr[|S \cap \langle v_1, \ldots, v_{i+1}\rangle^\perp| = 1] > \frac{1}{8}$.*

Proof. Observe that if $x \neq 0$ and $v \in \{0,1\}^n$ is chosen randomly, then $\Pr[v \cdot x = 0] = \frac{1}{2}$. Therefore, if $v_1, \ldots, v_j$ were chosen independently, $\Pr[v_i \cdot x = 0 \text{ for all } i = 1, \ldots, j] = \frac{1}{2^j}$.

Suppose we are in the first case where $0^n \in S$. Then by the union bound,

$$\Pr[\exists x \in S, x \neq 0, x \in \langle v_1, \ldots, v_{n+1}\rangle^\perp] \leq \frac{|S|-1}{2^{n+1}} < \frac{2^n}{2^{n+1}} = \frac{1}{2}.$$

This establishes the first case.

For the second case, assume that $x \neq y$ and $x, y \neq 0^n$. Given vectors $v_1, \ldots, v_{i+1}$, define $h(x) = (v_1 \cdot x, \ldots, v_{i+1} \cdot x)$. We can observe that

$$\Pr[h(x) = h(y) = 0^{i+1}] = \frac{1}{2^{2(i+1)}}$$

as we are assuming that x and y are linearly independent. Therefore, for fixed x, by the union bound and our assumption on $|S|$,

$$\Pr[\exists y \in S - \{x\}, h(x) = h(y) = 0^{i+1}] \leq \frac{|S|-1}{2^{2(i+1)}} < \frac{2^i}{2^{2(i+1)}} = \frac{1}{2^{i+2}}.$$

This calculation implies that for a fixed x,

$$\Pr[h(x) = 0^{i+1} \text{ and it is the unique solution in } S] > \frac{1}{2^{i+1}} - \frac{1}{2^{i+2}} = \frac{1}{2^{i+2}}.$$

Therefore, summing over all $x \in S$,

$$\Pr[\exists x \in S, h(x) = 0^{i+1} \text{ and it is the unique solution}] > \frac{|S|}{2^{i+2}} \geq \frac{2^{i-1}}{2^{i+2}} = \frac{1}{8}.$$

□