Forcing on Bounded Arithmetic

Gaisi Takeuti and Masahiro Yasumoto *

[1] Gasi Takeuti
Department of Mathematics,
University of Illinois,
Urbana, Illinois 61801, U.S.A.
email: takeutimath.uiuc.edu
[2] Masahiro Yasumoto
Graduate School of Polymathematics
Nagoya University
Chikusa-ku,
Nagoya, 464-01,
JAPAN
email: D42985A nucc.cc.nagoya-u.ac.jp

Forcing method on Bounded Arithmetic was first introduced by J. B. Paris and A. Wilkie in [10]. Then M. Ajtai started in [1], [2] and [3] elaborate use of the method to get excellent results on the pigeon hole principle and the module p counting principles. Ajtai's work were followed by many works by Beame et als, Krajíček and Riis in [4], [5], [8], [9], [11].

In this paper, we develop a Boolean valued version of forcing on Bounded Arithmetic using big Boolean algebra, and discuss its relation with $NP = co - NP$ problem and $P = NP$ problem.

As is well known, Gödel raised the problem closely related to $P = NP$ problem in his letter to von Neumann in 1956. We believe that Gödel would greatly contribute to it if the complexity theory would have started at the time.

We also would like to mention about Gödel's close felling to Boolean valued models. Forcing and Boolean valued model theory are equivalent. But Gödel was much more impressed by Boolean valued models than forcing in the following reason. Gödel did have a systematic reinterpretation of the logical operations with a view to a formal independence proof, but it was too messy for his taste. He realized that the Boolean valued models are a straightforward model-theoretic variant of his earlier reinterpretation.

When one of the authors started Boolean valued analysis by using Boolean algebras of projections in Hilbert space, he received a strong encouragement from Professor Gödel. We feel that our work is in the line of Gödel's vision.

1. The generic models

Let N be a countable nonstandard model of the true arithmetic $Th(\mathbb{N})$ where $\mathbb{N}$ is the standard model of arithmetic. Let n be a nonstandard element in N and $M = \{x \in N \mid \text{there exists some } n\#\cdots\#n \text{ such that } x \leq n\#\cdots\#n\}$.

* This is the final version of the paper which will not be published elsewhere.

Obviously M is a model of Buss' theory S_2. Let $n_0 = |n|$ and $M_0 = \{|x| \mid x \in M\}$. M_0 is an initial part of M and $x \in M_0$ iff there exists a polynomial p such that $x \leq p(n_0)$.

M can be considered as a first order structure as described above but also can be considered a second order structure over M_0 as follows. Let a second order object X be a pair of (a, b) where $a \in M$ and $b \in M_0$. Then by X we express the set defined by

$$X = \{i < b \mid \mathrm{Bit}(i, a) = 1\}.$$

In this case b is denoted by $|X|$. The second order structure thus obtained is denoted by (M_0, M).

In (M_0, M), the first order variables denote the member of M_0. The second order variables $X, Y, Z, \ldots$ denote sets of members of M_0. For X, Y, Z, $|X|$, $|Y|$, $|Z|, \ldots$ denote members of M_0.

The language of (M_0, M) is described as follows.

First order variables a, b, $c, \ldots$, x, y, $z, \ldots$.

Second order variables X, Y, $Z, \ldots$.

First order constants 0, 1,

First order function constants $+$, $\cdot$, $\lfloor \frac{1}{2} \rfloor$, $|\ |$

Second order function constants $|\ |$

First order predicate $\leq$, $=$

Second order predicate $\in$.

Terms.

1. 0, 1, the first order free variables a, b, $c, \ldots$ and $|X|$, $|Y|, \ldots$ are terms where X, $Y, \ldots$ are second order free variables.
2. If $t_1, \ldots, t_n$ are terms and f is a function constant, then $f(t_1 \cdots, t_n)$ is a term.
3. All terms are obtained by (1) and (2). In the structure (M_0, M), every term expresses a member of M_0.

Formulas.

1. If t_1 and t_2 and terms and X is a second order free variable, then $t_1 \leq t_2$, $t_1 = t_2$ and $t_1 \in X$ is a formula.
2. If φ and ψ are formula, then $\neg\varphi$, $\varphi \wedge \psi$, and $\varphi \vee \psi$ are formulas.
3. If $\varphi(a)$ is a formula and t is a term and X is a second order free variable, then
$$\forall x\varphi(x), \exists x\varphi(x), \forall x \leq t\varphi(x), \exists x \leq t\varphi(x), \forall x \in X\varphi(x)$$
and $\exists x \in X\varphi(x)$ are formulas, where x is a bound variable not occurring in $\varphi(a)$.
4. If $\varphi(X)$ is a formula and t is a term, then
$$\forall X\varphi(X), \exists X\varphi(x), \forall X \leq t\varphi(x), \exists X \leq t\varphi(x)$$
are formulas.

5. Every formula is obtained by (1)-(4).
   The meaning of $\forall X \leq t$ and $\exists X(\leq t$ are $\forall X(|X| \leq t \rightarrow \cdots)$ and $\exists X(|X| \leq t \wedge \cdots)$ respectively.

Definition 1.1. *In the second order language of (M_0, M), $\forall x \leq t$, $\exists x \leq t$, $\forall x \in X$, $\exists x \in X$ are called first order bounded quantifiers. These correspond to sharply bounded quantifiers in the first order language of M.*

Corresponding to hierachies of bounded formulas Σ_1^b, Π_i^b on M, we define hierachies of second order bounded formulas on (M_0, M) as follows.

$\Sigma_0^1(BD) = \Pi_0^1(BD)$ is the class of formulas in which every quantifier is a first order bounded quantifier.

For $i > 0$, $\Sigma_i^1(BD)$ and $\Pi_i^1(BD)$ are defined to be the smallest class of formulas satisfying the following conditions.

a) Both $\Sigma_1^1(BD)$ and $\Pi_i^1(BD)$ are subclass of $\Sigma_{i+1}^1(BD) \cap \Pi_{i+1}^1(BD)$.
b) If $\varphi \in \Sigma_{i+1}^1(BD)$, then $\exists X \leq t\varphi(X)$, $\forall x \leq t\varphi(x)$ and $\exists x \leq t\varphi(x)$ belong to $\Sigma_{i+1}^1(BD)$.
c) If $\varphi \in \Pi_{i+1}^1(BD)$, then $\forall X \leq t\varphi(X)$, $\exists X \leq t\varphi(X)$ and $\forall x \leq t\varphi(x)$ belong to $\Pi_{i+1}^1(BD)$.
d) If φ and ψ belong to $\Sigma_{i+1}^1(BD)$ then both $\varphi \wedge \psi$ and $\varphi \vee \psi$ belong to $\Sigma_{i+1}^1(BD)$. If φ and ψ belong to $\Pi_{i+1}^1(BD)$, then both $\varphi \wedge \psi$ and $\varphi \vee \psi$ belong to $\Pi_{i+1}^1(BD)$.
e) If $\varphi \in \Sigma_{i+1}^1(BD)$.
If $\varphi \in \Pi_{i+1}^1(BD)$, then $\neg\varphi \in \Sigma_{i+1}^1(BD)$ then $\neg\varphi \in \Sigma_{i+1}^1(BD)$.

A formula is said to be a bounded formula if it belongs to $\bigcup_i \Sigma_i^1(BD) = \bigcup_i \Pi_i^1(BD)$ A bounded formula in the second order language of (M_0, M) corresponds to a bounded formula in the first order language of M.

(M_0, M) satisfies the following axioms.

1. Basic axioms on the first order function constants and the first order predicate constants.
2. Axiom on $|X|$ $\forall x \forall X(x \in X \supset x < |X|)$
3. Comprehension Axioms

$$\forall a \exists X \leq a(|x| = a \wedge \forall x < a(x \in X \leftrightarrow \varphi(x)))$$

   where φ is a bounded formula.
4. The least number principleLNP

$$\forall X(X \neq \emptyset \supset \exists x \in X \forall y \in X(x \leq y)).$$

This axiom is equivalent to the Induction Axiom

$$\varphi(0) \wedge \forall x(\varphi(x) \supset \varphi(x+1)) \supset \forall x \varphi(x)$$

where φ is a bounded formula.

Now we are going to define a Boolean algebra. First we introduce Boolean variables $p_0, p_1, p_2, \cdots p_{n_0-1}$ and its negation $\bar{p}_0, \bar{p}_1, \bar{p}_2, \ldots, \bar{p}_{n_0-1}$. More precisely we define some coding of these literals. Now we generate free Boolean algebra from these literals.

In [6], S. Buss developed the theory of sequence in S^1_2. By RSUV-Isomorphisms in [13], the second order theory of sequences hold in (M_0, M) and "X is a sequence" is a $\Delta^1_1(BD)$ predicate where $\Delta^1_1(BD) = \Pi^1_1(BD) \cap \Sigma^1_1(BD)$.

The Boolean algebra B is the set of b which is a sequence $(X_0, X_1, \cdots, X_r)$ with $r \in M_0$ satisfying one of the following conditions.

1. X_i is p_j with $j < n_0$.
2. X_i is $\bar{p}_j$ with $j < n_0$.
3. X_i is $(\wedge, Y_0, Y_1, \cdots, Y_s)$ or $(\vee, Y_0, \cdots, Y_s)$ where $Y_j (j \leq s)$ is one of $(X_0, X_1, \cdots, X_{i-1}$, where the intended meaning of $(\wedge, Y_0, Y_1, Y_s)$ and $(V, Y_0, Y_1, \cdots, Y_s)$ are $Y_0 \wedge Y_1 \wedge \cdots \wedge Y_s$ and $Y_0 \vee Y_1 \vee \cdots \vee Y_s$ respectively.

It is easily seen that there exists a $\Delta^1_1(BD)$ formula φ such that

$$b \in B \quad iff \quad \varphi(b).$$

B is not definable in N since M is not definable in N. However $b \in B$ implies $b \in N$.

Let $b = (X_0, X_1, \cdots, X_s) \in B$. Then $\neg b$ is defined to be $(\bar{X}_0, \bar{X}_1, \cdots, \bar{X}_s)$ where $\bar{X}_i$ is defined by the following rules.

1. If X_i is p_j, then $\bar{X}_i$ is $\bar{p}_j$. If X_i is $\bar{p}_j$, then $\bar{X}_i$ is p_j.
2. If $X_i = (\vee, Y_0, \cdots, Y_t)$, then $\bar{X}_i = (\wedge, \bar{Y}_0, \cdots, \bar{Y}_t)$. If $X_i = (\wedge, Y_0, \cdots, Y_t)$, then $\bar{X}_i = (\wedge, \bar{Y}_0, \cdots, \bar{Y}_t)$. If $X_i = (\wedge, Y_0, \cdots, Y_t)$, then $\bar{X}_i = (\vee, \bar{Y}_0, \cdots, \bar{Y}_t)$.

Let for $i \leq t$ $b_i = (X^i_0, \cdots, X^i_{s_i}) \in B$. Then $\bigvee_{i \leq t} b_i$ is defined to be

$$(X^0_0, \cdots, X^0_{s0}, X^1_s, \cdots, X^1_{s_1}, \cdots, X^t_0, \cdots, X^t_{s_t}, Z)$$

where $Z = (\vee, X^0_{s_o}, \cdots, X^t_{s_t})$.

In the same way $\bigwedge_{i \leq t} b_i$ is defined to be

$$(X^0_0, \cdots, X^0_{s0}, X^1_0, \cdots, X^1_{s_1}, \cdots, X^t_{s_t}, Z^1)$$

where $Z^1 = (\wedge, X^0_{s0}, \cdots, X^t_{s_t})$.

Now let $A \in M$ be a subset of $\{0, \cdots, n_0 - 1\}$. Then A gives a truth value to $p_0, \cdots, p_{n_o-1}$ in the following way.

If $i \in A$, then it assigns 1 to p_i. If $i \notin A$, then it assigns 0 to p_i. So we call A an atom evaluation. Therefore for each $b \in B$, A makes an evaluation of b denoted by eval(A, b). eval(A, b) satisfies the following rules.

1. eval(A, b) is either 0 or 1.

2. $\text{eval}(A, p_i) = 1$ iff $i \in A$.
3. $\text{eval}(A, \neg b) = 1$ iff $\text{eval}(A, b) = 0$.
4. $\text{eval}(A, \wedge_i b_i) = \wedge_i \text{eval}(A, b_i)$
5. $\text{eval}(A, \vee_i b_i) = \vee_i \text{eval}(A, b_i)$.

For $b_1, b_2 \in B$, we define $b_1 \overset{B}{=} b_2$ to be $\forall A$ atom evaluation $(\text{eval}(A, b_1) = \text{eval}(A, b_2))$.

Then
$b_1 \overset{B}{=} b_2$ is $\Pi_1^1(BD)$ in (M_0, M) and Π_1^b in M.

The Boolean algebra we use is $B/\overset{B}{=}$ though we use B in the place of $B/\overset{B}{=}$ for simplicity.

Now we define M^B as follows. $M^B = \{X \in M | \exists y \in M_0(X : y \to B)\}$. Now let $x, y, z, \cdots \in M_0$ and $X \in M^B$. We define the truth value of formulas on (M_0, M^B) by the following rules.

$$[[x + y = z]] = 1 \quad \text{iff} \quad x + y = z$$
$$[[x \cdot y = z]] = 1 \quad \text{iff} \quad x \cdot y = z$$

In the same way for every atomic formula φ

$$[[\varphi]] = 1 \quad \text{iff} \quad M_0 \models \varphi \quad \text{and}$$
$$[[\varphi]] = 0 \quad \text{iff} \quad M_0 \not\models \varphi.$$

$$[[x \in M]] = \begin{cases} X(x) & : \text{ if } X : y \to B \text{ and } x < y \\ 0 & : \text{ otherwise} \end{cases}$$

$$\begin{aligned}
[[\varphi \vee \psi]] &= [[\varphi]] \vee [[\psi]] \\
[[\varphi \wedge \psi]] &= [[\varphi]] \wedge [[\psi]] \\
[[\neg\varphi]] &= \neg[[\varphi]] \\
[[\exists x \le t \varphi(x)]] &= \bigvee_{x \le t} [[\varphi(x)]] \\
[[\forall x \le t \varphi(x)]] &= \bigwedge_{x \le t} [[\varphi(x)]] \\
[[\forall x \in X \varphi(x)]] &= [[\forall x < |X|(x \in X \supset \varphi(x)]] \\
&= \bigwedge_{X < |X|} ([[x \in X]] \supset [[\varphi(x)]]) \\
[[\exists x \in X \varphi(x)]] &= [[\exists x < |X|(x \in X \wedge \varphi(x)]] \\
&= \bigvee_{x < |X|} ([[x \in X]] \wedge [[\varphi(x)]]).
\end{aligned}$$

The following lemma is obvious from the definition.

Lemma 1.1. *Let $\varphi \in \Sigma_0^1(BD)$. Then*

$$[[\varphi]] \in B$$

For $\varphi \notin \Sigma_0^1(BD)$, $[[\varphi]]$ is not defined.

Definition 1.2. *For $X \in M$, $\check{X}$ is defined by the equation*

$$\begin{aligned} \check{X} &= \{< x, 1 > \mid x < |X| \wedge x \in X\} \\ &\cup \{< x, 0 > \mid x < |X| \wedge x \notin X\} \end{aligned}$$

where $< a, b >$ expresses the ordered pair of a and b.

Definition 1.3. *A subset $I \subseteq B$ is said to be an ideal if $0 \in I$, $1 \notin I$, and I is closed under $\vee$ and satisfies $\forall b \in I \forall b' \in B(b' \leq b \supset b' \in I)$.*

A subset $D \subseteq B$ is said to be dense over I if the following condition is satisfied.

$$\forall X \in B - I \exists Y \in D - I(Y \leq X).$$

D is said to be definable if there exist a formula $\varphi(b)$ such that

$$D = \{b \in M | N \models \varphi(b)\}$$

where φ may contain members of N as parameters.

Let M be defined by the equation

$$\mathcal{M} = \{D \subseteq B | D \quad \text{is definable}\}.$$

Since N is countable, $\mathcal{M}$ is also countable and enumerated as

$$D_0, D_1, D_2, \dots.$$

Definition 1.4. *Let $G \subseteq B$. G is said to be $\mathcal{M}$-generic over I if the following condition is satisfied.*

For every $D \in \mathcal{M}$ if D is dense over I, then

$$G \cap (D - I) \neq \emptyset.$$

Let $I \supseteq B$ is an ideal of B. I is said to be M_0- complete if the following condition is satisfied.

$$\forall X \in M(\exists x \in M_0(X : x \to I) \supset \bigvee_{y<x} X(y) \in I).$$

"I is M_0-complete" belongs to $\Pi_1^1(BD)$.

Let $K \subseteq 2^{n_0}$ and be definable in N. Then for $b \in B$ we define $m_K(b)$ by the equation

$$m_K(b) = |\{a \in K | eval(a,b) = 1\}|$$

where $|\{a \in K|\cdots\}|$ *is the cardinality of* $\{a \in K|\cdots\}$ *calculated in* N.
Let $|K| \notin M_0$ *hold. then* I_k *is defined by the equation*

$$I_K = \{b \in B | m_K(b) \in M_0\}.$$

When $k = 2^{n_0}$, I_k *is denoted by* I_0.

Theorem 1.1. I_k *is* M_0 *complete.*

Proof. This is immediately implied by the following obvious property.

$$m_K(\bigvee_i b_i) \leq \Sigma_i m_K(b_i).$$

Example 1.1. Let $n_0 = a \cdot b$ and define $< x, y >$ such that for every $z < n_0$ there exists unique $x < a$ and $y < b$ such that $z =< x, y >$ and $\forall x < a \forall y < b(< x, y >< n_0)$. Define K by

$$K = \{f \in N | f : a \to b\}$$

where the meaning of the function is defined by $< x, y >$. Then $|K| \notin M_0$.

Definition 1.5. *Let* $F \subseteq B$. F *is said to be a filter over* I *if* $F \subseteq B - I$, $1 \in F$,

$$\forall b_1, b_2 \in F(b_1 \wedge b_2 \in F), \quad \text{and} \quad \forall b \in F \forall b' \in B(b \leq b' \to b' \in F).$$

F *is said to be a maximal filter over* I *if* F *is maximal among filters over* I.

Theorem 1.2. *Let* I *be a* M_0*-complete ideal of* B. *Then there exists and* $\mathcal{M}$*-generic maximal filter over* I,

Proof. Let D_0, D_1, $D_2, \cdots$ be an enumeration of all dense sets of $\mathcal{M}$ over I and b_0, b_1, b_2, $\cdots$ be an enumeration of all members of B. We define b_0^1, b_1^1, b_2^1, $\cdots$, as follows.

1. If $b_0 \notin I$, then define $b'_0 = b_0$. Otherwise define $b'_0 = 1$.
2. Let $b'_0 \geq b'_1 \geq \cdots \geq b'_{2i} \notin I$ have been defined. Since D_i is dense over I, there exists $b'_{2i+1} \leq b'_{2i}$ such that $b'_{2i+1} \in D_i - I$.
3. Let $b'_0 \geq b'_1 \geq \cdots \geq b'_{\geq i+1} \notin I$ have been defined. If $b'_{2i+1} \wedge b_i \notin I$, then define $b'_{2i+2} = b_{2i+1} \wedge b_i$. Otherwise define $b'_{2i+2} = b'_{2i+1}$.

After all b'_i are defined, define G by the equation

$$G = \{b \in B | \exists i(b'_i \leq b)\}.$$

Then G is obviously an $\mathcal{M}$-generic maximal filter over I.

Theorem 1.3. *Let I be an M_0-complete ideal of B, $X \in M$ satisfy $X : y \to B \wedge \bigvee_{x<y} X(x) = 1$, and G be an $\mathcal{M}$-generic maximal filter over I. Then the following holds.*

$$\exists x < y(X(x) \in G).$$

Proof. Let $D = \{b \in B | \exists x < y(b \leq X(x))\}$. We claim that D is dense over I. For this, let $b' \in B - I$. Then

$$\bigvee_{x<y} X(x) \wedge b' = b' \notin I.$$

Since I is M_0-complete, $\exists x < y(X(x) \wedge b' \in D - I)$. Since $X(x) \wedge b' \leq b'$, we have proved our claim. Since G is $\mathcal{M}$-generic, $\exists b' \in G \cap D$. Therefore $\exists x < y(b' \leq X(x))$ and $X(x) \in G$.

Let G be an $\mathcal{M}$-generic maximal filter over I and $X : y \to B$. Then we define $i_G(X)$ by the equation

$$i_G(X) = \{x < y | X(x) \in G\}.$$

Then we define $M[G]$ as follows.

$$M[G] = \{i_G(X) | \exists y \in M_0(X : y \to B)\}.$$

The following theorem is obvious.

Theorem 1.4. $i_G(\check{X}) = X$ *for every* $X \in M$.

Corollary 1.1. $M \subseteq M[G]$

Theorem 1.5. *Let $x_1, \cdots, \in M_0$, $X_1, \cdots \in M^B$, $\varphi \in \Sigma_0^1(BD)$, I M_0-complete, and G be an $\mathcal{M}$-generic maximal over I. Then we have the following equivalence.*

$$(M_0, M[G]) \models \varphi(x_1, \cdots, i_G(X_1), \cdots)$$

iff $[[\varphi(x_1, \cdots, X_1, \cdots)]] \in G$.

Proof. We prove this by the induction on the number of logical symbols in $\varphi(x_1, \cdots, X_1, \cdots)$. We treat only the nontrivial cases.

Remark 1.1 (Case 1). φ is of the form $x \in X$. Let $X : y \to B$. Then we have

$$\begin{aligned} [[x \in X]] \in G &\leftrightarrow X(x) \in G \\ &\leftrightarrow x \in i_G(X). \end{aligned}$$

Remark 1.2 (Case 2). φ is of the form $\exists x \le t\varphi(x)$.

$$\begin{aligned}
[[\exists x \le t\varphi(x)]] \in G \quad & \text{iff} \quad \bigvee_{x \le t} [[\varphi(x)]] \in G \\
& \text{iff} \quad \exists x \le t([[\varphi(x)]] \in G) \\
& \text{iff} \quad \exists x \le t(M_0, M[G]) \models \varphi(x) \\
& \text{iff} \quad (M_0, M[G]) \models \exists x \le t\varphi(x).
\end{aligned}$$

Let I be M_0-complete, G an M-generic maximal filter over I, $\tilde{X} = i_G(X)$, and $X : y \to B$. Then we define $|\tilde{X}|$ to be y.

Theorem 1.6. *Let* $\tilde{X} \in M[G]$. *Then the following LNP holds on* $(M_0, M[G])$.

$$\exists x \le t(x \in \tilde{X}) \to \exists x \le t(x \in \tilde{X} \wedge \forall y < x \neg y \in \tilde{X}).$$

Proof. Let $\tilde{X} = i_G(X)$ where $X : y \to B$ Then $Y : y \to B$ is defined by the equation

$$Y(x) = X(x) - \bigvee_{z<x} X(z).$$

Then we have $\bigvee_{x<t} X(x)$. Since the following two equations hold

$$[[\exists x \le t(x \in X)]] = \bigvee_{x \le t} X(x)$$

$$[[\exists x \le t(x \in X \wedge \forall y < x \neg y \in X)]] = \bigvee_{x \le t} (X(x) - \bigvee_{y<x} (X(y)),$$

the following holds.

$$[[\exists x \le t(x \in X)]] \in G \to [[\exists x \le t(x \in X \wedge \forall y < x \neg y \in X)]] \in G.$$

Theorem 1.7. $\Sigma_0^1(BD)$*-Comprehension Axioms hold in* $(M_0, M[G])$.

Proof. Let $\varphi(x) \in \Sigma_0^1(BD)$. If suffices to show that for every $a \in M_0$ the following holds.

$$\{x \le a | (M_0, M[G]) \models \varphi(x)\} \in M[G].$$

Define $Y \in M$ by the conditions $Y : a \to B$ and

$$x \le a \to Y(x) = [[\varphi(x)]]$$

Then the proof follows from the following equivalencies

$$\begin{aligned}
x \in i_G(Y) \quad & \text{iff} \quad x \le a \wedge [[\varphi(x)]] \in G \\
& \text{iff} \quad x \le a \wedge (M_0, M[G]) \models \varphi(x).
\end{aligned}$$

So far we have considered the second order version (M_0, M) of the first order structure M. In the same way, we will consider the first order version $M[G]$ of the second order structure $(M_0, M[G])$.

For M^B, we can add every polynomial time computable function since every polynomial time computable function can be expressed by a polynomial size circuit and the Boolean algebra B is closed by any polynomial size circuit.

¿From this follows that we can introduce all polynomial time computable functions in the structure of $M[G]$. Therefore from now on we always assume that all polynomial time computable functions are defined on the first order structure $M[G]$.

Theorem 1.8. *Let $\varphi(x)$ be sharply bounded. Then if $M \models \forall x \varphi(x)$, then $M[G] \models \forall x \varphi(x)$.*

Proof. Let a be an atom evaluation. (Previously an atom evaluation was denoted by A since we consider it in the second order structure (M_0, M^B). We are now considering it in the first order structure M^B. Therefore it is now denoted by a.) Let x be expressed by $X : y \to B$ and $X^a : y \to \{0,1\}$ be defined by

$$x < y \to X^a(x) = eval(a, X(x)).$$

We also denote the first order expression of X^a by x^a. Then eval$(a, [[\varphi(x)]]) = 1$ iff $M \models \varphi(x^a)$. Therefore $M \models \forall x \varphi(x)$ implies $\forall a$(eval$(a, [[\varphi(x)]]) = 1)$. Therefore $[[\varphi(x)]] \overset{B}{=} 1$. Therefore for every $x \in M[G]$, $M[G] \models \varphi(x)$ and we have $M[G] \models \forall x \varphi(x)$.

Every polynomial time computable function f can be defined by successive function equations from basic functions. This defining equation is called the defining axiom of f.

Theorem 1.9. *Every polynomial time computable function f satisfies the defining axiom of f in $M[G]$.*

Proof. The defining axiom of f can be expressed by a form $\forall \mathbf{x} \varphi(\mathbf{x})$, where $\varphi(\mathbf{x})$ is sharply bounded. Therefore the theorem is immediately implied by Theorem 1.8.

Corollary 1.2. *Let f be a polynomial time computable function and $a \in M_0$. Let $f(a) = b$ in M. Then $f(a) = b$ in $M[G]$.*

Proof. This is immediate from Theorem 1.8.

Definition 1.6. *A sequent $\Gamma \to \Delta$ is said to be Σ_1^b if every formula in Γ or Δ is Σ_1^b.*

Theorem 1.10. *Let $\Gamma \to \Delta$ be Σ_1^b and provable in S_2^1. Then $M[G] \models \Gamma \to \Delta$.*

Proof. This is immediately implied by Buss' Witness Theorem in [6].

It is very difficult to prove that $M[G]$ is a model of Bounded Arithmetic stronger than Σ_1^b-part of S_2^1. One reason is that $[[\varphi]]$ has no reasonable definition when φ is not sharply bounded. In this situation the development of forcing in set theory suggests us that $M[G]$ is probably not a model of S_2.

Let $K \subseteq 2^{n_0}$ satisfy $|K| \notin M_0$. In order to investigate I_k, first we prove the following lemma.

Lemma 1.2. *Let G be an m-generic maximal filter over I_k, $A = \{i < n_0 | p_i \in G\}$, $C \in M$, and D defined by the following equation*

$$D = \{b \in B | \exists i < n_0 (i \in C \wedge b \leq \bar{p}_i) \vee \exists i < n_0 (i \notin C \wedge b \leq p_i)\}.$$

Then D is dense over I_k

Proof. Let $b \in B - I_k$. Then $m_K(b) \notin M_0$. Define b_i for $i < n_0$ as follows.

$$b_i = \begin{cases} & b \wedge \bar{p}_i & : \\ mboxif & i \in C & : \\ & b \wedge p_i & : \text{ otherwise} \end{cases}$$

Then we have

$$\begin{aligned} m_K(\bigvee_{i<n_0} b_i) &= m_K(b \wedge (\bigvee_{i \in C} \bar{p}_i \vee \bigvee_{i \notin C} p_i)) \\ &= m_K(b \wedge \neg(\bigvee_{i \in C} p_i \wedge \bigwedge_{i \notin C} \bar{p}_i)) \geq m_K(b) - 1 \notin M_0. \end{aligned}$$

Therefore $\bigvee_{i<n_0} b_i \notin I_k$. Hence follows $\exists i < n_0 (b_i \notin I_k)$. Since $b_i \leq b \wedge b_i \in D - I_k$, the proof is completed.

Theorem 1.11. *Let G be an $\mathcal{M}$-generic maximal filter over I_k. Then $M[G] \notin M$.*

Proof. Let A and D be defined in Lemma 1.2. By Lemma 1.2 D is dense over I_k. Therefore we have

$$G \cap D \neq \emptyset.$$

Let $b \in G \cap D$

Remark 1.3 (Case 1). $\exists i < n_0 (i \in C \wedge b \leq \bar{p}_i)$. In this case $\bar{P}_i \in G$. Therefore $i \notin A$ and $A \neq C$.

Remark 1.4 (Case 2). $\exists i < n_0 (i \notin C \wedge b \leq p_i)$

In this case $p_i \in G$. Therefore $i \in A$ and $A \neq C$.

Since $b \in D$, either Case 1) or Case 2) holds. Therefore $A \neq C$. Since $C \in M$ is arbitrary, we can conclude that $A \notin M$ and $M \neq M[G]$.

Remark 1.5. So far we have assumed the definability of K. For general (non definable) $X \subseteq 2^{n_0}$ and $a \in N$, we define $|X|$ as follows.

$$| X | \leq a \quad \text{iff} \quad \forall Y \subseteq X (Y \text{ is definable in } N \to |Y| \leq a)$$

Then we define I_K by the equation

$$I_K = \{b \in B | |\{a \in K | \text{eval}(a, b) = 1\}| < a \quad \text{for all} \quad a \in N - M_0\}.$$

We can generalize our theory for this generalized case.

Let 2^{2h+1} be in M_0. We consider the set $\{1, 2, \cdots, 2^{2h+1} - 1\}$ to be a tree with the height $2h$ i.e. we stipulate that 1 is the root and $2^{2h}, 2^{2h} + 1 - 1$ are leaves. In this tree, we call $1, \cdots, 2^{2h} - 1$ nodes and if a is a node, then $2a$ and $2a + 1$ are called its successors. We also define the height of $2^i, 2^i + 1$, $\cdots$, $2^{i+1} - 1$ to be i.

A function

$$f : \{1, 2, \cdots, 2^{2h+1} - 1\} \to \{\vee, \wedge, 0, 1, p_0, \cdots, p_{n_0-1}, \bar{p}_0, \cdots, \bar{p}_{n_0-1}\}$$

is said to be a formula if the following conditions are satisfied.

1. If a is a node with an even height, then $f(a) = \vee$.
2. If a is a node with an odd height, then $f(a) = \wedge$.
3. If a is a leaf, then $f(a)$ is one of $0, 1, p_0, \cdots, p_{n_0-1}, \bar{p}_0, \cdots, \bar{p}_{n_0-1}$.

Obviously f can be interpreted as a Boolean formula of $p_0, \cdots, p_{n_0-1}$ in the usual sense. E.g. let f be defined on $\{1, 2, \cdots, 6, 7\}$ and $f(4) = p_3, f(5) = \bar{p}_4, f(6) = \bar{p}_5$ and $f(7) = p_6$. then f represents $(p_3 \wedge \bar{p}_4) \vee (\bar{p}_5 \wedge p_6)$.

For a theory of the thus formalized formulas see the discussion on complete normal $(\vee, \wedge)-$ formulas in [15].

Let B_0 be the set of all formulas. We make B_0 a Boolean algebra by defining the operations $\neg, \vee$ and $\wedge$ on B_0 as in [15].

Then we embed B_0 into B in the natural way and consider B_0 to be subalgebra of B.

Now we assume $NC^1 \neq P$, where NC^1 and P are non uniform NC^1 and P respectively. Then we have $B_0 \neq B$. Let $x \in B - B_0$. Define I_x by the equation

$$I_x = \{y \in B \mid \exists z \in B_o(z < x \wedge y \leq z)\}.$$

Then I_x is an M_0-complete ideal of B. We define $\tilde{I}_x = I_x \vee I_{\neg x} = \{z_1 \vee z_2 \mid z_1 \in I_x \text{ and } z_2 \in I_{\neg x}\}$. Then $\tilde{I}_x$ is again M_0-complete and $1 \notin \tilde{I}_x$.

Lemma 1.3. *Let* $C \in M$ *and* $b_0 = \bigwedge_{i \in C} p_i \wedge \bigwedge_{i \notin C} \bar{p}_i$.

Then $b_0 \in \tilde{I}_x$.

Proof. Since b_0 is a minimal nonzero element of B, $b_0 \wedge x = b_0$ or $b_0 \wedge x = 0$.

Remark 1.6 (Case 1). $b_0 \wedge x = b_0$. In this case we have $b_0 \leq x$ and $b_0 \in I_x$.

Remark 1.7 (Case 2). $b_0 \wedge x = 0$. In this case we have $b_0 \leq \neg x$ and $b_0 \in I_{\neg x}$.

Lemma 1.4. *Let $C \in M$ and $b_0 = \bigwedge_{i \in C} p_i \wedge \bigwedge_{i \notin C} \bar{p}_i$.*

If $b \in B - \tilde{I}_n$, then $b \wedge \neg b_0 \in B - \tilde{I}_x$.

Proof. Since $b \leq (b \wedge \neg b_0) \vee b_0$ we have

$$\begin{aligned} (b \wedge \neg b_0) \in \tilde{I}_x &\rightarrow (b \wedge \neg b_0) \vee b_0 \in \tilde{I}_x \\ &\rightarrow b \in \tilde{I}_x \end{aligned}$$

Lemma 1.5. *Let $D = \{b \in B \mid \exists i < n_0 (i \in C \wedge b \leq \bar{p}_i) \vee \exists i < n_0 (i \notin C \wedge b \leq p_i)\}$. Then D is dense over $\tilde{I}_x$*

Proof. Define b_i by the following equation

$$b_i = \begin{cases} b \wedge \bar{p}_i & : \text{ if } \ i \in C \\ b \wedge p_i & : \text{ otherwise} \end{cases} .$$

Then we have

$$\bigvee_{i < n_0} b_i = b \wedge \neg b_0 \notin \tilde{I}_x .$$

Therefore we have $\exists i < n_0 (b_i \notin \tilde{I}_x)$.

Now let G be an $\mathcal{M}$-generic maximal filter over $\tilde{I}_x$. Then we have $G \notin M$ in the same way as in Theorem 1.11.

2. $M[G]$ and $NP = co - NP$.

In this section we consider M and $M[G]$ as first order structures. Let ψ be a set of formulas with parameters from M.

Let I be an M_0-complete ideal of B and G be an $\mathcal{M}$- generic maximal filter over I.

Definition 2.1. *$M[G]$ is said to be a Ψ-extension of M if for every formula $\varphi(\mathbf{a})$ in Ψ the following property holds.*

$$\forall \mathbf{a} \in M (M \models \varphi(\mathbf{a}) \rightarrow M[G] \models \varphi(\mathbf{a})).$$

When Ψ is the set of all sharply bounded formulas, we denote Ψ-extension by sb-extension. When Ψ is the set of all bounded formulas, we denote Ψ-extension by bounded-extension. The following theorem is immediate from Theorem 1.8 in 1.

Theorem 2.1. *$M[G]$ is a sb-extension of M.*

As we discussed in 1., we can hardly expect that M[G] is a model of S_2 and we conjecture that $M[G]$ is not a model of S_2. In the same way, we conjecture that $M[G]$ is not a bounded-extension of M.

In the following we shall show that our conjectures imply $NP \neq co-NP$ therefore $P \neq NP$.

Theorem 2.2. *If $M[G]$ is not a model of S_2, then $NP \neq co - NP$ and therefore $P \neq NP$.*

Proof. Suppose that $NP = co{-}NP$ holds. Then there exists an NP-complete predicate $\exists x \leq t(a)A(x,a)$ with sharply bounded $A(x,a)$ and a sharply bounded $B(y,a)$ such that $\exists x \leq t(a)A(x,a) \leftrightarrow \forall y \leq s(a)B(y,a)$. Then there exists polynomial time computable functions f and g such that the following two sequents hold.

$$b \leq t(a), c \leq s(a), A(b,a) \rightarrow B(c,a)$$
$$f(a) \leq s(a) \supset B(f(a),a) \rightarrow g(a) \leq t(a) \wedge A(g(a),a).$$

It follows from Theorem 1.8 in 1. that these sequents also hold on $M[G]$. Therefore every bounded formula on $M[G]$ is equivalent to Σ_1^b formula on $M[G]$. This implies that $M[G]$ is a model of S_2, since $M[G]$ is a model of Σ_1^b-part of S_2^1.

Theorem 2.3. *If M[G] is not a bounded-extension of M, then $NP \neq co - NP$.*

Proof. Suppose $NP = co - NP$. Then every bounded formula is equivalent to Π_1^b formula. From the proof of Theorem 2.2 it follows that $NP = co - NP$ also holds on $M[G]$. From Theorem 1.8 in 1. it follows that $M[G]$ is an Π_1^b-extension of M. Therefore $M[G]$ is a bounded-extension which is a contradiction.

Definition 2.2. *A predicate $A(x)$ is said to be sparse, if there exists a term $t(a)$ satisfying the following condition.*

$$| \{x \mid A(x) \wedge x < a\} | \leq |t(a)|$$

where $| \{x \mid \varphi(x)\} |$ is the number of all x satisfying $\varphi(x)$. In this definition we are considering some structure e.g. M or $M[G]$ and notions defined on them.

Let $A(x)$ be a formula of S_2. We say that "$A(x)$ is sparse" is provable in S_2, if there exists a term in S_2 and the following formula is provable in S_2.

$$\exists w \leq BdSq(a,t(a))(Seq(w) \wedge \beta(1,w) = \mu x < aA(x)$$
$$\wedge Len(w) = |t(a)|$$
$$\wedge \forall i <| t(a) \mid (0 < i \supset \beta(i+1,w) = \mu x < a(\beta(i,w) < x \wedge A(x))$$
$$\wedge \forall x < a(A(x) \supset \exists i <| t(a) \mid (0 < i \wedge x = \beta(i,w)))$$

where BdSq, Seq, $\beta(i,w)$, Len are notations in [6] and the intended meaning of Seq(w), $\beta(i,w)$, Len(w) and BdSq($a,t(a)$) are "w is a number expressing a sequence", "i-th member of the sequence w", "the length of the sequence w", and an upperbound of all sequences whose members $\leq a$ and whose length $\leq |t(a)|$.

The meaning of the above formula is that one can emunerate all x satisfying $x < a \wedge A(x)$ according to its order. We denote the formula by

$$\exists w \leq \mathrm{BdSq}(a,t(a))B(w,a).$$

If A is a bounded formula, then B is also a bounded formula.

Theorem 2.4. *Let a bounded formula $A(a)$ be sparse and "$A(a)$ is sparse" be provable in S_2. If $a \in M[G] - M$ and $M[G] \models A(a)$, the $NP \neq co-NP$.*

Proof. Take $b \in M$ such that $a < b$. If $NP = co - NP$ then $M[G] \models S_2$. Therefore we have

$$M[G] \models \exists w \leq \mathrm{BdSq}(b,t(b))(B(w,b) \wedge \exists k < |t(b)|(a = \beta(k,w)).$$

Therefore there exists $k < |t(b)|$ satisfying

$$M[G] \models \exists w \leq \mathrm{BdSq}(b,t(b))(B(w,b) \wedge a = \beta(k,w))$$

Since M is a model of S_2, there exists $c \in M$ satisfying

$$M \models c < b \wedge \exists w \leq \mathrm{BdSq}(b,t(b))(B(w,b) \wedge c = \beta(k,w)).$$

Therefore there exists $w \in M$ satisfying

$$M \models w \leq \mathrm{BdSq}(b,t(b)) \wedge B(w,b) \wedge c = \beta(k,w),$$

If $NP = Co - NP$, then $M[G]$ is a bounded extension of M. Therefore the following holds

$$M[G] \models w \leq \mathrm{BdSq}(b,t(b)) \wedge B(w,b) \wedge c = \beta(k,w).$$

This implies that $c = a$ holds on $M[G]$ which is a contradiction.

3. Proper class forcing.

Now we shall consider a bigger Boolean algebra. The Boolean algebra $\tilde{B}$ is the set of b which is a sequence $(X_0, X_1, \cdots, X_v)$ with $r \in M_0$ satisfying one of the following conditions.

1. X_i is p_j with $j \in M_0$.
2. X_i is $\bar{p}_i$ with $j \in M_0$.
3. X_i is $(\wedge, Y_0, \ldots, Y_s)$ or $(V, Y_0, \ldots, Y_s)$.

where $Y_j (j \leq s)$ is one of $X_0, X_1, \ldots, X_{i-1}$. The difference between B and $\tilde{B}$ is that p_j or $\bar{p}_i$ are restricted to $j < n_0$ in B but there are no such restriction in $\tilde{B}$. Even for $\tilde{B}$. $b \in \tilde{B}$ is $\Delta_1^1(BD)$ and $b \in \tilde{B}$ implies $b \in N$.

We can define $\neg b$, $\bigvee_{i \leq t} b_i$ and $\bigwedge_{i \leq t} b_i$ as before for members b, b_i in $\tilde{B}$.

For every $b \in \tilde{B}$, there exists $\delta \in M_0$ such that if p_i or $\bar{p}_i$ occurs in b, then $i < \delta$. Such δ is called a bound for b. Let δ be a bound for b and $A \in M$ be a subset of $\{0, \ldots, \delta - 1\}$. Then A gives a truth value to $p_0, \ldots, p_{\delta-1}$ as before and is called an atom evaluation of b.

As before we define $b_1 \overset{\tilde{B}}{=} b_2$ for $b_1, b_2 \in \tilde{B}$ by $\forall A$ atom evaluation $(\text{eval}(A, b_1) = \text{eval}(A, b_2))$. We can take only A which is a subset of $\{0, 1, \ldots, \delta - 1\}$ and δ is a bound for both b_1 and b_2. Therefore $b_1 \overset{\tilde{B}}{=} b_2$ is $\Pi_1^1(BD)$ in (M_o, M).

We define $[[\varphi]]$ for $\Sigma_1^1(BD)$ formula φ, $\check{X}$ for $X \in M$, an ideal I of $\tilde{B}$, a dense definable set over I, M_0-completeness of an ideal I, and M in the same way as before.

Now we are going to define M_0 complete ideals $\tilde{I}_0$ and $\tilde{I}_k$ of $\tilde{B}$.

For $\delta \in M_0$, B_δ be the subset of $\tilde{B}$ which consists of the element b whose bound is δ. Then $\tilde{B} = \bigcup_{\delta \in M_0} B_\delta$. Now for $b \in B_\delta$, we define $\tilde{m}(b)$ by

$$\tilde{m}(b) = \frac{|\{a < 2^\delta | \text{eval}(a, b) = 1|\}|}{2^\delta}$$

Then the value $\tilde{m}(b)$ does not depend on δ if δ is bound for b.

We define $\tilde{I}_0$ by

$$\tilde{I}_0 = \{b \in \tilde{B} \mid \forall \alpha \in M_0 (\alpha \tilde{m}(b) < 1)\} \quad \text{and} \quad I_\delta = \tilde{I}_0 \cap B_\delta.$$

We are going to show that $\tilde{I}_0 = \bigcup_{\delta \in M_0} I_\delta$ is M_0-complete.

Let $X : y \to \tilde{I}_0$. Then $\forall x < y (X(x) \in \tilde{I}_0)$. Then for every $x < y$, define $\alpha(x)$ to be the minimum α such that $\alpha \tilde{m}(X(x)) \geq 1$. Then $\alpha(y) \notin M_0$. Define $\alpha_0 = \min\{\alpha(x) \mid x < y\} - 1$. Then $\alpha_0 \notin M_0$ and $\forall x < y (\alpha_0 m(X(x)) < 1)$.

For any $\alpha \in M_0$ we have

$$\alpha \tilde{m}(\bigvee_{x<y} X(x)) \leq \alpha \sum_{x<y} \tilde{m}(X(x)) < \alpha y \frac{1}{\alpha_0} < 1.$$

Therefore $\bigvee_{x<y} X(x) \in \tilde{I}_0$.

Now we are going to generalize $\tilde{I}_0$ to $\tilde{I}_k$. Let K be definable in N.

Let $\mu \in N - M$ be fixed. We define

$$K_\mu = \{a \in K \mid a < 2^\mu\}.$$

For $b \in \tilde{B}$, we define $\tilde{m}_K(b)$ by the equation

$$\tilde{m}_K(b) = \frac{|\{a \in K_\mu \mid \mathrm{eval}(a,b) = 1\}|}{|K_\mu|}$$

and $\tilde{I}_K$ by the equation

$$\tilde{I}_K = \{b \in \tilde{B} | \exists \alpha \notin M_0 (\tilde{m}_K(b) \leq \frac{1}{\alpha})\}$$

For $K = N$, $\tilde{I}_k$ coincides with $\tilde{I}_0$. Now we are going to show that $\tilde{I}_k$ is M_0-complete.

Let $X : y \to \tilde{B}$ and $\forall x < y (X(x) \in \tilde{I}_k)$.

Consider the following value for $x < y$

$$|\{a \in K_\mu \mid \mathrm{eval}(a, X(x)) = 1\}|.$$

Let m be the maximum of them. Then there exists $\alpha_0 \notin M_0$ such that

$$\frac{m}{|K\mu|} \leq \frac{1}{\alpha_0}$$

Therefore there exists $\alpha \notin M_0$ such that

$$\alpha y \leq \alpha_0.$$

then we have $\tilde{m}_k(\bigvee_{x<y} X(x)) \leq \frac{1}{\alpha}$.

Remark 3.1. As before the definability of K is not necessary. For general $K \subseteq N$, we define

$$\begin{aligned}\tilde{I}_K = \{b \in \tilde{B} \mid \forall V, W \subseteq 2^\mu \exists \alpha \notin M_o (V \subseteq K_\mu \subseteq W \\ \wedge (V, W \quad \text{are definable in} N) \supset \\ \frac{|\{a \in V \mid \mathrm{eval}(a,b) = 1\}|}{|w|} \leq \frac{1}{\alpha})\}\end{aligned}$$

Everything goes in the same way as in the definable case.

We define $M^{\tilde{B}}, [[\varphi]], \check{X}, \tilde{\mathcal{M}}, G$ etc. in the same way as before. Then the theorems in 1. and 2. can be proved in the same way by just changing B to $\tilde{B}$ and $\mathcal{M}$ to $\tilde{\mathcal{M}}$.

Let δ_0, $\delta_1 \in M_0$ and $\delta_0 < \delta_1$. We define

$$\Omega(\delta_0,\delta_1) = \{b \in \tilde{B} \mid b = q_{\delta_0} \wedge q_{\delta_0+1} \wedge \ldots \wedge q_{\delta_1 -1} \text{ where } q_i \text{ is } p_i \text{or } \bar{p}_i\}$$

The following lemma is obvious.

Lemma 3.1. *If* $2^{\delta_1-\delta_0} \in M_0$*, then*

$$\forall b \in \Omega(\delta_0,\delta_1)(b \in \tilde{I}_0).$$

Theorem 3.1. *Let* G *be an* $\tilde{\mathcal{M}}$ *generic maximal filter over* $\tilde{I}_k$*. Then we have*

$$\forall b \in \Omega(\delta_0,\delta_1)(b \in \tilde{I}_k) \rightarrow A = \{i \mid \delta_0 \leq i < \delta_1 \wedge p_i \in G\} \notin M$$

Proof. Let $C \in M$ an $C \subseteq [\delta_0,\delta_1)$.
We define

$$D = \{Y \in \tilde{B} \mid \exists i \in C(Y \leq \neg p_i) \vee \exists i \notin C(Y \leq p_i)\}.$$

We claim that D is dense over $\tilde{I}_k$. Let $b \in \tilde{B} - \tilde{I}_k$. Then we have

$$\exists \alpha \in M_0(\tilde{m}_K(b) > \frac{1}{\alpha}).$$

Define b_i by the equation
$$b_i = \begin{cases} b \wedge \neg p_i & : \text{ if } i \in C \\ b \wedge p_i & : \text{ otherwise} \end{cases}.$$

Define $C' = [\delta_0,\delta_1) - C$.

$$\begin{aligned} \tilde{m}_K(\bigvee_{\delta_0 \leq i < \delta_1} b_i) &= \tilde{m}_K(b \wedge (\bigvee_{i \in C} \bar{p}_i \vee \bigvee_{i \in C'} p_i)) \\ &= \tilde{m}_K(b \wedge \neg(\bigwedge_{i \in C} p_i \wedge \bigwedge_{i \in C'} \bar{p}_i)) \\ &\geq \tilde{m}_K(b) - \tilde{m}_K(\bigwedge_{i \in C} p_i \wedge \bigwedge_{i \in C'} \bar{p}_i) \end{aligned}$$

Since $\bigwedge_{i \in C} p_i \wedge \bigwedge_{i \in C'} \bar{p}_i \in \tilde{I}_k$, we have

$$\exists \alpha \notin M_0(\tilde{m}_K(\bigwedge_{i \in C} Pi \wedge \bigwedge_{i \in C'} \bar{p}_i) < 1/\alpha).$$

Therefore we have $\bigvee_{\delta_0 \leq i < \delta_1} b_i \notin \tilde{I}_K$. Since $\tilde{I}_k$ is M_0-complete, we have $\exists i \in [\delta_0,\delta_1)(b_i \notin \tilde{I}_k)$. Since $b_1 \leq b$ and $b_1 \in D$, D is dense over $\tilde{I}_K$.
Since G is $\tilde{m}$-generic, $G \cap D \neq \emptyset$. Let $a \in G \cap D$.

Remark 3.2 (Case 1). $\exists i \in C(a \leq \bar{p}_i)$. Then $\bar{p}_i \in G$. Therefore $i \notin A$ and $A \neq C$.

Remark 3.3 (Case 2). $\exists i \in C'(a \leq p_i)$. In this case $p_i \in G$ and $i \in A$. Therefore $A \neq C$. Therefore $A \neq C$ for any $C \in M$. Therefore $A \notin M$.

References

1. M. Ajtai, *The complexity of the pigeon hole principle,* Proc. IEEE 29th Annual Symp. Foundation of Computer Science, 1988, 346-355,
2. M. Ajtai, *Parity and the pigeon hole principle,* Feasible Mathematics, editors: S.R. Buss and P.J. Scott, Birkhauser, 1-24 1990
3. M. Ajtai, *The independence of the modulo p counting principles,* Proc. of the 26th Annual ACM Symp. on Theory of Computing, 402-417, ACM Press, 1994,
4. P. Beame, R. Impagliazo, J. Krajíček, T. Pitassi, and P. Pudlák, Lower bounds on Hilbert's Nullstellensatz and, propositional proofs, to appear.,
5. P. Beame, R. Impagaliazzo, J. Krajíček, T. Pitassi, and P. Pudlák and A. Woods, *Exponential lower bounds for the pigeon hole principle,* Proc. of the 24th Annual ACM Symp. on Theory of Computing, 200-221, ACM Press, 1992,
6. S. Buss, Bounded Arithmetic, Bibliopolis, Napoli, 1986,
7. K. Gödel, *A letter to von Neumann,* Arithmetic, Proof Theory, and Computational Complexity, editors: P. Clote and J. Krajíček, Oxford University Press, 1993,
8. J. Krajíček, *On Frege and Extended Frege Proof Systems,* Feasible Mathematics II., editors: P. Clote and J.B. Remmel, Birkhaüser, 1995, 284-319,
9. J. Krajíček, *Bounded, Propositional Logic, and Complexity Theory,* Cambridge University Press, 1995,
10. J.B. Paris and A. Wilkie, *Counting problems in bounded arithmetic,* Methods in Mathematical Logic, LNM 1130, 317-340, Springer Verlag, 1985,
11. S. Riis, *Making Infinite Structures Finite in Models of Second Order Bounded Arithmetic,* Arithmetic, Proof Theory, and Computational Complexity, editors: P. Clote and J. Krajíček, Oxford University Press, 289-319,
12. G. Takeuti, Two Applications of Logic to Mathematics, Princeton University Press, 1978,
13. G. Takeuti, *RSUV Isomorphisms,* Arithmetic, Proof Theory, and Computational Complexity, editors: P. Clote and J. Krajíček, Oxford University Press, 364-386,
14. G. Takeuti, *RSUV Isomorphisms for TAC^i, TNC^i and TLS,* Arch. Math. Logic, 427-453, 1995,
15. G. Takeuti, *Frege proof System and TNC^o,* to appear in J. Symbolic Logic.