

Modular Counting Functions in Second Order Bounded Arithmetic

Shuheï Misumi(三隅修平)

Graduate School of Mathematics, Nagoya University
(名古屋大学大学院多元数理科学研究科 D1)

1 Preliminary

J. Paris and A. Wilkie(1985) proposed following counting problems in Bounded Arithmetic in [2]:

Problem 1. Let A be a Δ_0 set.

1. Is $\{\langle n, m \rangle \mid m = |A \cap n|\}$ Δ_0 definable?
2. Is $\{\langle n, i \rangle \mid i < p \wedge i \equiv |A \cap n| \pmod p\}$ Δ_0 definable for prime p ?
3. Let p, q be prime and $p \neq q$. If $\{\langle n, i \rangle \mid i < p \wedge i \equiv |A \cap n| \pmod p\}$ is Δ_0 definable, is $\{\langle n, i \rangle \mid i < q \wedge i \equiv |A \cap n| \pmod q\}$ Δ_0 definable?

We locally call the above *counting function problems*. All these problems are still open, however, they proved a relativized problem with using Ajtai's combinatorics[1].

Theorem 1 (Paris and Wilkie). *There exists $A \subseteq \mathbb{N}$ such that Δ_0^A is not closed under counting mod 2.*

They also proposed a problem related to theorem 1.

Problem 2. Is there any $A \subseteq \mathbb{N}$ such that Δ_0^A is closed under counting mod 2 but not closed under counting.

In this paper we prove this problem affirmatively.

Remark. Recently, we found almost same results in Zambella's work[6]. His proof contains some combinatorics developed only for the proof. We directly use a famous theorem in circuit complexity.

1.1 Second order Bounded Arithmetic

We define a second order theory $\mathbf{S}_2$. Let language $\mathcal{L}$ be $\langle +, \cdot, |, \lfloor \frac{\cdot}{2} \rfloor, \#; \leq; 0, 1; \in \rangle$

Definition 1. Σ^b is the class of $\mathcal{L}$ -formulae only with first order bounded quantifiers.

Definition 2. $\mathbf{S}_2$ is a $\mathcal{L}$ -theory consists of

1. BASIC for $\mathcal{L}$
2. Σ^b -CA
3. LNP

, where $\{\phi(x, X)\}$ -CA(comprehension axiom) and LNP(least number principle) denote

$$\forall X \exists Y \forall x (x \in Y \leftrightarrow \phi(x, X))$$

and

$$\forall X (\exists x (x \in X) \rightarrow \exists x (x \in X \wedge \forall y < x (\neg y \in X)))$$

respectively.

The following definition is the same in [2].

Definition 3.

$$\begin{aligned} \text{COUNT}_p \stackrel{\text{def}}{\Leftrightarrow} & \forall X \exists Y \forall x \forall y (\langle x, y \rangle \in Y \leftrightarrow ((x = 0 \wedge y = 0) \\ & \vee (x > 0 \wedge x - 1 \in X \wedge 0 < y < p \wedge \langle x - 1, y - 1 \rangle \in Y) \\ & \vee (x > 0 \wedge x - 1 \in X \wedge y = 0 \wedge \langle x - 1, p - 1 \rangle \in Y) \\ & \vee (x > 0 \wedge x - 1 \notin X \wedge \langle x - 1, y \rangle \in Y))). \end{aligned}$$

Next is the main theorem.

Theorem 2. For any prime p and integer $q > 1$ such that $p \nmid q$

$$\text{Con}(\mathbf{S}_2 + \text{COUNT}_p + \neg \text{COUNT}_q).$$

Remark. Those who are familiar with Bounded Arithmetic and Complexity Theory may recall *counting principle*, say $\text{Count}(p)$ defined by Ajtai and

Definition 4. Let A a set such that $|A| = an + 1$ and let $[A]^p = \{X \subseteq A \mid |X| = p\}$. Variables P_X are defined for each $X \in [A]^a$.

$$Count_n^p \equiv \bigvee_{X \neq Y, X \cap Y \neq \emptyset} (P_X \wedge P_Y) \vee \bigvee \bigwedge_{i \in A, i \in X} \neg P_X.$$

It is also written as the following scheme:

$$\begin{aligned} \forall X ((\forall y < pn + 1 \exists x < n \langle x, y \rangle \in X) \wedge \forall x \exists y_0, \dots, y_{p-1} \\ (y_0 < \dots < y_{p-1} \wedge \langle x, y_0 \rangle \in X \wedge \dots \wedge \langle x, y_{p-1} \rangle \in X) \\ \exists y < pn + 1 (\forall x < n \langle x, y \rangle \notin Y \wedge \forall z < pn + 1 \exists x < n \\ z \neq y \rightarrow \langle x, z \rangle \in Y) \wedge \forall x \exists y_0, \dots, y_{p-1} (y_0 < \dots < y_{p-1} \\ \wedge \langle x, y_0 \rangle \in Y \wedge \dots \wedge \langle x, y_{p-1} \rangle \in Y))) \end{aligned}$$

$COUNT_p$ is much powerful than $Count^p$.

2 Some Models of S_2

Through this section we use some techniques developed in [5] which modify the method of Boolean extension in set theory. Take a countable nonstandard model $N \succ \mathbb{N}$ and $n \in N - \mathbb{N}$. Let (M, S) be a model of S_2 . First(resp. second) order variables range over M (resp. S). We give a base model (M, S) such that

$$\begin{aligned} M &:= \{x \in N \mid x < n \# \dots (s \text{ times}) \dots \# n, \exists s \in \mathbb{N}\} \text{ and} \\ S &:= \{X \subseteq M \mid \exists \alpha \in N (\forall i \in M (\text{bit}(\alpha, i) = 1 \leftrightarrow i \in X))\}. \end{aligned}$$

Lemma 1.

$$(M, S) \models S_2.$$

Proof. Obviously, M satisfies 1 in definition 2.

Since N has a code α of a sequence with length $\leq 2^n$ of bounded formula $\phi(x)$, 2 holds.

Let $X \in S$. By definition of (M, S) there exists $\alpha \in N$ such that α codes X . Because of $N \succ \mathbb{N}$, we derive that

$$N \models \forall x \exists y (2^y | x \wedge \forall z (2^z | x \rightarrow z \leq y)).$$

Let $x = \alpha$, then $z \in N$ is the least number in X . □

We aim to construct extended model $(M, S[G])$ by the method of boolean extension. So we define some notion.

Definition 5. A Boolean algebra $B \subseteq S$ is called M -complete iff

$$\forall x \in M \forall X \in S (X : M \rightarrow B \\ \rightarrow \bigwedge_{y < x} X(y) \in B \text{ and } \bigvee_{y < x} X(y) \in B).$$

Example 1. *Let*

$$B := \{X \in S \mid X \text{ codes a constant depth super-polynomial size circuit}\}$$

with variables $v_0, v_1, \dots, v_i, \dots \in B$, $i \in M$, then B is non-atomic M -complete Boolean algebra.

2.1 Coding circuits and sets of circuits

A circuit C is a directed acyclic graph with labelled nodes, say gates. Gates at one edge are called input gates consist of $v_0, \dots, v_{n-1}$. Gates at the other edge are output gates. The remaining gates are called connective gates computing some Boolean functions. Unless we specify differently, connective gates are $\wedge$, $\vee$ and $\neg$. The size of circuit C is defined as the number of connective gates of C and the depth of it is defined as the length of the longest path from an input gate to the output gate of C .

In this paper, we assume that a circuit has inputs $v_i, i \in M$ and only one output. We also assume that super-polynomial size means $n^{\log n}$, $n \in N - \mathbb{N}$.

Lemma 2. *Let C be a constant depth super-polynomial size circuit. If N has a code of C , there exists $X \in S$ which codes C .*

Next we code a set of circuits.

Lemma 3. *Let C be a set of constant depth super-polynomial size circuits. If $|C|$ is super-polynomial size and each circuits in C is coded in N , then there is $X \in S$ which codes C .*

2.2 Generic models and truth lemma

Definition 6. For each $x \in M$ and $X \in S$ let

$$(X)_x := \{y \in M \mid \langle x, y \rangle \in X\}$$

and

$$S^B := \{X \in S \mid \forall x \in M ((X)_x \in B)\}.$$

Definition 7. Let $x, y, z \in M$, $X \in S^B$.

- $\|x + y = z\| = 1_B \Leftrightarrow x + y = z.$
- $\|x \cdot y = z\| = 1_B \Leftrightarrow x \cdot y = z.$
- $\|x < y\| = 1_B \Leftrightarrow x < y.$
- $\|x \in X\| := (X)_x.$
- $\|\phi \vee \psi\| := \|\phi\| \vee \|\psi\|.$
- $\|\exists x < y \phi(x)\| := \bigvee_{x < y} \|\phi(x)\|.$

Theorem 3. If ϕ is Σ^b formula then $\|\phi\| \in B$.

Definition 8. $F \subseteq B$ is M -generic ultra filter iff

1. $\forall a \in F \forall b \in B (a \leq b \rightarrow b \in F).$
2. $\forall a, b \in F (a \wedge b \in F).$
3. $\forall a \in B (a \in F \text{ or } \neg a \in F).$
4. $\forall X \in S^B \forall x \in M (\forall y < x ((X)_y \in F) \rightarrow \bigwedge_{y < x} (X)_y \in F).$

Definition 9. Let $F \subseteq B$ a M -generic ultra filter. For $X \in S^B$ let

$$i_F(X) := \{x \in M \mid (X)_x \in F\}$$

$$S[F] := \{i_F(X) \mid X \in S^B\}.$$

Definition 10. For every $X \in S$ define $\check{X} \subseteq M$ such that

$$\forall y (((\check{X})_y = 1_B \leftrightarrow y \in X) \wedge ((\check{X})_y = 0_B \leftrightarrow y \notin X)),$$

where $0_B, 1_B$ is the minimum element, the maximum element respectively in Boolean algebra B .

Theorem 4. *If $X \in S$ then*

$$i_F(\check{X}) = X.$$

Corollary 1. *If $F \subseteq B$ is a M -generic ultra filter then*

$$S \subseteq S[F].$$

Proof. It is sufficient to check that $\check{X} \subseteq M$ is in S^B for any $X \in S$. By definition, there exists $\alpha \in N$ such that $\forall x \in M (x \in X \leftrightarrow \text{bit}(\alpha, i) = 1)$. So we can find the code of $\check{X}$ in N . $\square$

Theorem 5 (truth lemma). *Let ϕ be a Σ^b formula with variables $x_0, \dots, x_i \in M, X_0, \dots, X_j \in S^B$. Suppose that F is a M -generic ultra filter then*

$$\begin{aligned} (M, S[F]) \models \phi(x_0, \dots, x_i, i_F(X_0), \dots, i_F(X_j)) &\Leftrightarrow \\ \|\phi(x_0, \dots, x_i, X_0, \dots, X_j)\| &\in F. \end{aligned}$$

Proof. By induction on the complexity of formula.

1. Let ϕ a atomic formula. It is obvious if ϕ is a first order formula. Without loss of generality we can assume that ϕ can be represented in the form $x \in X$. By definition

$$\begin{aligned} \|x \in X\| \in F &\Leftrightarrow (X)_x \in F \\ &\Leftrightarrow (M, S[F]) \models x \in i_F(X). \end{aligned}$$

2. Suppose that ψ and θ satisfy (5). It is easy to show that ϕ also satisfies (5) if $\phi \equiv \psi \wedge \theta, \psi \vee \theta$ or $\neg\psi$. Let $\phi \equiv \exists x < y \psi(x)$.

$$\begin{aligned} \|\exists x < y \psi(x)\| \in F &\Leftrightarrow \bigvee_{x < y} \|\psi(x)\| \in F \\ &\Leftrightarrow \exists x < y (\|\psi(x)\| \in F) \\ &\Leftrightarrow (M, S[F]) \models \exists x < y \psi(x). \end{aligned}$$

2.3 Generic models of $\mathbb{S}_2$

Lemma 4. *Let F a M -generic ultra filter. then $(M, S[F]) \models LNP$.*

Proof. Let X be an arbitrary nonempty set in $S[F]$. By the definition of generic extension, there exists $\underline{X} \in S^B$ such that $i_F(\underline{X}) = X$. Let $Y \in N$ be a set satisfying the following.

$$\forall x \in M ((Y)_x = (\underline{X})_x \wedge \neg \bigvee_{y < x} (\underline{X})_y).$$

We remark that such a Y can be found in S^B by lemma 3.

$$\bigvee_{x \leq z} (Y)_x = \bigvee_{x \leq z} (\underline{X})_x = \|\exists x \leq z (x \in \underline{X})\| \geq \|z \in \underline{X}\| \in F.$$

There exists such a $z \in X$ since X is nonempty. F is M -generic ultra filter. So there exists $x \leq z$ such that $(Y)_x \in F$. For this x

$$\begin{aligned} \|x \in \underline{X} \wedge \forall y \in \underline{X} (x \leq y)\| &\geq (\underline{X})_x \wedge \bigwedge_{y \leq z} ((\underline{X})_y \rightarrow \|x \leq y\|) \\ &= (\underline{X})_x \wedge \bigwedge_{y < x} \neg (\underline{X})_y = (Y)_x \in F \end{aligned}$$

By truth lemma we thus derive that

$$(M, S[F]) \models x \in X \wedge \forall y \in X (x \leq y).$$

□

Lemma 5. *For any M -generic ultra filter F $(M, S[F]) \models \Sigma^b\text{-CA}$.*

Proof. Let $\phi(x, X) \in \Sigma^b$ and let $x \in M$, $X \in S[F]$. By the definition of generic extension there exists $\underline{X} \in S^B$ such that

$$(\underline{X})_x \in F \leftrightarrow x \in X.$$

Claim. There exists $\underline{Y} \in S^B$ such that $(\underline{Y})_x = \|\phi(x, \underline{X})\|$ for any $x \in M$.

At first glance we can find such a $\underline{Y}$ in S . Since $\phi(x, \underline{X}) \in \Sigma^b$, $\|\phi(x, \underline{X})\|$ is written as some finite (AND OR)-alternations of p constant depth super-polynomial size circuits, where p a super-polynomial of n . Thus $\|\phi(x, \underline{X})\|$ is also constant depth super-polynomial size and so in B .

We then obtain $Y = i_F(\underline{Y})$ which codes $\phi(x, \underline{X})$.

□

By Lemmas

Theorem 6. *Let B a M -complete Boolean algebra. If $F \subseteq B$ a M -generic ultra filter then*

$$(M, S[F]) \models \mathbf{S}_2.$$

3 An Application of Boolean Valued Models

We devote this section to construct a generic model such that COUNT_p holds but COUNT_q fails. Take a following Boolean algebra:

$$B_p := \{\text{constant depth super-polynomial size circuit with mod } p \text{ gates}\}.$$

Theorem 7. *Let $F \subseteq B_p$ a M -generic ultra filter. Then*

$$(M, S[F]) \models \mathbf{S}_2 + \text{COUNT}_p.$$

Proof. By theorem, 6 it is sufficient to show that $(M, S[F])$ satisfies COUNT_p . So we construct modulo p counting function for arbitrary $X \in S[F]$. Let $\underline{X}$ be a element of S^{B_p} such that $i_F(\underline{X}) = X$. Then define $b_i = \text{MOD}_p((\underline{X})_0, \dots, (\underline{X})_{i-1})$ for every $i \in M$. Each b_i is a element of Boolean algebra B_p since the connective gates mod p are allowed in B_p . Thus there exists $Y \in S^{B_p}$ such that $(Y)_i = b_i$ for all $i \in B_p$. It is clear that $i_F(Y)$ counts X modulo p . $\square$

3.1 Proof of the main theorem

To prove the main theorem(theorem 2) we have to choose a filter F so that

$$(M, S[F]) \models \neg(\forall X \exists Y (Y \text{ counts } X \text{ with modulo } q)).$$

It is the following theorem that provides the key combinatorics for this proof.

Theorem 8 (Smolensky[4]). *For any prime p and integer $q > 1$ such that $p \nmid q$, no constant depth super-polynomial size circuits with mod p gates computes mod q gate.*

Fix a Boolean algebra $B := B_p$. Since $|S^B| = \omega_0$ it is able to enumerate all the elements of S^B :

$$X_0, X_1, \dots, X_i, \dots \quad i \in \mathbb{N}.$$

Let us give a target set,

$$A := \{\langle x, v_x \rangle \mid x \in M\}.$$

We determine whether v_x should be in F or not for all $x \in M$ such that no $Y \in S[F]$ counts the interpretation $i_F(A)$ modulo q . Let us note the definition of counting function again. X counts $i_F(A)$ iff

$$\begin{aligned} & \forall x \in M ((X)_{\langle x-1,0 \rangle} \in F \text{ and } \forall i < q (i \neq 0 \text{ and} \\ & \quad (X)_{\langle x-1,i \rangle} \notin F)) \Leftrightarrow \text{MOD}_q(v_0, \dots, v_{x-1}) = 0) \\ & \text{and } \forall x \in M ((X)_{\langle x-1,0 \rangle} \notin F \text{ and } \forall i < q (i \neq 0 \text{ and} \\ & \quad (X)_{\langle x-1,i \rangle} \in F)) \Leftrightarrow \text{MOD}_q(v_0, \dots, v_{x-1}) = 1). \end{aligned}$$

By induction on $j \in \mathbb{N}$, we make partial mapping $\sigma_i : \subseteq V \rightarrow \{0, 1\}$ each for X_i , $i \in \mathbb{N}$.

Stage (0). Here we assign boolean value to the variables $v_0, \dots, v_{n-1}$ and thus $\text{MOD}_q(v_0, \dots, v_{n-1})$.

Let $\rho_0 : \{v_0, \dots, v_{n-1}\} \rightarrow \{0, 1\}$.

1. Suppose that

$$\begin{aligned} & \exists \rho_0 (((X_0)_{\langle n-1,0 \rangle} \upharpoonright_{\rho_0} \equiv 1 \text{ and } |\rho_0| \not\equiv 0 \pmod{q}) \\ & \quad \text{or } 0 < \exists i < q ((X_0)_{\langle n-1,i \rangle} \upharpoonright_{\rho_0} \equiv 1 \text{ and } |\rho_0| \equiv \\ & \quad 0 \pmod{q}) \\ & \quad \text{or } ((X_0)_{\langle n-1,0 \rangle} \upharpoonright_{\rho_0} \equiv 0 \text{ and } |\rho_0| \equiv 0 \pmod{q}) \\ & \quad \text{or } 0 < \exists i < q ((X_0)_{\langle n-1,i \rangle} \upharpoonright_{\rho_0} \equiv 0 \text{ and } |\rho_0| \not\equiv \\ & \quad 0 \pmod{q})). \end{aligned}$$

Take such a ρ_0 and define $\sigma_0 := \rho_0$.

2. If

$$\exists \rho_0 \exists i < q ((X_0)_{\langle n-1,i \rangle} \upharpoonright_{\rho_0} \neq 0, 1)$$

then take such a ρ_0 and define $\sigma_0 := \rho_0$.

Claim. Any cases except 1 or 2 cause contradiction.

If not in case 1,2 then all the partial mapping ρ_0 give boolean value to $(X_0)_{\langle n-1,i \rangle}$ for all $i < p$ and the value represent $|\rho_0| \bmod q$. This contradicts Smolensky's result.

Stage (1). *Case 1.* Suppose that case 1 is chosen at stage (0). Let us determine boolean value for $\text{MOD}_q(v_0, \dots, v_{n\#n-1})$.

We have already known the value of $v_0, \dots, v_{n-1}$ by ρ_0 .

Let $\rho_1 : \{v_n, \dots, v_{n\#n-1}\} \rightarrow \{0, 1\}$. σ_1 can be chosen by similar way of stage (0).

Case 2. Think in case 2 at stage (0).

Since $(X_0)_{\langle n-1,i \rangle} \in B$, there exists the maximum index $z \in M$ such that v_z appears in $(X_0)_{\langle n-1,i \rangle}$. By definition of M there is $k \in \mathbb{N}$ such that

$$z \leq \underbrace{n\# \dots \# n}_k.$$

Fix the minimum $k \in \mathbb{N}$ of such ks . We now determine the value for $\text{MOD}_q(v_0, \dots, v_{\underbrace{n\# \dots \# n}_{k+1}-1})$. Variables $v_0, \dots, v_{n-1}$ are all assigned by ρ_0 ,

and so is $\text{MOD}_q(v_0, \dots, v_{n-1})$. Thus we can find

$$\pi_1 : \{v_n, \dots, v_{\underbrace{n\# \dots \# n}_{k+1}-1}\} \rightarrow \{0, 1\}$$

such that

$$(X_0)_{\langle n-1,0 \rangle} \upharpoonright_{\rho_0} \upharpoonright_{\pi_1} \neq \text{MOD}_q(v_0, \dots, v_{n-1}).$$

It is possible since $(X_0)_{\langle n-1,0 \rangle} \upharpoonright_{\rho_0} \neq 0, 1$.

Next we define

$$\tau_1 : \{\underbrace{v_{n\# \dots \# n}_k}, \dots, v_{\underbrace{n\# \dots \# n}_{k+1}-1}\} \rightarrow \{0, 1\}$$

with using the same argument at stage(0) and let $\sigma_1 := \tau_1$.

By induction step we obtain $\sigma_i \quad \forall i \in \mathbb{N}$, so that

$$\bigcup_{i \in \mathbb{N}} \sigma_i : \{v_x \mid x \in M\} \rightarrow \{0, 1\}.$$

Fix a ultra filter F such that $\bigcup_{i \in \mathbb{N}} \sigma_i \subseteq F$. Then we have

$$(M, S[F]) \models \forall X (X \text{ does not count } i_F(A) \text{ with modulo } q).$$

□

Remark. There are some problems related to theorem 2.

1. Let $p < q < r$ are primes. Can $S_2 + \text{COUNT}_p + \text{COUNT}_q$ prove COUNT_r ?
2. Moreover, can $S_2 + \text{COUNT}_{p_1} + \dots + \text{COUNT}_{p_s}$ prove $\text{COUNT}_{p_{s+1}}$ for any $s \in \mathbb{N}$?

We finally remark the difficulty of our defining systems which could not be improved in here. In this paper we have studied *non*-bounded version of comprehension axiom and counting principles. We believe, however, that to study a bounded version of them is more suitable in terms of Bounded Arithmetic.

References

- [1] M. Ajtai. σ_1^1 -formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.
- [2] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. In *Methods in Mathematical Logic*, volume 1130 of *Lecture Notes in Mathematics*, pages 317–340. Springer Berlin, 1985.
- [3] S. Riis. $\text{Count}(q)$ does not imply $\text{count}(q)$. *Annals of Pure and Applied Logic*, 90:1–56, 1997.
- [4] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. Proc. 19th ACM Symposium on Theory of Computing, pages 77–82, 1987.
- [5] Masahiro Yasumoto. Bounded second order arithmetic. volume 930 of *Suurikaiseikikenkyokoukyuroku*, pages 10–19, 1995.
- [6] D. Zambella. Algebraic methods and bounded formulas. *Notre Dame J. Formal Logic*, 38:37–48, 1997.