Consistency proof of an arithmetic with substitution inside a bounded arithmetic

Yoriyuki Yamagata

Kyoto University

October 6, 2016

Language

Definition (Language L)

1. *Constant:* 0
2. *Function symbols:* $S, +, \times, \lfloor \frac{\cdot}{2} \rfloor, |\cdot|, \#$
3. *Relation symbols:* $=, \leq$

Remark

1. $\lfloor \frac{a}{2} \rfloor$ *is the division by two*
2. $|a|$ *is the length of bits of a*
3. $a \# b = 2^{|a| \cdot |b|}$

Bounded arithmetic

Definition (Bounded arithmetic over L)

A theory of arithmetic of which axioms consist in

1. *BASIC* axioms
2. induction schema only for *bounded* formulas

Remark

All quantifiers of a bounded formula must be bounded by terms of L.

Hierarchy of bounded formulas

$\forall x \leq |t|, \exists x \leq |t|$: *sharply* bounded quantifiers

$\forall x \leq t, \exists x \leq t$: *bounded* quantifiers

The hierarchy of bounded formulas

$$\Pi^b_0 \subset \Pi^b_1 \subset \cdots \subset \Pi^b_i \subset \cdots$$

$$\Sigma^b_0 \subset \Sigma^b_1 \subset \cdots \subset \Sigma^b_i \subset \cdots$$

defined by alternation of bounded quantifiers ignoring *sharply* bounded quantifiers.

Many induction schemata

For any term t and $A \in \Sigma^b_i$

1. $\Sigma^b_i - IND$: $A(0) \supset \forall x(A(x) \supset A(Sx)) \supset A(t)$
2. $\Sigma^b_i - PIND$: $A(0) \supset \forall x(A(\lfloor \frac{x}{2} \rfloor) \supset A(x)) \supset A(t)$
3. $\Sigma^b_i - LIND$: $A(0) \supset \forall x(A(|x|) \supset A(S|x|)) \supset A(|t|)$

etc...

Remark

1. $\Sigma^b_{i+1} - PIND \Rightarrow \Sigma^b_i - IND \Rightarrow \Sigma^b_i - PIND$
2. $\Sigma^b_i - PIND \Leftrightarrow \Sigma^b_i - LIND$

Buss's bounded arithmetics

Definition

1. S^i_2: $BASIC$-axioms $+ \Sigma^b_i - PIND$
2. T^i_2: $BASIC$-axioms $+ \Sigma^b_i - IND$
3. $S_2 = \bigcup_{i \in \mathbb{N}} S^i_2 = \bigcup_{i \in \mathbb{N}} T^i_2$

Remark

$S^1_2 \subseteq T^1_2 \subseteq \cdots \subseteq S^i_2 \subseteq T^i_2 \subseteq \cdots$

S^i_2 and Polynomial Hierarchy (PH)

T: a theory of arithmetic $\Rightarrow$
PT(T): the set of provably total functions in T

Fact (Buss 1988)

1. $\mathrm{PT}(S^1_2) = \{\textit{PTIME functions}\}$
2. $\mathrm{PT}(S^i_2) = \{\textit{PTIME functions using a } \Sigma^p_{i-1} \textit{oracle}\}$

Language

Definition (L^{PV})

1. Constant: 0
2. Function symbols: $s_0, s_1, S, +, \dot{-}, \times, \mathrm{Cond}, \lfloor \frac{\cdot}{2} \rfloor, |\cdot|, \boxplus, \#$ plus all PTIME-functions
3. Predicate: $=$

Axioms

1. $s_0 0 = 0$
2. Defining axioms for primitive function symbols
3. Limited recursion on notations:

$$\begin{aligned} f(0, \overline{x}) &= g(\overline{x}) \\ f(s_0 x, \overline{x}) &= \min\{g_0(x, f(x, \overline{x}), \overline{x})), k(s_0 x, \overline{x})\} \\ f(s_1 x, \overline{x}) &= \min\{g_1(x, f(x, \overline{x}), \overline{x})), k(s_1 x, \overline{x})\} \end{aligned}$$

4. Equational axioms
5. Substitution axiom $t(x) = u(x) \Rightarrow t(s) = u(s)$
6. Induction axiom

PV and related systems

1. PV: Full
2. PV$^-$: PV without induction
3. PV^{--}: PV without induction and substitution
4. Adding $_p$ subscript: addition of propositional logic

Is Buss's hierarchy strict?

Conjecture

$S_2^1 \subsetneq S_2^2 \subsetneq \cdots \subsetneq S_2^i \subsetneq S_2^{i+1} \subsetneq \cdots$

Remark

1. *Major open problem*
2. *If* $S_2^1 = S_2$, $P = NP$

Separation of S^i_2 through Gödel sentences

Fact (Buss, 1988)

Incompleteness theorems hold in S^i_2, that is, $S^i_2 \nvdash \mathrm{Con}(S^i_2)$

Question

$S_2 \vdash \mathrm{Con}(S^1_2)$?

Answer (Wilkie and Paris, 1980)

$S_2 \nvdash \mathrm{Con}(Q)$

More unprovability results

Fact

1. $S_2^i \nvdash \mathrm{BdCon}(S_2^i)$ *(Buss, 1988)*
2. $S_2 \nvdash \mathrm{BdCon}(S_2^1)$ *(Púdlak, 1990)*
3. $S_2 \nvdash \mathrm{BdCon}(S_2^{-1})$ *(Takeuti, 1990, Buss and Ignjatović, 1996)*
4. $S_2^1 \nvdash \mathrm{Con}(\mathrm{PV}_p^- + BASIC)$ *(Buss and Ignjatović, 1996)*

etc...

Conjecture (Takeuti, 1991)

$S_2^1 \nvdash \mathrm{Con}(S_2^{-\infty})$

Answer (Beckmann, 2002)

Yes!

Provability results

Theorem (Beckmann, 2002)

$S^1_2 \vdash \mathrm{Con}(PV^{--})$

Remark

1. *Actually, any rewriting system with good properties is okay*
2. *Not many provability results on consistency are known (except 2nd order propositional logic)*

Main result: $S^2_2 \vdash \mathrm{Con}(PV^-)$

Theorem (Yamagata, 2016 (preprint))

$S^2_2 \vdash \mathrm{Con}(PV^-)$

Remark

To prove inside S^1_2 could be possible, but it requires explicit construction of witness during induction on Π^b_2-formulas

BHK reading of equality

Read

$$\begin{array}{c} \vdots\ \pi \\ t = u \end{array}$$

as a "construction" from "computation" of t to u and vice verse, which preserves the value of a computation

Proof strategy

1. "computation" $=$ derivation in big-step semantics
2. Bounds a number of *steps* of computations of u by that of t and vice verse
3. Bounds the *size* of a computation by its steps

Judgment

$$\langle t, \rho \rangle \downarrow v$$

1. t : a term of PV
2. ρ : a sequence of substitutions
3. v : the *approximated* value using $*$

Big-step semantics

$$\frac{\langle t, \rho_2\rangle \downarrow v}{\langle x, \rho_1[t/x]\rho_2\rangle \downarrow v}\ \text{Subst} \qquad \frac{}{\langle t, \rho\rangle \downarrow *}\ *$$

$$\frac{\langle \epsilon, ()\rangle \downarrow \epsilon \quad \langle \epsilon, \rho\rangle \downarrow \epsilon}{\langle \epsilon, \rho\rangle \downarrow \epsilon}\ \epsilon \qquad \frac{}{\langle \epsilon, ()\rangle \downarrow \epsilon}\ \epsilon n$$

$$\frac{\langle s_i v^*, ()\rangle \downarrow s_i v^* \quad \langle t, \rho\rangle \downarrow v}{\langle s_i t, \rho\rangle \downarrow s_i v^*}\ s_i \qquad \frac{\langle v, ()\rangle \downarrow v}{\langle s_i v, ()\rangle \downarrow s_i v}\ s_i n$$

$$\frac{\langle \epsilon, ()\rangle \downarrow \epsilon \quad (\langle t_i, \rho\rangle \downarrow v_i)_{i\in X}}{\langle \epsilon^m(t_1, \dots, t_m), \rho\rangle \downarrow \epsilon}\ \epsilon^m \qquad \frac{\langle v_i^*, ()\rangle \downarrow v_i^* \quad (\langle t_j, \rho\rangle \downarrow v_j)_{j\in X}}{\langle \mathrm{proj}^i_m(t_1, \dots, t_m), \rho\rangle \downarrow v_i^*}\ \mathrm{proj}^i_m$$

$$\frac{\langle g(\overline{w^*}), ()\rangle \downarrow z \quad \langle h^1(\overline{v^1}), ()\rangle \downarrow w_1 \cdots \langle h^m(\overline{v^m}), ()\rangle \downarrow w_m \quad (\langle t_i, \rho\rangle \downarrow v_i)_{i\in X}}{\langle f(t_1, \dots, t_n), \rho\rangle \downarrow z}\ \text{comp}$$

$$\frac{\langle g_\epsilon(\overline{v^1}), ()\rangle \downarrow z \quad \{\langle t, \rho\rangle \downarrow \epsilon\} \quad (\langle t_i, \rho\rangle \downarrow v_i)_{i\in X}}{\langle f(t, t_1, \dots, t_n), \rho\rangle \downarrow z}\ \text{rec-}\epsilon$$

$$\frac{\langle g_i(v_0^1, w^1, \overline{v^1}), ()\rangle \downarrow z \quad \{\langle t, \rho\rangle \downarrow s_i v_0\} \quad \langle f(v_0^2, \overline{v^2}), ()\rangle \downarrow w \quad (\langle t_j, \rho\rangle \downarrow v_j)_{j\in X}}{\langle f(t, t_1, \dots, t_n), \rho\rangle \downarrow z}\ \text{rec-}s_i$$

Computation

Definition

Computation is a DAG of which nodes are judgments and edges are inferences of big-step semantics

1. Judgments which are not used as premises, are called *conclusions*
2. $\sigma \vdash \langle t_1, \rho_1 \rangle \downarrow v_1, \dots$
   computation σ, conclusions $\langle t_1, \rho_1 \rangle \downarrow v_1, \dots$

Notation

1. $||t||$: *Number of primitive symbols in any object* t
2. $|||\sigma|||$: *Number of nodes in* σ

Main proposition

Proposition

Fix a large U. For any tree-like PV^-*-proof* π

$$\begin{array}{c} \vdots\ \pi \\ t = u \end{array}$$

and $||\rho||, ||\alpha||, |||\sigma||| \leq U - ||\pi||$ *s.t.* $\sigma \vdash \langle t, \rho \rangle \downarrow v, \alpha$
$\Rightarrow \exists \tau$ *s.t.*

1. $|||\tau||| \leq |||\sigma||| + ||\pi||$
2. $\tau \vdash \langle u, \rho \rangle \downarrow v, \alpha$

Proof of main proposition

Induction on π.
The induction formula is Π^b_2-formula with U as a parameter

Transformation for projection

$$\mathrm{proj}^k_m(t_1, \ldots, t_m) = t_k$$

$$\frac{\langle v^*_i, \rho \rangle \downarrow v^*_i \quad \langle t_1, \rho \rangle \downarrow v_1 \quad \cdots \quad \langle t_m, \rho \rangle \downarrow v_m}{\langle \mathrm{proj}^n_i(t_1, \ldots, t_n), \rho \rangle \downarrow v^*_i}$$

$$\Downarrow$$

$$\langle t_i, \rho \rangle \downarrow v_i$$

Transformation for projection

$$\mathrm{proj}_m^k(t_1, \ldots, t_m) = t_k$$

$$\frac{\langle v_i, \rho \rangle \downarrow v_i \quad \langle t_1, \rho \rangle \downarrow * \quad \cdots \quad \langle t_i, \rho \rangle \downarrow v_i \quad \cdots \quad \langle t_m, \rho \rangle \downarrow *}{\langle \mathrm{proj}_i^n(t_1, \ldots, t_n), \rho \rangle \downarrow v_i}$$

$$\Uparrow$$

$$\langle t_i, \rho \rangle \downarrow v_i$$

Transformation for composition

$$f(\vec{u}) = g(h_1(\vec{u}), \ldots, h_m(\vec{u}))$$

$$\dfrac{\dfrac{\overline{\beta}}{\langle g(\overline{w^*}), ()\rangle \downarrow v} \quad \dfrac{\overline{\gamma_1}}{\langle h_1(\overline{z^1}), ()\rangle \downarrow w_1} \quad \ldots \quad (\langle u_i, \rho\rangle \downarrow z_i)_{i \in X}}{\langle f(\overline{u}), \rho\rangle \downarrow v.}$$

$$\Updownarrow$$

$$\dfrac{\overline{\beta} \quad \dfrac{\overline{\gamma_1} \quad (\langle u_i, \rho\rangle \downarrow z_i^1)_{i \in X}}{\langle h_1(\overline{u}), \rho\rangle \downarrow w_1} \quad \ldots}{\langle g(\overline{h}(\overline{u})), \rho\rangle \downarrow v}$$

Substitution Lemma I

1. U : a large integer.
2. σ : a computation s.t.
   1. $\sigma \vdash \langle t_1[u/x], \rho \rangle \downarrow v_1, \ldots, \langle t_m[u/x], \rho \rangle \downarrow v_m, \overline{\alpha}$
   2. $|||\sigma||| \leq U - ||t_1[u/x]|| - \cdots - ||t_m[u/x]||$

$\Rightarrow \exists \tau$ s.t.

1. $\tau \vdash \langle t_1, [u/x]\rho \rangle \downarrow v_1, \ldots, \langle t_m, [u/x]\rho \rangle \downarrow v_m, \overline{\alpha}$
2. $|||\tau||| \leq |||\sigma||| + ||t_1[u/x]|| + \cdots + ||t_m[u/x]||$

Substitution Lemma II

1. U : a large integer.
2. σ : a computation s.t.
   1. $\sigma \vdash \langle t_1, [u/x]\rho\rangle \downarrow v_1, \ldots, \langle t_m, [u/x]\rho\rangle \downarrow v_m, \overline{\alpha}$
   2. $|||\sigma||| \leq U - ||t_1[u/x]|| - \cdots - ||t_m[u/x]||$

$\Rightarrow \exists \tau$ s.t.

1. $\tau \vdash \langle t_1[u/x], \rho\rangle \downarrow v_1, \ldots, \langle t_m[u/x], \rho\rangle \downarrow v_m, \overline{\alpha}$
2. $|||\tau||| \leq |||\sigma||| + ||t_1[u/x]|| + \cdots + ||t_m[u/x]||$

Transformation for substitution

$$\dfrac{\begin{array}{c}\vdots\ \pi_1\\ t(x) = u(x)\end{array}}{t(s) = u(s)}$$

$$\sigma \vdash \langle t(s), \rho \rangle \downarrow v, \alpha$$

Transformation for substitution

$$\dfrac{\begin{array}{c}\vdots\ \pi_1\\ t(x) = u(x)\end{array}}{t(s) = u(s)}$$

$$\sigma_0 \vdash \langle t(x), [s/x]\rho\rangle \downarrow v, \alpha$$
$$|||\sigma_0||| \leq |||\sigma||| + ||t(s)||$$

Transformation for substitution

$$\dfrac{\begin{array}{c}\vdots\ \pi_1\\ t(x) = u(x)\end{array}}{t(s) = u(s)}$$

$$\tau_0 \vdash \langle u(x), [s/x]\rho\rangle \downarrow v, \alpha$$
$$|||\tau_0||| \leq |||\sigma||| + ||\pi_1|| + ||t(s)||$$

Transformation for substitution

$$\dfrac{\begin{array}{c}\vdots\ \pi_1 \\ t(x) = u(x)\end{array}}{t(s) = u(s)}$$

$$\tau \vdash \langle u(s), \rho \rangle \downarrow v, \alpha$$
$$|||\tau||| \leq |||\sigma||| + ||\pi_1|| + ||t(s)|| + ||u(s)||$$

Conclusion

Theorem

$S^2_2 \vdash \mathrm{Con}(PV^-)$

Future works

Question

$S_2 \vdash \mathrm{Con}(PV_p^-(d))$?

Question

$S_2 \vdash \mathrm{Con}(PV_p^-(d) + BASIC)$?

Remark

The last statement may imply $S_2^1 \subsetneq S_2$