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 \(\Sigma_{\infty}^B\) is provably equivalent to a \(\Sigma_0^B\) 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 \(APC^{\oplus _P}_2\) which extends \(T_1^2\) by the modular counting quantifier and surjective weak pigeonhole principle for \(PV^{\oplus _P}_2\) 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 \(S_1^2\) 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 deterministic Turing machine with oracle accesses to a function in $#P$. A set $A$ is in the parity class $\oplus P$ if

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

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

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

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 $x \leq y, x \in X$.

The classes $\Sigma^B_i$ and $\Pi^B_i$ for $i \geq 0$ is defined inductively as follows:

- $\Sigma^B_i = \Pi^B_i$ consists of all $L_2$ formulas containing only bounded number quantifiers.
- $\Sigma^B_{i+1}$ is the smallest class containing $\Pi^B_i$ and closed under Boolean operations bounded number quantifications and positive occurrences of bounded existential string quantifiers.
- $\Pi^B_{i+1}$ is the smallest class containing $\Sigma^B_i$ 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

$$\Sigma^B_0 \cdot COMP : \exists X \forall x < a(x \in X \leftrightarrow \varphi(x)), \varphi \in \Sigma^B_0.$$  

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

$$S(X) = Y \iff$$
$$\exists i < |X| \neg X(i) \rightarrow$$
$$(|X| = |Y| \land \forall i < |X| (i \leq i_{min} \rightarrow (X(i) \leftrightarrow \neg Y(i))) \land (i > i_{min} \rightarrow (X(i) \leftrightarrow Y(i))))$$
$$\land \forall i < |X| X(i) \rightarrow$$
$$(|X| + 1 = |Y| \land Y(|Y| - 1) \land i < |Y| - 1 \rightarrow \neg Y(i))$$

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

$$X <_s Y \iff |X| < |Y| \lor$$
$$(|X| = |Y| \land \exists i < |X| (\neg X(i) \land Y(i) \land \forall j < |X| (j > i \rightarrow (X(j) \leftrightarrow Y(j)))))$$

where $i_{min} = \min\{j : \neg X(j)\}$, and
Axioms $\text{Ax-C}[\varphi(X)]$ consists of the followings:

\begin{align*}
C[\varphi(X)](0,0) \\
C[\varphi(X)](Y,Z) \land C[\varphi(X)](Y,Z') & \rightarrow Z = Z' \\
C[\varphi(X)](Y,Z) \land \varphi(S(Y)) & \rightarrow C[\varphi(X)](S(Y),S(Z)) \\
C[\varphi(X)](Y,Z) \land \neg \varphi(S(Y)) & \rightarrow C[\varphi(X)](S(Y),Z)
\end{align*}

Intuitively,

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

**Definition 1** The $\text{L}_C$ theory $V^\#_C$ has the following axioms:

- $\Sigma^B_0$ axioms,
- $\Sigma^B_0$-COMP,
- $MCV \equiv \exists Y \leq a + 2\delta_{MCV}(a,G,E,Y)$, where

\[
\delta_{MCV}(a,G,E,Y) \equiv
\neg Y(0) \land Y(1) \land \forall x < a2 \leq x \rightarrow
Y(x) \leftrightarrow [(G(x) \land \forall y < x(E(y,x) \rightarrow Y(y))) \lor (-G(x) \land \exists y < x(E(y,x) \land Y(y)))]
\]

- $Ax-C[\varphi(X)]$ for $\varphi \in \Sigma^B_0(L_2)$

**Theorem 1** A function is $\Sigma^B_1$ definable in $V^\#_C$ if and only if it is in $FP^\#_P$.

### 3 Formalizing Toda’s theorem

We augment 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:

- $\Sigma^B_1$-SIND: $\varphi(0) \land \forall X(\varphi(X) \rightarrow \varphi(S(X))) \rightarrow \forall X \varphi(X)$.
- $\Sigma^B_\infty$-Implication: for $\Sigma^B_\infty$-formulas $\varphi, \psi$,

\[
\forall X < A(\varphi(X) \rightarrow \psi(X)) \land CX[\varphi(X)](A,Z) \land CX[\psi(X)](A,Z') \rightarrow Z \leq Z'.
\]

- $\Sigma^B_\infty$-Surjection: for $\Sigma^B_\infty$-formula $\varphi, \psi$ and $F \in PV_2$,

\[
\forall F : \varphi(X) < A \rightarrow \psi(X) < A : \text{onto} \land CX[\varphi(X)](A,Z) \land CX[\psi(X)](A,Z') \rightarrow Z \geq Z'.
\]

Toda’s theorem is formalized in bounded arithmetic as

**Theorem 2** For any $\varphi(X) \in \Sigma^B_\infty$ there exists a $\Sigma^B_0$ formula $\psi(X,Y)$ and a $PV$ predicate $P(Z)$ such that

\[
\varphi(B) \land CY[\psi(X,Y)](A,B,Z) \rightarrow P(Z) \\
\varphi(B) \land CY[\psi(X,Y)](A,B,Z) \rightarrow \neg P(Z)
\]
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. \( \varphi(X) \rightarrow \Pr_{W}[\oplus Z F(X,Z,W) = 1] \geq 3/4 \)
2. \( \neg \varphi(X) \rightarrow \Pr_{W}[\oplus Z F(X,Z,W) = 1] \leq 1/4 \)

Note that we cannot compute the exact value of \( \Pr_{W}[\oplus Z F(X,Z,W) = 1] \) since it counts \( \oplus \) predicate. Nevertheless, we can approximate it by \( \#P \) functions using Implication 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

\[
\exists Y < t \varphi(X,Y) \rightarrow \Pr_{Z}[\exists Y < t \varphi(X,Y) \land \tau(Y,Z)] > 1/8n
\]

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

\[
\exists Y < t \varphi(X,Y) \rightarrow \Pr_{Z}[\oplus Y F(X,Y,Z) = 1] > 1/8n
\]

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

\[
\Pr[\exists x \in Sh(x) = 0^k] \geq \sum_{x \in S} \Pr[h(x) = 0^k] - \sum_{x < x' \in S} \Pr[h(x) = 0^k \land h(x') = 0^k]
\]

and the union bound

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

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

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

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

**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 $\varphi$. 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 $\phi$ 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

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

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 $B(\Sigma^B_1)$ 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 formulated using counting over $\Sigma^B_{1}$, i.e. $\Sigma^B_1$ 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 of constant-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 $PV + B(\Sigma^B_1)$-counting prove Toda’s Theorem?
References
