On Takeuti-Yasumoto forcing

Satoru Kuroda

Gunma Prefectural Women's University

Logic Colloquium 2019

Outline of this talk

We apply the forcing construction à la Takeuti and Yasumoto (1996) to construct generic extensions for subclasses of PTIME; NC^1 and NL.

Outline of this talk

We apply the forcing construction à la Takeuti and Yasumoto (1996) to construct generic extensions for subclasses of PTIME; NC^1 and NL.

Then we discuss the problem of relating separation problems in computational/proof complexity to properties of generic extensions.

Subclasses of PTIME

Many complexity classes are define inside PTIME:

- AC^0=constant depth polynomial size Boolean circuits
- $NC^1 = ALOGTIME$: $O(\log n)$-time bounded alternating TMs
- L=$O(\log n)$-space bounded DTMs
- NL=$O(\log n)$-space bounded NTMs

However, no separations are known above AC^0:

$$AC^0 \subsetneq NC^1 \subseteq L \subseteq NL \subseteq P \subseteq NP.$$

Two-sort Bounded Arithmetic

Two-sort language comprises

- number variables : $x, y, z, \ldots$,
- string variables : $X, Y, Z, \ldots$,
- functions and predicates : $Z(x) = 0$, $x + y$, $x \cdot y$, $|X|$, $x \in X$, $x \leq y$.

Two-sort structures consist of pairs of universes (M_0, M) where M_0 is the number part and M is the string part.

$\Sigma^B_0 =$ formulas with only bounded number quantifiers,

Σ^B_i, Π^B_i are defined by counting the alternations of bounded string quantifier.

Two-sort theories

$\forall\Sigma^B_1$-theorems of bounded arithmetic theories correspond to subclasses of PTIME:

- $V^0 = \Sigma^B_0$-COMP$\equiv AC^0$, $V^1 = \Sigma^B_1$-COMP $\equiv P$,
- $VP = V^0$+Monotone Circuit Value $\equiv P$,
- $VNC^1 = V^0$+Boolean Formula Value $\equiv NC^1$,
- $VNL = V^0$+Reachability of undirected graphs $\equiv NL$,

Takeuti-Yasumoto forcing : construction of generic

Given a countable nonstandard model $\mathfrak{M} = (M_0, M) \models V^1 + \neg exp$ and a Boolean algebra $\mathbb{B} \subseteq M$ of computational objects over inputs $p_1, \ldots, p_{n-1}$ for a fixed $n \in M_0 \setminus \omega$.

Takeuti-Yasumoto forcing : construction of generic

Given a countable nonstandard model $\mathfrak{M} = (M_0, M) \models V^1 + \neg exp$ and a Boolean algebra $\mathbb{B} \subseteq M$ of computational objects over inputs $p_1, \ldots, p_{n-1}$ for a fixed $n \in M_0 \setminus \omega$.

e.g. $\mathbb{B} = \{C \in M : C \text{ is a circuit with } n \text{ inputs}\}$

Takeuti-Yasumoto forcing : construction of generic

Given a countable nonstandard model $\mathfrak{M} = (M_0, M) \models V^1 + \neg exp$ and a Boolean algebra $\mathbb{B} \subseteq M$ of computational objects over inputs $p_1, \ldots, p_{n-1}$ for a fixed $n \in M_0 \setminus \omega$.

e.g. $\mathbb{B} = \{C \in M : C \text{ is a circuit with } n \text{ inputs}\}$

We assume some partial order on $\mathbb{B}$.

Takeuti-Yasumoto forcing : construction of generic

Given a countable nonstandard model $\mathfrak{M} = (M_0, M) \models V^1 + \neg exp$ and a Boolean algebra $\mathbb{B} \subseteq M$ of computational objects over inputs $p_1, \ldots, p_{n-1}$ for a fixed $n \in M_0 \setminus \omega$.

e.g. $\mathbb{B} = \{C \in M : C \text{ is a circuit with } n \text{ inputs}\}$

We assume some partial order on $\mathbb{B}$.

Examples:

- $X \leq_e Y \Leftrightarrow \forall A \in 2^n \, (A \models X \to A \models Y)$.
- $X \leq_{\mathcal{F}} Y \Leftrightarrow \mathfrak{M} \models \exists P \; Prf_{\mathcal{F}}(P, X \to Y)$.

Takeuti-Yasumoto forcing : construction of generic

A M_0-complete ideal $\mathbb{I} \subseteq \mathbb{B}$ is a nontrivial ideal such that for any $X = \langle X_0, \ldots, X_k \rangle \in M^{\mathbb{B}}$,

$$X_0, \ldots, X_k \in \mathbb{I} \Rightarrow \bigvee_{i \leq k} X_i \in \mathbb{I}$$

Elements of the ideal are ruled out from the generic extension.

Takeuti-Yasumoto forcing : construction of generic

A M_0-complete ideal $\mathbb{I} \subseteq \mathbb{B}$ is a nontrivial ideal such that for any $X = \langle X_0, \ldots, X_k \rangle \in M^{\mathbb{B}}$,

$$X_0, \ldots, X_k \in \mathbb{I} \Rightarrow \bigvee_{i \leq k} X_i \in \mathbb{I}$$

Elements of the ideal are ruled out from the generic extension.

A set $\mathbb{D} \subseteq \mathbb{B}$ is dense over a M_0-complete ideal $\mathbb{I}$ if for any $X \in \mathbb{B} \setminus \mathbb{I}$ there is $X' \in \mathbb{D} \setminus \mathbb{I}$ such that $X' \leq X$.

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

Takeuti-Yasumoto forcing : forcing theorem

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

$M_{\mathbb{G}} = \{i_{\mathbb{G}}(X) : X \in M, X : a \to \mathbb{B}, \text{ for some } a \in M_0\}$

$\mathfrak{M}[\mathbb{G}] = (M_0, M_{\mathbb{G}})$

Takeuti-Yasumoto forcing : forcing theorem

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

$M_{\mathbb{G}} = \{i_{\mathbb{G}}(X) : X \in M, X : a \to \mathbb{B}, \text{ for some } a \in M_0\}$

$\mathfrak{M}[\mathbb{G}] = (M_0, M_{\mathbb{G}})$

Theorem (Forcing Theorem)

There is a translation $[\![\cdot]\!] : \Sigma_0^B \to \mathbb{B}$ *such that for* $\varphi(\bar{x}, \bar{X}) \in \Sigma_0^B$, $\bar{a} \in M_0$, $A_1, \ldots, A_k \in M$, *with* $A_i : b_i \to \mathbb{B}$ *and* $\mathcal{M}$*-generic* $\mathbb{G}$,

$$\mathfrak{M}[\mathbb{G}] \models \varphi(\bar{a}, i_{\mathbb{G}}(A_1), \ldots, i_{\mathbb{G}}(A_k)) \Leftrightarrow [\![\varphi(\bar{a}, A_1, \ldots, A_k)]\!] \in \mathbb{G}.$$

Boolean algebras for NC^1

Boolean algebra for NC^1 is constructed by using the fact that NC^1 circuits are essentially Boolean formulas.

$\mathit{Formula}(\bar{p})$ = the set of Boolean formulas with variables $\bar{p} = p_0, \ldots, p_{n-1}$

Boolean algebras for NC^1

Boolean algebra for NC^1 is constructed by using the fact that NC^1 circuits are essentially Boolean formulas.

$Formula(\bar{p})$ = the set of Boolean formulas with variables $\bar{p} = p_0, \ldots, p_{n-1}$

Partial orders:

- $X \leq_e Y \Leftrightarrow \forall A \in 2^n \, (A \models X \to A \models Y)$.
- $X \leq_{PK} Y \Leftrightarrow \mathfrak{M} \models \exists P \; Prf_{PK}(P, X \to Y)$.

Boolean algebras for NC^1

Boolean algebra for NC^1 is constructed by using the fact that NC^1 circuits are essentially Boolean formulas.

$Formula(\bar{p})$ = the set of Boolean formulas with variables $\bar{p} = p_0, \ldots, p_{n-1}$

Partial orders:

- $X \leq_e Y \Leftrightarrow \forall A \in 2^n \, (A \models X \to A \models Y)$.
- $X \leq_{PK} Y \Leftrightarrow \mathfrak{M} \models \exists P \; Prf_{PK}(P, X \to Y)$.

$\mathbb{B}_{NC} = Formula(\bar{p})/=_e$, $\mathbb{B}_{PK} = Formula(\bar{p})/=_{PK}$.

Basic Properties of generic sets

Let $\mathbb{B}$ be either $\mathbb{B}_{NC}$ or $\mathbb{B}_{PK}$.

Lemma

Let I be an M_0-complete ideal. For any $X \in \mathbb{B} \setminus I$ there exists a $\mathcal{M}$-generic $\mathbb{G}$ such that $X \in \mathbb{G}$.

A set $\mathbb{S} \subseteq \mathbb{B}$ is PK-consistent if

$$\mathfrak{M} \models \text{ there is no } PK\text{-proof of } \bot \text{ from } S.$$

Lemma

If $\mathbb{S} \subseteq \mathbb{B}$ is PK-consistent then there exists a $\mathcal{M}$-generic $\mathbb{G}$ such that $\mathbb{S} \subseteq \mathbb{G}$.

Boolean algebra for *NL*

Boolean algebra for *NL* is obtained by extending propositional formulas to allow transitive closure operators.

TC connective: $TC^k_{n,a,b}(p_{0,1}, \ldots, p_{n-1,n-2})$.

Intended meaning:
there is a path of length $\leq k$ from a to b in the graph defined by $p_{0,1}, \ldots, p_{n-1,n-2}$.

Partial orders:

- $X \leq_e Y \Leftrightarrow \forall A \in 2^n \, (A \models X \to A \models Y)$.
- $X \leq_{PTCK} Y \Leftrightarrow \mathfrak{M} \models \exists P \; Prf_{PTCK}(P, X \to Y)$.

NB : *PTCK* is *PK* extended by axioms for TC connectives.

$\mathbb{B}_{TC} = Formula(\bar{p})/=_e, \quad \mathbb{B}_{PTCK} = TCF(\bar{p})/=_{PTCK}$

Generic models for NC^1 and NL

Theorem

1. *If* $\mathbb{G} \subseteq \mathbb{B}_{NC}$ *or* $\mathbb{B}_{PK}$ *is* $\mathcal{M}$*-generic then* $\mathfrak{M}[\mathbb{G}] \models VNC^1$.
2. *If* $\mathbb{G} \subseteq \mathbb{B}_{TC}$ *or* $\mathbb{B}_{PTCK}$ *is* $\mathcal{M}$*-generic then* $\mathfrak{M}[\mathbb{G}] \models VNL$.

Generic models for NC^1 and NL

Theorem

1. *If* $\mathbb{G} \subseteq \mathbb{B}_{NC}$ *or* $\mathbb{B}_{PK}$ *is* $\mathcal{M}$*-generic then* $\mathfrak{M}[\mathbb{G}] \models VNC^1$.
2. *If* $\mathbb{G} \subseteq \mathbb{B}_{TC}$ *or* $\mathbb{B}_{PTCK}$ *is* $\mathcal{M}$*-generic then* $\mathfrak{M}[\mathbb{G}] \models VNL$.

Proof is given by constructing Boolean formulas/TC formulas witnessing Boolean formula value problem/st-connectivity resp.

Relating generic models and computational complexity

Theorem (K)

Let $\mathfrak{M} \models V^1$. $\mathfrak{M} \models P \subseteq NC^1$ *if and only if* $\mathfrak{M}[\mathbb{G}] \models VP$ *for any* $\mathcal{M}$*-generic* $\mathbb{G} \subseteq \mathbb{B}_{NC}$.

Relating generic models and computational complexity

Theorem (K)

Let $\mathfrak{M} \models V^1$. $\mathfrak{M} \models P \subseteq NC^1$ if and only if $\mathfrak{M}[\mathbb{G}] \models VP$ for any $\mathcal{M}$-generic $\mathbb{G} \subseteq \mathbb{B}_{NC}$.

(From left to right).

If $\mathfrak{M} \models P \subseteq NC^1$ then we can witness Monotone Circuit Value by Boolean formulas.

Relating generic models and computational complexity

Theorem (K)

Let $\mathfrak{M} \models V^1$. $\mathfrak{M} \models P \subseteq NC^1$ if and only if $\mathfrak{M}[\mathbb{G}] \models VP$ for any $\mathcal{M}$-generic $\mathbb{G} \subseteq \mathbb{B}_{NC}$.

(From left to right).

If $\mathfrak{M} \models P \subseteq NC^1$ then we can witness Monotone Circuit Value by Boolean formulas.

(From right to left).

If $\mathfrak{M} \models P \not\subseteq NC^1$ then we can construct a PK-consistent set violating MCV.

Relating generic models and proof complexity

Theorem (K)

Let $\mathfrak{M} \models V^1$ and suppose that the following conditions hold in $\mathfrak{M}$.

- $G_1^* \leq_p G_0$.
- *Propositional translations of Σ_1^B-theorems of V^1 have polynomial size G_1^* proofs*

Then $\mathfrak{M}[\mathbb{G}] \models VP$ for any $\mathcal{M}$-generic $\mathbb{G} \subseteq \mathbb{B}_F$.

Theorem (K)

Let $\mathfrak{M} \models V^1$ and suppose that $\mathfrak{M} \models EF \not\leq_p F$. Then there exists an $\mathcal{M}$-generic $\mathbb{G} \subseteq \mathbb{B}_F$ such that

$$\mathfrak{M}[\mathbb{G}] \not\models V^1.$$

Problems

- Construct Boolean algebras for other complexity classes; eg. three-sort models for PSPACE.
- Develop techniques to decide whether a given $\Sigma_2^B \cup \Pi_2^B$ formula holds or not in generic extensions.