Redeveloping Takeuti-Yasumoto forcing

Satoru Kuroda

GPWU, Gunma, Japan

9, September, 2017
CTFM 2017

Forcing in Bounded Arithmetic

- Forcing was introduced in bounded arithmetic by Paris-Wilkie proving the relativized independence of the pigeonhole principle, followed by Ajtai and Riis.
- Krajíček gave several forcing construction for PTIME theories in a different context.
- Takeuti and Yasumoto succeeded in building a theory of Boolean valued models in bounded arithmetic.
- We will give a reformulation of Takeuti-Yasumoto forcing in two-sort bounded arithmetic.
- Correct proofs are given for some theorems of Takeuti-Yasumoto.
- T-Y forcing method can be applied to other complexity classes such as NC^1.
- We wil also discuss relations to Krajíček's forcing.

Forcing in Bounded Arithmetic : An Overview

Paris-Wilkie used forcing argument to prove a relativized independence of the Pigeonhole Principle from weak system of arithmetic

Theorem (Paris-Wilkie)

There exists a model $(M, R) \models I\exists_1(R)$ *in which* R *is a bijection from* $n+1$ *to* n *for some* $n \in M$*.*

The construction of R uses a simple back-and-force argument but can be regarded as a forcing construction.
Ajtai uses a similar idea to prove a stronger result

Theorem (Ajtai)

There exists a model $(M, R) \models I\Delta_0(R)$ *in which* R *is a bijection from* $n+1$ *to* n *for some* $n \in M$*.*

Ajtai's construction resembles to Cohen style forcing; R is defined as a generic in the forcing condition

$$\mathcal{P} = \{f \subset n+1 \to n \ : \ |f| < n^{1-\epsilon} \text{ for some } \epsilon > 0\}.$$

However the proof requires a difficult argument which utilizes special type of switching lemma.

Krajíček Forcing

- Paris-Wilkie-Ajtai forcing gives a only relativized result.
- On the other hand, Krajíček introduced a different view in forcing construction.
- Krajíček's idea is to construct a models of weak arithmetic having particular properties starting from a nonstandard model with some assumption in computational complexity or proof complexity.

Theorem (Krajíček)

Let $M \models PV + NP \not\subseteq P/poly$. Then there exists a Π_1^B-elementary extension M' in which $NP \not\subseteq co\text{-}NP$.

Theorem (Krajíček)

Let $M \models V^1$ in which there is no EF-proof of a propositional formula τ. Then there exists a Π_1^B-elementary extension $M' \models V^1$ in which $\neg\tau$ is satisfiable.

Takeuti-Yasumoto forcing

- In two consecutive papers, Takeuti and Yasumoto gave a construction of generic models of Bounded Arithmetic which is a disguise of Boolean valued models in set theory.
- Their construction is inspired by the previous forcing arguments but the motivation is rather different.
- Namely, they tried to relate the separation problem in the standard world to the generic models.
- However, we are interested in the technical aspects of Takeuti-Yasumoto forcing so we ignore their original motivations.
- Our motivation is to give a general framework for forcing in bounded arithmetic based on Takeuti-Yasumoto's approach.

Basic Bounded Arithmetic

One-sort systems (Buss)

- Language:
  First order language L_A comprises

$$0,\ s_0(x) = 2x,\ s_1(x) = 2x+1, x+y,\ x \cdot y,\ \lfloor x/2 \rfloor,$$
$$|x| = \lceil \log(x+1) \rceil,\ x\#y = 2^{|x|\cdot|y|}.$$

- Quantifiers and classes of formulas
  $\forall x < |t|$, $\exists x < |t|$: sharply bounded quantifiers
  $\forall x < t$, $\exists x < t$: nonsharply bounded quantifiers
  Σ_i^b is the set of L_A formulas with $\leq i$ alternations of nonsharply bounded quantifiers starting with an existential quantifier.
  Π_i^b is defined dually.
- Connections with complexity classes
  Σ_0^b formulas are polynomial time predicates
  Σ_1^b and Π_1^b are exactly NP and co-NP predicates resp.

Basic Bounded Arithmetic

Two-sort systems (Cook-Nguyen)

- Language:
  Two-sort language L_A^2 comprises number variables $x, y, z, \ldots$, string variables $X, Y, Z, \ldots$ and

$$0,\ x+y,\ x\cdot y,\ |X|,\ x\in X.$$

- Quantifiers and classes of formulas
  $\forall x < t, \exists x < t$: bounded number quantifiers
  $\forall X < t \equiv \forall X(|X| < t \to \cdots), \exists X < t \equiv \exists X(|X| < t \wedge \cdots)$: bounded string quantifiers
  Σ_i^B is the set of L_A^2 formulas with $\leq i$ alternations of bounded string quantifiers starting with an existential quantifier.
  Π_i^b is defined dually.
- Connections with complexity classes
  Σ_0^B formulas are FO predicates
  Σ_1^B and Π_1^B are exactly NP and co-NP predicates resp.

Theories for the Polynomial Hierarchy

Definition (Buss)

For $i \geq 0$, S_2^i is the L_A-theory whose axioms are defining axioms for L_A symbols together with
Σ_i^b-PIND : $\varphi(0) \wedge \forall x\, (\varphi(\lfloor x/2 \rfloor) \to \varphi(x)) \to \forall x \varphi(x), \quad \varphi(x) \in \Sigma_i^b$.

Definition (Cook-Nguyen)

For $i \geq 0$, V^i is the L_A^2-theory whose axioms are defining axioms for L_A^2 symbols together with
Σ_i^B-COMP : $\forall a\, (\exists X < a \forall y < a (y \in X \leftrightarrow \varphi(y)), \quad \varphi(x) \in \Sigma_i^B$.

Proposition

V^0 proves Σ_i^B-IND $\leftrightarrow$ Σ_i^B-COMP.

Theorem (Buss, Cook-Nguyen)

For $i \geq 1$, A function is computable in $P^{\Sigma_i^p}$ if and only if it is Σ_i^b definable in S_2^i if and only if it is Σ_i^B definable in V^i.

RSUV isomorphism

Theorem (Takeuti, Razborov)

There are translations $\varphi^{\#} \in \Sigma^B_\infty$ for $\varphi \in \Sigma^b_\infty$ and $\psi^\flat \in \Sigma^b_\infty$ for $\psi \in \Sigma^B_\infty$ such that

- *if $S^i_2 \vdash \varphi$ then $V^i \vdash \varphi^{\#}$,*
- *if $V^i \vdash \psi$ then $S^i_2 \vdash \psi^\flat$,*
- *if $(\varphi^{\#})^\flat = \varphi$ and $(\psi^\flat)^\varphi = \psi$.*

This theorem is more intuitively understood in a model theoretical manner.
An L^2_A-structure consists of a pair (M_0, M) of universes where M_0 is a set of numbers and M is a set of strings. Then

Theorem

If $(M_0, M) \models V^i$ then $M \models S^i_2$ where each element of M is regarded as number in binary. Conversely, if $M \models S^i_2$ and $M_0 = \{|x| : x \in M\}$ then $(M_0, M) \models V^i$.

Theories for polynomial time

Definition

Let L_{PV} be the language which consists of function symbols for polynomial time functions. PV denotes the L_{PV}-theory whose axioms are defining axioms for symbols together with open induction.

Definition (Cook-Nguyen)

VP is the L_A^2-theory V^0 extended by a single axiom MCV which expresses that any monotone circuits can be evaluated.

Proposition

PV is a conservative extension of VP. V^1 is $\forall\Sigma_1^B$ conservative over VP.

The following result is known as KPT witnessing:

Theorem (Krajíček-Pudlák-Takeuti, Buss)

If $VP = V^1$ then VP proves that $PH = NP/poly$.

Basic definitions for T-Y forcing

Let $M \models Th(\mathbb{N})$ be countable nonstandard, $n \in M \setminus \omega$ and $n_0 = |n|$. Define

$$M^* = \{x \in M : x \leq \underbrace{n \# \cdots \# k}_{k} \text{ for some } k \in \omega\}$$

and $M_0^* = \{|x| : x \in M^*\}$.

We define the Boolean algebra
$\mathbb{B}_C = \{C \in M^* : C \text{ is a circuit with } n_0 \text{ inputs}\}$.

For $C, C' \in \mathbb{B}_C$, $C \leq C' \Leftrightarrow \forall X\, (|X| = n \rightarrow eval(C, X) \leq eval(C', X))$.

An ideal $I \subseteq \mathbb{B}_C$ is M_0-complete if it is closed under $\bigvee_{i<a}$ with $a \in M_0$.

A set $D \subseteq \mathbb{B}_C$ is dense over I if for all $X \in \mathbb{B}_C \setminus I$ there is $Y \in D \setminus I$ such that $Y \leq X$.

A maximal filter $G \subseteq \mathbb{B}_C$ is $\mathcal{M}$-generic over I if for any D dense over I and definable in M, $(D \setminus I) \cap G \neq \emptyset$.

Generic model

$M^{\mathbb{B}_C} = \{X \in M^* : X : a \to \mathbb{B}$ for some $a \in M_0^*\}$. i.e. $M^{\mathbb{B}_C}$ is the set of sequences of circuits.

For $X : a \to \mathbb{B}_C$ and $\mathcal{M}$-generic maximal filter G, define $i_G(X) = \{x < a : X(x) \in G\}$.

(String part of) Generic Model is defined as $M[G] = \{i_G(X) : X \in M^{\mathbb{B}_C}\}$

As in set theory, we can show that

Lemma

If G is $\mathcal{M}$-generic then $M^* \subseteq M[G]$.

Since all strings in $M[G]$ are of length $a \in M_0^*$, we may regard $(M_0^*, M[G])$ as a L_A^2-structure.
Takeuti and Yasumoto gave several examples of M_0-complete ideals I so that $M^* \subsetneq M[G]$.

Forcing theorem

We have a translation of $\varphi(\bar{x}, \bar{X}) \in \Sigma_0^B$ into a propositional formula such as Paris-Wilkie translation. We fix such a translation and denote by $[\![\varphi(\bar{x}, \bar{X})]\!]$. Then we have a forcing theorem for Σ_0^B formulas.

Theorem

Let $\varphi(\bar{x}, \bar{X}) \in \Sigma_0^B$, $\bar{x} \in M_0^*$ and $X_i : a \to M^{\mathbb{B}_C}$. If G is a $\mathcal{M}$-generic over some M_0-complete ideal $I \subseteq \mathbb{B}_C$ then

$$(M_0^*, M[G]) \models \varphi(\bar{x}, i_G(X_1), \ldots, i_G(X_k)) \Leftrightarrow [\![\varphi(\bar{x}, X_1, \ldots, X_k)]\!] \in G.$$

Since $\mathbb{B}_C$ is closed under polynomial time functions, we also have

Theorem

$(M_0^*, M[G]) \models VP$.

Remark

Note that any open PV-formula can be represented by circuits. So we assume that there is a translation of open PV-formulas in $\mathbb{B}_C$.

Relating Generic model and $P = NP$

Theorem (Takeuti-Yasumoto,K)

If $P = NP$ then for any M_0-complete ideal $I \subseteq \mathbb{B}_C$ and $\mathcal{M}$-generic maximal filter G over I, $(M_0^*, M[G]) \models \Sigma_1^B$-COMP, i.e. $M[G] \models S_2^1$.

(Proof Sketch). If $P = NP$ is true then for any Σ_1^b formula $\exists Z < t\, \varphi(x, X, Z)$, we can compute the witness Z by a polynomial time function $F(x, X)$ using binary search. The function $F(x, X)$ can be represented in (M_0^*, M^*) by a sequences $C_0^x, \ldots, C_t^x$ of circuits in $\mathbb{B}_C$. Then we can construct $Y : a \to \mathbb{B}_C$ such that for all $x < a$,

$$Y(x) \in G \Leftrightarrow \text{ there is } Z : t \to \mathbb{B}_C \text{ such that } [\![\varphi(x, X, Z)]\!] \in G.$$

For each $x < a$, $C_{x,X} : t \to \mathbb{B}_C$ be such that $C_{x,X}(i) = C_i^x(X)$ and set

$$Y(x) = [\![\varphi(x, X, C_{x,X})]\!].$$

Generic model and $NP \neq co\text{-}NP$

Krajíček considers the problem of extending the model of $VP + P \neq NP$ to a model of VP in which $NP \neq co\text{-}NP$.
The construction of generic model by Krajíček can be obtained by T-Y forcing.

Theorem (Krajíček, K)

If $(M_0^*, M^*) \models NP \not\subseteq P/poly$ then there exists an M_0-complete ideal $I \subseteq \mathbb{B}_C$ such that $(M_0^*, M[G]) \models NP \not\subseteq co\text{-}NP$.

(Proof Sketch).
Let $Sat_n(X)$ denote the formula "X is a satisfiable formula with n inputs".
Suppose that $(M_0^*, M^*) \models P \not\subseteq P/poly$. Then $Sat_{n_0}(X)$ is not computed by a circuit in (M_0^*, M^*) for some $n_0 \in M_0^*$.
We construct a chain $M^* = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ inductively. Assume that we have constructed M_i and let $\varphi(X, Z) \in \Sigma_0^B$ be such that $\exists Z < t(|X|)\, \varphi(X, Z)$ represents a Σ_1^B complete predicate withe parameters from M_i. Let $\bar{p} = p_0, \ldots, p_{n_0}$ and define

$$T = \{\neg[\![W \models \bar{p}]\!] : W : n_0 \to \mathbb{B}_C\} \cup \{[\![\varphi(\bar{b}, Z)]\!] : Z : t(n_0) \to \mathbb{B}_C\}.$$

Generic model and $NP \neq co\text{-}NP$

T is consistent in (M_0^*, M^*), i.e. there is no $T' \subseteq T$ such that $|T'| \in M_0^*$ and $(M_0^*, M^*) \models \exists P\,(P$ is an EF-proof of $\bigwedge T \to)$.

From now, we switch the partial order on $\mathbb{B}_C$ to

$$X \leq X \Leftrightarrow \exists P\,(P \text{ is an EF-proof of } X \to X').$$

Lemma (K)

If $T \subseteq \mathbb{B}_C$ is consistent then there exists a M_0-complete ideal $I \subseteq \mathbb{B}_C$ such that $T \subseteq G$ whenever G is $\mathcal{M}$-generic over I.

(Proof). Define the M_0-complete ideal I_T by

$$I_T = \{C \in \mathbb{B}_C : T \cup \{C\} \text{ is inconsistent}\}.$$

Let $X \in T$ and define $D_X = \{Z \in \mathbb{B}_C : Z \leq X\}$.

Claim: D_X is dense over I_T.

Generic model and $NP \neq co\text{-}NP$

Claim: D_X is dense over I_T.

To see this, let $Y \in \mathbb{B}_C \setminus I_T$. Then $T \cup \{Y\}$ is consistent. So we have $X \wedge Y \leq X$ and $X \wedge Y \leq Y$. Since $X \wedge Y \notin I$ we have the claim.

Let G be $\mathcal{M}$-generic over I_T. Then there is $Z \in G \cap D_X$ and since G is upward closed, $X \in G$.
Let $M^{i+1} = M^i[G]$ be the generic model obtained form M^i. Since

$$T = \{\neg[\![W \models \bar{p}]\!] : W : n_0 \to \mathbb{B}_C\} \cup \{[\![\varphi(\bar{b}, Z)]\!] : Z : t(n_0) \to \mathbb{B}_C\} \subseteq G$$

we have

$$(M_0^*, M^i[G]) \models \neg Sat_{n_0}(i_G(\bar{p})) \wedge \forall Z < t(n_0)\varphi(i_G(\bar{p}), Z).$$

where φ contains parameters from M^i. So repeating this construction, we have the claim of the theorem.

Generic model satisfying Σ_1^B induction

Krajíček gave a construction of a generic model of Σ_1^B-IND based on the forcing notion.
A set $S \subseteq \mathbb{B}_C$ is I-consistent if there is no EF proof of 0 from S.

$$\mathcal{P} = \{S \subseteq \mathbb{B}_C : \quad S \text{ is definable in } M \text{ and } S \text{ is } I\text{-consistent for some } I \in M_0 \setminus M_0^*\}.$$

$\mathcal{P}$ is partially ordered with the reverse inclusion.
A set $\mathcal{D} \subseteq \mathcal{P}$ is definable if there exists a formula $\varphi(S)$ where S is a extra predicate symbol such that

$$\mathcal{D} = \{S \in \mathcal{P} : (M_0, M) \models \varphi(S)\}.$$

$\mathcal{D}$ is dense in $\mathcal{P}$ if for all $S \in \mathcal{P}$ there exists $S' \in \mathcal{D}$ such that $S' \leq_{\mathcal{P}} S$.
$\mathcal{G} \subseteq \mathcal{P}$ is $\mathcal{P}$-generic if it intersects with any dense definable subset of $\mathcal{P}$.

Remark

- *The generic extension $M[G]$ is defined as for T-Y forcing.*
- *It is easily seen that we can take $\mathcal{G}$ so that $G = \cup\mathcal{G}$ is a maximal filter.*

Generic model satisfying Σ_1^B induction

Theorem (Krajíček)

If $\mathcal{G}$ is $\mathcal{P}$-generic and $G = \cup\mathcal{G}$ then $(M_0^*, M[G]) \models \Sigma_1^B$-IND. Moreover, there is no EF-proof of τ in (M_0^*, M^*) then

$$(M_0^*, M[G]) \models Sat(\neg\tau).$$

The fact that $(M_0^*, M[G]) \models \Sigma_1^B$-IND follows from the following observation:

Lemma

Let $S \subseteq \mathbb{B}_C$ be a l-consistent set, $\varphi(x, Z) \in \Sigma_0^B$ and $a \in M_0^*$. Then at least one of the following sets is $l^{1/3}$-consistent:

- $S \cup \{\neg[\![\varphi(0, Z)]\!] : Z : a \to \mathbb{B}_C\}$.
- $S \cup \{[\![\varphi(a, Z)]\!]\}$ *for some* $Z : a \to \mathbb{B}_C$.
- $S \cup \{[\![\varphi(x, Z)]\!]\} \cup \{\neg[\![\varphi(x+1, Z)]\!] : Z : a \to \mathbb{B}_C\}$. *for some* $x < a$ *and* $Z : a \to \mathbb{B}_C$.

Generic model satisfying Σ_1^B induction

$G = \cup\mathcal{G}$ in the previous slide can be obtained as a $\mathcal{M}$-generic in the sense of Takeuti-Yasumoto.

Theorem (K)

There is an M_0-complete ideal $I \subseteq \mathbb{B}_C$ such that if $\mathcal{G}$ is $\mathcal{P}$-generic then $G = \cup\mathcal{G}$ is $\mathcal{M}$-generic over I.

(Proof). Define an M_0-complete ideal

$$I_{\mathcal{P}} = \{X \in \mathbb{B}_C : \quad \text{there exists } S \text{ such that } \{X\} \cup S \text{ is } I\text{-inconsistent for some } I \in M_0^*\}$$

Let $\mathcal{G}$ be $\mathcal{P}$-generic. We show that $G = \cup\mathcal{G}$ is $\mathcal{M}$-generic over $I_{\mathcal{P}}$. Let D be dense over $I_{\mathcal{P}}$ and define

$$\mathcal{D} = \{S \in \mathcal{P} : S \cap (D \setminus I_{\mathcal{P}}) \neq \emptyset\}.$$

Claim: $\mathcal{D}$ is dense in $\mathcal{P}$.

Let $S \in \mathcal{P}$. If $S \notin \mathcal{D}$ then $S \cap D = \emptyset$. So there exists $X \in S \setminus I_{\mathcal{P}}$ such that $X \notin D$. Since D is dense over $I_{\mathcal{P}}$, we have $X' \in D \setminus I_{\mathcal{P}}$ such that $X' \leq X$.

Generic model satisfying Σ_1^B induction

We claim that $S' = \{X'\} \cup S \in \mathcal{D}$.

$S' \cap (D \setminus I_{\mathcal{P}}) \neq \emptyset$ is trivial.

To show that $S' \in \mathcal{P}$, notice that $X' \notin I_{\mathcal{P}}$. so $\{X'\} \cup S$ is I-consistent for all S and $I \in M_0^*$.

Fix one such S. Note that S is definable in M. So by overspill, there exists $I \in M_0 \setminus M_0^*$ such that $\{X'\} \cup S$ is I-consistent. Thus we have $S' \in \mathcal{P}$.

By Claim we obtain $\mathcal{G} \cap \mathcal{D} \neq \emptyset$ and so $G \cap (D \setminus I_{\mathcal{P}}) \neq \emptyset$.

Corollary

There is an M_0-complete ideal $I \subseteq \mathbb{B}_C$ and an $\mathcal{M}$-generic G over I such that $(M_0, M[G]) \models \Sigma_1^B$-COMP. Moreover, if a propositional formula τ does not have a EF proof in (M_0^*, M^*) then $(M_0^*, M[G]) \models Sat(\neg\tau)$.

Summary and Open Problems

We have proved that

Theorem

Let G be $\mathcal{M}$-generic over M_0-complete ideal $I \subseteq \mathbb{B}_C$. If $P = NP$ then $(M_0^*, M[G]) \models \Sigma_1^B$-IND.

and

Theorem

There exists an M_0-complete ideal I and $\mathcal{M}$-generic G over I such that $(M_0^*, M[G]) \models \Sigma_1^B$-IND.

On the other hand, it is hard to construct a model violating Σ_1^B-IND without assumptions since it implies $P \neq NP$.
So we might expect to prove the existence of such a model under some natural assumption and we conjecture the following.

Problem

Show that if $P \neq NP$ then there exists an M_0-complete ideal such that $(M_0^*, M[G]) \not\models \Sigma_1^B$-IND whenever G is $\mathcal{M}$-generic over I.

Summary and Open Problems

As we have seen, generic models also have relations with Propositional Proofs.
Intuitively, $\mathbb{B}_C$ corresponds to extended Frege proofs. So it seems that the following problem arises naturally.

Problem

Show that if Extended Frege system is not super then there is an M_0-complete ideal I such that $(M_0^*, M[G]) \models TAUT \not\in \Sigma_1^B$ whenever G is $\mathcal{M}$-generic over I.

One of the main goals is to show that certain combinatorial principles are independent from weak systems. That is

Problem

Let Φ denote some combinatorial principle in NP or beyond. Show that there exists a generic model $(M_0^*, M[G]) \models \neg\Phi$ under the assumption $P \neq NP$.

References

- J. Krajíček, On Frege and Extended Frege Proof Systems. in:Feasible Mathematics II, Birkhäuser, (1995) pp.284–319.
- G. Takeuti and M. Yasumoto, Forcing on Bounded Arithmetic. in:Gödel '96, Lecture Notes in Logic, vol.6, (1996) pp.120–138.
- G. Takeuti and M. Yasumoto, Forcing on Bounded Arithmetic II. JSL, vol.63(3) (1998), pp.860–868.