<table>
<thead>
<tr>
<th>Title</th>
<th>Modular Counting Functions in Second Order Bounded Arithmetic (Towards new interaction between category theory and proof theory)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Misumi, Shuhei</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2001), 1217: 75-85</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2001-06</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/41233">http://hdl.handle.net/2433/41233</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Modular Counting Functions in Second Order Bounded Arithmetic

Shuhei 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 $\Delta_0$ set.
1. Is $\{\langle n, m \rangle | m = |A \cap n| \}$ $\Delta_0$ definable?
2. Is $\{\langle n, i \rangle | i < p \land i \equiv |A \cap n| \mod p \}$ $\Delta_0$ definable for prime $p$?
3. Let $p, q$ be prime and $p \neq q$. If $\{\langle n, i \rangle | i < p \land i \equiv |A \cap n| \mod p \}$ is $\Delta_0$ definable, is $\{\langle n, i \rangle | i < q \land i \equiv |A \cap n| \mod q \}$ $\Delta_0$ 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 $\Delta^A_0$ 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 $\Delta^A_0$ 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 $S_2$. Let language $L$ be $\langle +, \cdot, |, \lfloor \overline{2} \rfloor, \#; \leq ; 0, 1; \in \rangle$

**Definition 1.** $\Sigma^b$ is the class of $L$-formulae only with first order bounded quantifiers.

**Definition 2.** $S_2$ is a $L$-theory consists of

1. BASIC for $L$
2. $\Sigma^b$-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

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

respectively.

The following definition is the same in [2].

**Definition 3.**

$$\text{COUNT}_p \leftrightarrow \forall X \exists Y \forall x \forall y (\langle x, y \rangle \in Y \leftrightarrow (x = 0 \land y = 0) \lor (x > 0 \land x - 1 \in X \land 0 < y < p \land \langle x - 1, y - 1 \rangle \in Y) \lor (x > 0 \land x - 1 \in X \land y = 0 \land \langle x - 1, p - 1 \rangle \in Y) \lor (x > 0 \land x - 1 \not\in X \land \langle x - 1, y \rangle \in Y))).$$

Next is the main theorem.

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

$$\text{Con}(S_2 + \text{COUNT}_p + \neg \text{COUNT}_q).$$

**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 $X \in [A]^a$.

\[
\text{Count}^p_n \equiv \bigvee_{X \neq Y, X \cap Y \neq \emptyset} (P_X \land P_Y) \lor \bigvee_{i \in A \cap i \in X} \neg P_X.
\]

It is also written as the following scheme:

\[
\forall X ((\forall y < pn + 1 \exists x < n (x, y) \in X) \land \forall x \exists y_0, \ldots, y_{p-1} \quad (y_0 < \cdots < y_{p-1} \land (x, y_0) \in X \land \cdots \land (x, y_{p-1}) \in X) \\
\exists y < pn + 1 (\forall x < n (x, y) \not\in Y \land \forall z < pn + 1 \exists x < n (z \neq y \rightarrow (x, z) \in Y) \land \forall x \exists y_0, \ldots, y_{p-1} (y_0 < \cdots < y_{p-1} \land (x, y_0) \in Y \land \cdots \land (x, y_{p-1}) \in Y))).
\]

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

\[
M := \{x \in N \mid x < n \# \cdot \cdots \cdot \# n, \exists s \in \mathbb{N}\} \quad \text{and} \\
S := \{X \subseteq M \mid \exists \alpha \in N (\forall i \in M (\text{bit}(\alpha, i) = 1 \leftrightarrow i \in X))\}.
\]

**Lemma 1.**

\[(M, S) \models S_2.\]

**Proof.** Obviously, $M$ satisfies 1 in definition 2.

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

Let $X \in S$. By definition of $(M, S)$ there exists $\alpha \in N$ such that $\alpha$ codes $X$.

Because of $N \succ \mathbb{N}$, we derive that

\[N \models \forall x \exists y (2^y | x \land \forall z (2^z | x \rightarrow z \leq y)).\]

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

\[
B := \{X \in S | X \text{ codes a constant depth super-polynomial size circuit}\}
\]

with variables \(v_0, v_1, \ldots, v_i, \ldots \in B, \ i \in M,\) 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 \(v_0, \ldots, v_{n-1}\). 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 \(\land, \lor\) 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 \(n^\log n, \ n \in N - N\).

**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

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

and

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

Definition 7. Let $x, y, z \in M$, $X \in S^B$.
- $||x + y = z|| = 1_B \iff x + y = z$.
- $||x \cdot y = z|| = 1_B \iff x \cdot y = z$.
- $||x < y|| = 1_B \iff x < y$.
- $||x \in X|| := (X)_x$.
- $||\phi \lor \psi|| := ||\phi|| \lor ||\psi||$.
- $||\exists x < y \phi(x)|| := \bigvee_{x < y} ||\phi(x)||$.

Theorem 3. If $\phi$ is $\Sigma^b$ 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. $\forall a, b \in F(a \land b \in F)$.
3. $\forall a \in B(a \in F$ 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

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

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

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

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

where $0_B, 1_B$ is the minimum element, the maximum element respectively in Boolean algebra $B$. 
Theorem 4. If $X \in S$ then

$$i_F(\check{X}) = X.$$
2.3 Generic models of $S_2$

**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 $X \in S^B$ such that $i_F(X) = X$. Let $Y \in N$ be a set satisfying the following.

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

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

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

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 $x$

$$\|x \in X \land \forall y \in X (x \leq y)\| \geq (X)_x \land \bigwedge_{y \leq z} ((X)_y \rightarrow \|x \leq y\|)$$

$$= (X)_x \land \bigwedge_{y < z} \neg (X)_y = (Y)_x \in F$$

By truth lemma we thus derive that

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

$\square$

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

*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 $X \in S^B$ such that

$$(X)_x \in F \leftrightarrow x \in X.$$ 

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

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

We then obtain $Y = i_F(Y)$ which codes $\phi(x, X)$. $\square$
By Lemmas

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

$$(M,S[F]) \models S_2.$$  

3 An Application of Boolean Valued Models

We devote this section to construct a generic model such that $\text{COUNT}_p$ holds but $\text{COUNT}_q$ 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

$$(M,S[F]) \models S_2 + \text{COUNT}_p.$$  

**Proof.** By theorem, 6 it is sufficient to show that $(M,S[F])$ satisfies $\text{COUNT}_p$. So we construct modulo $p$ counting function for arbitrary $X \in S[F]$. Let $X$ be a element of $S^{B_p}$ such that $i_F(X) = X$. Then define $b_i = \text{MOD}_p((X)_0, \ldots, (X)_{i-1})$ 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 $p$.  

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 $S^B$:

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

Let us give a target set,

$$A := \{(x,v_x) | x \in M\}.$$

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

$$\forall x \in M((X)_{(x-1,0)} \in F \text{ and } \forall i < q(i \neq 0 \text{ and } (X)_{(x-1,i)} \not\in F)) \Leftrightarrow \text{MOD}_q(v_0, \ldots, v_{x-1}) = 0$$

and

$$\forall x \in M((X)_{(x-1,0)} \not\in F \text{ and } \forall i < q(i \neq 0 \text{ and } (X)_{(x-1,i)} \in F)) \Leftrightarrow \text{MOD}_q(v_0, \ldots, v_{x-1}) = 1.$$ 

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

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

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

1. Suppose that

$$\exists \rho_0((X_0)_{(n-1,0)} \upharpoonright_{\rho_0} = 1 \text{ and } |\rho_0| \equiv 0 \text{ mod } q)$$

or

$$0 < \exists i < q((X_0)_{(n-1,i)} \upharpoonright_{\rho_0} = 1 \text{ and } |\rho_0| \equiv 0 \text{ mod } q)$$

or

$$((X_0)_{(n-1,0)} \upharpoonright_{\rho_0} = 0 \text{ and } |\rho_0| \equiv 0 \text{ mod } q)$$

or

$$0 < \exists i < q((X_0)_{(n-1,i)} \upharpoonright_{\rho_0} = 0 \text{ and } |\rho_0| \not\equiv 0 \text{ mod } q)).$$

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

2. If

$$\exists \rho_0 \exists i < q((X_0)_{(n-1,i)} \upharpoonright_{\rho_0} \not\equiv 0, 1)$$

then take such a $\rho_0$ 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 $\rho_0$ give boolean value to $(X_0)_{(n-1,0)}$ for all $i < p$ and the value represent $|\rho_0| \mod q$. This contradicts Smolensky's result.

Stage (1). Case 1. Suppose that case 1 is chosen at stage (0). Let us determine boolean value for $\text{MOD}_q(v_0, \cdots, v_{n\#n-1})$.
We have already known the value of $v_0, \cdots, v_{n-1}$ by $\rho_0$.
Let $\rho_1 : \{v_n, \cdots, v_{n\#n-1}\} \rightarrow \{0, 1\}$. $\sigma_1$ can be chosen by similar way of stage (0).

Case 2. Think in case 2 at stage (0).
Since $(X_0)_{(n-1,0)} \in B$, there exists the maximum index $z \in M$ such that $v_z$ appears in $(X_0)_{(n-1,0)}$. By definition of $M$ there is $k \in \mathbb{N}$ such that

$$z \leq n\#\cdots\#_k \cdots n.$$

Fix the minimum $k \in \mathbb{N}$ of such $ks$. We now determine the value for $\text{MOD}_q(v_0, \cdots, v_{n\#\cdots\#n-1})$. Variables $v_0, \cdots, v_{n-1}$ are all assigned by $\rho_0$, and so is $\text{MOD}_q(v_0, \cdots, v_{n-1})$. Thus we can find

$$\pi_1 : \{v_n, \cdots, v_{n\#\cdots\#n-1}\} \rightarrow \{0, 1\}$$

such that

$$(X_0)_{(n-1,0)} \upharpoonright \rho_0 \upharpoonright \pi_1 \neq \text{MOD}_q(v_0, \cdots, v_{n-1}).$$

It is possible since $(X_0)_{(n-1,0)} \upharpoonright \rho_0 \neq 0, 1$.
Next we define

$$\tau_1 : \{v_{n\#\cdots\#n}, v_{n\#\cdots\#n-1}\} \rightarrow \{0, 1\}$$

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

By induction step we obtain $\sigma_i \forall i \in \mathbb{N}$, 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
\[
(M, S[F]) \vDash \forall X (X \text{ does not count } i_F(A) \text{ with modulo } q).
\]

\[\Box\]

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 $\text{COUNT}_r$?

2. Moreover, can $S_2 + \text{COUNT}_{p_1} + \cdots + \text{COUNT}_{p_s}$ 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


