数理解析研究所講究録
第 1950 巻 2015 年 28-33

Bounded arithmetic theory for the counting functions and Toda's theorem

Satoru Kuroda
Gunma Prefectural Women's University

Abstract

In this paper we give a two sort bounded arithmetic whose provably total functions coincide with the class $FP^{\#P}$. Our first aim is to show that the theory proves Toda's theorem in the sense that any formula in Σ_{∞}^{B} is provably equivalent to a Σ_{0}^{B} formula in the language of $FP^{\#P}$. We also argue about some problems concerning logical theories for counting classes.

1 Introduction

In this note, we argue about logical theories for the counting class $P^{\#P}$. In [2], Toda proved the celebrated result that $PH\subseteq P^{\#P}$, thus the whole polynomial hierarchy collapses to polynomial time with the aid of $\#P$ oracles.

In the context of Bounded Reverse Mathematics, it is natural to ask whether there is a minimal theory for $FP^{\#P}$ which proves Toda's theorem. Here, minimal intuitively means that it provably defines all functions in $FP^{\#P}$ and any such theory contains it.

Toda's original proof is divide it into two part; firstly it is proved that PH is probabilistically simulated in polynomial time with oracle access to $\oplus P$, then $BP\cdot\oplus P$ is derandomized by the counting function.

In [1], Buss et.al. proved that the first part of Toda's theorem can be formalized and proved in their theory $APC_{2}^{\oplus_{p}P}$ which extends T_{2}^{1} by the modular counting quantifier and surjective weak pigeonhole principle for $PV_{2}^{\oplus_{p}P}$ functions.

Here we pose on the problem of whether a minimal theory for $P^{\#P}$ proves the whole Toda's theorem. A candidate for such a theory is PV or S_{2}^{1} extended by axioms stating that

> for any PTIME relation $\varphi(\bar{X}, Y)$ and a term t we can compute $C_{\varphi}(\bar{X})=\#Y< t\varphi(\bar{X}, Y)$.

However, it seems that we need some extra concept for proving Toda's theorem. The main obstacle is that Toda's proof requires a bijection defined by PV_{2} functions, which is not known to be formalized in our theory.

Below we will give a sketch of a partial result on the provability of the whole Toda's theorem together with some open problems.

2 A Theory for $P^{\#P}$

First we overview complexity classes which are treated in this paper. Let FP denote the class of functions computable by some deterministic Turing machine within time bounded by a polynomial in the length of the input. The counting class $\#P$ consists of functions

$$F_M(X) = \text{the number of accepting path of } M \text{ on input } X$$

for some polynomial time bounded nondeterministic Turing machine M. $FP^{\#P}$ is the class of functions which are computable by some polynomial time bounded determinstic Turing machine with oracle accesses to a function in $\#P$. A set A is in the parity class $\oplus P$ if

$$X \in A \Leftrightarrow \text{the number of accepting path of } M \text{ on input } X \text{ is odd}$$

Probabilistic classes also plays crucial roles in the proof of Toda's theorem. A set A is in PP if there exist a nondeterministic polynomial time machine M and a polynomial $q(n)$ such that

$$X \in A \Leftrightarrow |\{W \in \{0,1\}^{q(|X|)} : M(X,W) = 1\} > 2^{q(|X|)}/2.$$

The language L_2 of two-sort bounded arithmetic comprises number variables $x, y, z, \ldots$ and string variables $X, Y, Z, \ldots$ together with function symbols $Z() = 0, x + y, x \cdot y, |X|$ and relation symbols $x \le y, x \in X$.

The classes Σ_i^B and Π_i^B for $i \ge 0$ is defined inductively as follows:

- $\Sigma_i^B = \Pi_i^B$ consists of all L_2 formulas containing only bounded number quantifiers.
- Σ_{i+1}^B is the smallest class containing Π_i^B and closed under Boolean operations bounded number quantifications and positive occurrences of bounded exsitential string quantifiers.
- Π_{i+1}^B is the smallest class containing Σ_i^B and closed under Boolean operations bounded number quantifications and positive occurrences of bounded universal string quantifiers.

The L_2 theory V_0 consists of defining axioms for symbols in the language L_2 together with

$$\Sigma_0^B\text{-}COMP : \exists X \forall x < a(x \in X \leftrightarrow \varphi(x)), \ \varphi \in \Sigma_0^B.$$

We extend the language L_2 by a symbol expressing the cardinality of finite sets. Let L_C be the language L_2 extended by a function symbol $S(X)$, relation symbol $X <_s Y$ and an operator C. Defining axioms for $S(X)$ and $X <_s Y$ are

$$\begin{aligned}
&S(X) = Y \Leftrightarrow \\
&\exists i < |X| \neg X(i) \rightarrow \\
&(|X| = |Y| \wedge \forall i < |X|(i \le i_{min} \rightarrow (X(i) \leftrightarrow \neg Y(i))) \wedge (i > i_{min} \rightarrow (X(i) \leftrightarrow Y(i)))) \\
&\wedge \forall i < |X| X(i) \rightarrow \\
&(|X| + 1 = |Y| \wedge Y(|Y| - 1) \wedge i < |Y| - 1 \rightarrow \neg Y(i))
\end{aligned}$$

where $i_{min} = \min\{j : \neg X(j)\}$, and

$$\begin{aligned}
&X <_s Y \Leftrightarrow |X| < |Y| \vee \\
&(|X| = |Y| \wedge \exists i < |X|(\neg X(i) \wedge Y(i) \wedge \forall j < |X|(j > i \rightarrow (X(j) \leftrightarrow Y(j))))))
\end{aligned}$$

Axioms Ax-$\mathsf{C}[\varphi(X)]$ consists of the followings:

$$\begin{array}{l}\mathsf{C}[\varphi(X)](0,0)\\ \mathsf{C}[\varphi(X)](Y,Z) \wedge \mathsf{C}[\varphi(X)](Y,Z') \rightarrow Z = Z'\\ \mathsf{C}[\varphi(X)](Y,Z) \wedge \varphi(S(Y)) \rightarrow \mathsf{C}[\varphi(X)](S(Y),S(Z))\\ \mathsf{C}[\varphi(X)](Y,Z) \wedge \neg\varphi(S(Y)) \rightarrow \mathsf{C}[\varphi(X)](S(Y),Z)\end{array}$$

Intuitively,

$$\mathsf{C}[\varphi(X)](Y,Z) \Leftrightarrow |\{X <_s Y : \varphi(X)\}| = Z.$$

Definition 1 *The L_C theory $V\#C$ has the following axioms:*

- *BASIC axioms,*
- *$\Sigma_0^B(L_C)$-COMP,*
- *$MCV \equiv \exists Y \leq a + 2\delta_{MCV}(a,G,E,Y)$, where*

  $$\begin{array}{l}\delta_{MCV}(a,G,E,Y) \equiv\\ \neg Y(0) \wedge Y(1) \wedge \forall x < a2 \leq x \rightarrow\\ Y(x) \leftrightarrow [(G(x) \wedge \forall y < x(E(y,x) \rightarrow Y(y))) \vee (\neg G(x) \wedge \exists y < x(E(y,x) \wedge Y(y)))]\end{array}$$

- *Ax-$\mathsf{C}[\varphi(X)]$ for $\varphi \in \Sigma_0^B(L_2)$*

Theorem 1 *A function is Σ_1^B definable in $V\#C$ if and only if it is in $FP^{\#P}$.*

3 Formalizing Toda's theorem

We augument the theory $V\#C$ by some axioms and show that Toda's theorem can be proven in the extended theory.

Definition 2 *CPV is the theory $V\#C$ extended by the following axioms:*

- *Σ_1^B-SIND: $\varphi(0) \wedge \forall X(\varphi(X) \rightarrow \varphi(S(X))) \rightarrow \forall X\varphi(X)$.*
- *Σ_∞^B-Implication: for Σ_∞^B-formulas φ, ψ,*

  $$\begin{array}{l}\forall X < A(\varphi(X) \rightarrow \psi(X)) \wedge CX[\varphi(X)](A,Z) \wedge CX[\psi(X)](A,Z')\\ \rightarrow Z \leq Z'.\end{array}$$

- *Σ_∞^B-Surjection: for Σ_∞^B-formula φ, ψ and $F \in PV_2$,*

  $$\begin{array}{l}\forall F : \varphi(X)_{<A} \longrightarrow \psi(X)_{<A} \ :\ \textit{onto} \wedge CX[\varphi(X)](A,Z) \wedge CX[\psi(X)](A,Z')\\ \rightarrow Z \geq Z'.\end{array}$$

Toda's theorem is formalized in bounded arithmetic as

Theorem 2 *For any $\varphi(X) \in \Sigma_\infty^B$ there exists a Σ_0^B formula $\psi(X,Y)$ and a PV predicate $P(Z)$ such that*

$$\begin{array}{l}\varphi(B) \wedge CY[\psi(X,Y)](A,B,Z) \rightarrow P(Z)\\ \varphi(B) \wedge CY[\psi(X,Y)](A,B,Z) \rightarrow \neg P(Z)\end{array}$$

The first part of the theorem is formalized as follows:

Theorem 3 (CPV) *For any* $\varphi(X) \in \Sigma^B_\infty$ *there exists a Boolean PV function* $F(X, Z, W)$ *such that*

1. $\varphi(X) \to Pr_W[\oplus_Z F(X, Z, W) = 1] \geq 3/4$
2. $\neg\varphi(X) \to Pr_W[\oplus_Z F(X, Z, W) = 1] \leq 1/4$

Note that we cannot compute the exact value of $Pr_W[\oplus_Z F(X, Z, W) = 1]$ since it counts $\oplus P$ prdicate. Nevertheless, we can approximate it by $P^{\#P}$ functions using Implicaiton and Surjection axioms.

The first part of Toda's theorem is proved using

Theorem 4 (Valiant-Vazirani in CPV**)** *For any* $\varphi(X, Y) \in \Sigma^B_0$ *there exists* $\tau(Y, Z) \in \Sigma^B_0$ *such that*

$$\exists Y < t\varphi(X, Y) \to Pr_Z[\exists! Y < t\varphi(X, Y) \wedge \tau(Y, Z)] > 1/8n$$

So NP predicates can be probabilistically reduced to PTIME predicates with unique solution. The construction depends only on the value t.

Valiant-Vazirani theorem yields

Theorem 5 (CPV) *For any* $\varphi(X, Y) \in \Sigma^B_0$ *there exists a PV-function* $F(X, Y, Z)$ *such that*

$$\exists Y < t\phi(X, Y) \to Pr_Z[\oplus_Y F(X, Y, Z) = 1] > 1/8n$$

The following combinatorial property is the key to the proof of V-V:

Lemma 1 (Valiant-Vazirani Lemma in CPV**)** *Let* $n \geq 1$ *and* $S \subseteq \{0, 1\}^n$ *be such that* $2^{k-2} \leq |S| \leq 2^{k-1}$ *where* $k \leq n$. *For a pairwise independent hash function family* $\mathcal{H}_{n,k}$

$$Pr_{h \in \mathcal{H}_{n,k}}[\exists! x \in Sh(x) = 0^k] \geq 1/8.$$

Proof. Use the inclusion-exclusion principle

$$\begin{aligned} &Pr[\exists x \in Sh(x) = 0^k] \\ &\geq \textstyle\sum_{x \in S} Pr[h(x) = 0^k] - \sum_{x < x' \in S} Pr[h(x) = 0^k \wedge h(x') = 0^k] \end{aligned}$$

and the union bound

$$Pr[\exists^{\geq 2} x \in Sh(x) = 0^k] \leq \sum_{x < x' \in S} Pr[h(x) = 0^k \wedge h(x') = 0^k].$$

To prove these principles we construct a PV_2 surjection and use Surjection axiom.

Given n and $k \leq n$ we define a family of pairwise independent hash functions

$$\mathcal{H}_{n,k} = \{h_{A,b}(x) = Ax + b \bmod 2 \ : \ A \in \{0, 1\}^{n \times k}, b \in \{0, 1\}^k\}.$$

Let $S_X = \{Y \in \{0, 1\}^n \ : \ \varphi(X, Y)\}$ and k be such that $2^{k-2} \leq |S| \leq 2^{k-1}$

By Valiant-Vazirani Lemma,

$$Pr_{h \in \mathcal{H}_{n,k}}[\exists! Y \in S_X h(Y) = 0^k] > 1/8.$$

So first take $1 \leq k \leq n$ randomly and then pick $h \in \mathcal{H}_{n,k}$ yields a formula such that

$$\exists Y \varphi(X,Y) \rightarrow Pr_{h \in \mathcal{H}_{n,k}}[\exists! Y \varphi(X,Y) \wedge ||h(Y) = 0^k||] > 1/8n$$

Theorem 6 (CPV) *For any $\varphi(X) \in \Sigma^B_\infty$ there exists a Boolean PV function $F(X,Z,W)$ such that*

1. $\varphi(X) \Rightarrow Pr_W[\oplus_Z F(X,Z,W) = 1] \geq 3/4$
2. $\neg\varphi(X) \Rightarrow Pr_W[\oplus_Z F(X,Z,W) = 1] \leq 1/4$

(Proof Sketch).

We construct F by structural induction on φ. We only sketch the case for the formula $\exists Y < t\psi(X,Y)$. In this case, we iterately apply Valiant-Vazirani Theorem $O(n)$ times and take conjunction of them. Then if $\exists Y < t\psi(X,Y)$ is true then with high probability $\oplus_Y F(X,Y,W) = 1$. We also note that Valiant-Vazirani theorem does not use any information from the propositional formula ϕ except for the number of variables in it. □

The second part is easily formalized in CPV.

Theorem 7 (CPV) $BP \cdot \oplus P \subseteq P^{\#P}$

(Proof Sketch).

The probabilistic reduction $F(X,Z,W)$ is actually a PTIME function on two inputs and we can derandomize it using "Toda polynomial"

Lemma 2 *There exists a PTIME function $T(\phi, l)$ such that*

$$\phi \in \oplus SAT \Rightarrow \#T(\phi,l) \equiv -1 \bmod 2^l$$
$$\phi \notin \oplus SAT \Rightarrow \#T(\phi,l) \equiv 0 \bmod 2^l$$

Using this we compute

$$\sum_w \#T(f(\phi,w),|w|+2)$$
$$= \sum_{w,\phi \in \oplus P} \#T(f(\phi,w),|w|+2) + \sum_{w,\phi \notin \oplus P} \#T(f(\phi,w),|w|+2)$$

Computing RHS requires $\mathcal{B}(\Sigma^B_1)$ counting. □

4 Final Remarks

We conjecture that the theory the provably total functions of CPV are $FP^{\#P}$. It is likely that the proof of Toda's theorem does not require counting over $\oplus P$ predicates. Instead, the proof may be formalized using counting over $\Sigma^{B,1}_1$, i.e. Σ^B_1 formulas where $\exists X < t$ is replaced by $\exists! X < t$. The circuit-based proof of Toda's theorem by Kannan et. al. establishes a probabilistic simulation ofconstant-depth exp-size circuits by exp-size XOR circuits. Formalization of the circuit proof may yield an alternative proof of our result in a different theory.

Finally, we give an idea of weaken the theory CPV as an open problem:

Problem 1 *Does $PV + \mathcal{B}(\Sigma^B_1)$-counting prove Toda's Theorem?*

References

[1] S. R. Buss, L. A. Kołodziejczyk and K. Zdanowski, Collapsing modular counting in bounded arithmetic and constant depth propositional proofs, to appear in Transactions of the AMS. (2015).

[2] S. Toda, PP is as hard as the polynomial-time hierarchy, SIAM J.Computing 20(1991),pp.865-877.