Consistency proof of an arithmetic with substitution inside a bounded arithmetic

Yoriyuki Yamagata

Kyoto University

October 6, 2016
Definition (Language $L$)

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

Remark

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

∀x ≤ |t|, ∃x ≤ |t| : \(\text{sharply bounded quantifiers}\)

∀x ≤ t, ∃x ≤ t : \(\text{bounded quantifiers}\)

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 \text{sharply} bounded quantifiers.
Many induction schemata

For any term \( t \) and \( A \in \Sigma^b_i \)

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

etc...

Remark

1. \( \Sigma^b_{i+1} - \text{PIND} \Rightarrow \Sigma^b_i - \text{IND} \Rightarrow \Sigma^b_i - \text{PIND} \)
2. \( \Sigma^b_i - \text{PIND} \Leftrightarrow \Sigma^b_i - \text{LIND} \)
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. $PT(S^1_2) = \{PTIME \text{ functions}\}$
2. $PT(S^i_2) = \{PTIME \text{ functions using a } \Sigma^p_{i-1} \text{ oracle}\}$
Main result: $S^2_2 \vdash \text{Con}(\text{PV}^-)$

Proof

Conclusion

Language

Definition ($L^{PV}$)

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

1. \( s_00 = 0 \)
2. Defining axioms for primitive function symbols
3. Limited recursion on notations:
   \[
   f(0, \bar{x}) = g(\bar{x})
   \]
   \[
   f(s_0x, \bar{x}) = \min\{g_0(x, f(x, \bar{x}), \bar{x}), k(s_0x, \bar{x})\}
   \]
   \[
   f(s_1x, \bar{x}) = \min\{g_1(x, f(x, \bar{x}), \bar{x}), k(s_1x, \bar{x})\}
   \]
4. Equational axioms
5. Substitution axiom \( t(x) = u(x) \implies t(s) = u(s) \)
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

\[ S^1_2 \subsetneq S^2_2 \subsetneq \cdots \subsetneq S^i_2 \subsetneq S^{i+1}_2 \subsetneq \cdots \]

Remark

1. Major open problem
2. If \( S^1_2 = S_2 \), \( P = NP \)
Separation of $S_2^i$ through Gödel sentences

Fact (Buss, 1988)

*Incompleteness theorems hold in $S_2^i$, that is, $S_2^i \not\vdash \text{Con}(S_2^i)$*

Question

$S_2 \vdash \text{Con}(S_2^1)$?

Answer (Wilkie and Paris, 1980)

$S_2 \not\vdash \text{Con}(Q)$
More unprovability results

Fact

1. $S^i_2 \not\vdash \text{BdCon}(S^i_2)$ (Buss, 1988)
2. $S_2 \not\vdash \text{BdCon}(S^1_2)$ (Púdlak, 1990)
3. $S_2 \not\vdash \text{BdCon}(S^{−1}_2)$ (Takeuti, 1990, Buss and Ignjatović, 1996)
4. $S^1_2 \not\vdash \text{Con}(\text{PV}^- \text{ + BASIC})$ (Buss and Ignjatović, 1996)

etc...

Conjecture (Takeuti, 1991)

$S^1_2 \not\vdash \text{Con}(S^{−\infty}_2)$

Answer (Beckmann, 2002)

Yes!
Provability results

Theorem (Beckmann, 2002)

$S_2^1 \vdash \text{Con(PV}^\rightarrow)$

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

Theorem (Yamagata, 2016 (preprint))
$S^2_2 \vdash \text{Con}(PV^-)$

Remark
To prove inside $S^1_2$ could be possible, but it requires explicit construction of witness during induction on $\Pi^b_2$-formulas
BHK reading of equality

Read

$$\vdash \pi$$

$$t = u$$

as a “construction” from “computation” of $t$ to $u$ and vice versa, 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 versa
3. Bounds the size of a computation by its steps
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss’s bounded arithmetic

Cook and Urquhart’s PV

Separation of Buss’s hierarchy

Main result: \[ S^2_2 \vdash \text{Con}(PV^-) \]

Proof

Conclusion

\[ \langle t, \rho \rangle \downarrow v \]

1. \( t \) : a term of PV
2. \( \rho \) : a sequence of substitutions
3. \( v \) : the \textit{approximated} value using \( * \)
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss's bounded arithmetic
Cook and Urquhart's PV
Separation of Buss's hierarchy

Main result: $S_2^2 \vdash \text{Con}(PV^-)$

Proof

Conclusion
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. \( \sigma \vdash \langle t_1, \rho_1 \rangle \downarrow v_1, \ldots \)

   computation \( \sigma \), conclusions \( \langle t_1, \rho_1 \rangle \downarrow v_1, \ldots \)

Notation

1. \( ||t||: \text{Number of primitive symbols in any object } t \)

2. \( |||\sigma|||: \text{Number of nodes in } \sigma \)
Main proposition

Proposition

Fix a large $U$. For any tree-like $PV^-$-proof $\pi$

$$\vdash \pi$$

$t = u$

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 $\pi$.
The induction formula is $\Pi^b_2$-formula with $U$ as a parameter
Transformation for projection

\[ \text{proj}_m^k(t_1, \ldots, t_m) = t_k \]

\[
\begin{align*}
\langle v_i^*, \rho \rangle & \downarrow v_i^* & \langle t_1, \rho \rangle & \downarrow v_1 & \cdots & \langle t_m, \rho \rangle & \downarrow v_m \\
\langle \text{proj}_i^n(t_1, \ldots, t_n), \rho \rangle & \downarrow v_i^* \\
\downarrow \\
\langle t_i, \rho \rangle & \downarrow v_i
\end{align*}
\]
Transformation for projection

\[
\text{proj}^k_m(t_1, \ldots, t_m) = t_k
\]

\[
\langle v_i, \rho \rangle \downarrow v_i \quad \langle t_1, \rho \rangle \downarrow * \quad \cdots \quad \langle t_i, \rho \rangle \downarrow v_i \quad \cdots \quad \langle t_m, \rho \rangle \downarrow *
\]

\[
\langle \text{proj}^n_i(t_1, \ldots, t_n), \rho \rangle \downarrow v_i
\]

\[
\uparrow
\]

\[
\langle t_i, \rho \rangle \downarrow v_i
\]
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss's bounded arithmetic
Cook and Urquhart's PV
Separation of Buss's hierarchy

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

Proof

Conclusion

Transformation for composition

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

$$\overline{\beta} \quad \overline{\gamma_1}$$

$$\langle g(\vec{w}^*), () \rangle \downarrow v \quad \langle h_1(\vec{z}^1), () \rangle \downarrow w_1 \quad \ldots \quad (\langle u_i, \rho \rangle \downarrow z_i)_{i \in X}$$

$$\langle f(\vec{u}), \rho \rangle \downarrow v.$$}

$$\Leftrightarrow$$

$$\overline{\gamma_1} \quad (\langle u_i, \rho \rangle \downarrow z_i^1)_{i \in X}$$

$$\overline{\beta}$$

$$\langle h_1(\vec{u}), \rho \rangle \downarrow w_1 \quad \ldots \quad \langle g(h(\vec{u})), \rho \rangle \downarrow v$$
Substitution Lemma 1

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

$\Rightarrow \exists \tau$ s.t.
1. $\tau \vdash \langle t_1, [u/x]\rho \rangle \downarrow v_1, \ldots, \langle t_m, [u/x]\rho \rangle \downarrow v_m, \bar{\alpha}$
2. $|||\tau||| \leq |||\sigma||| + ||t_1[u/x]|| + \cdots + ||t_m[u/x]||$
Substitution Lemma II

1. \( U \) : a large integer.
2. \( \sigma \) : 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. \( ||\sigma|| \leq U - ||t_1[u/x]|| - \cdots - ||t_m[u/x]|| \)

\[ \Rightarrow \exists \tau \text{ s.t.} \]

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. \( ||\tau|| \leq ||\sigma|| + ||t_1[u/x]|| + \cdots + ||t_m[u/x]|| \)
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss’s bounded arithmetic
Cook and Urquhart’s PV
Separation of Buss’s hierarchy
Main result: \( S^2_2 \vdash \text{Con}(PV^-) \)

Proof

Conclusion

Transformation for substitution

\[ \vdash \pi_1 \]
\[ t(x) = u(x) \]
\[ t(s) = u(s) \]

\[ \sigma \vdash \langle t(s), \rho \rangle \downarrow v, \alpha \]
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss’s bounded arithmetic
Cook and Urquhart’s PV

Separation of Buss’s hierarchy

Main result: $S_2^2 \vdash \text{Con}(PV^-)$

Proof

Conclusion

Transformation for substitution

\[
\vdash \pi_1 \\
\frac{t(x) = u(x)}{t(s) = u(s)}
\]

\[
\sigma_0 \vdash \langle t(x), [s/x] \rho \rangle \downarrow \nu, \alpha \\
norm{\sigma_0} \leq \norm{\sigma} + \norm{t(s)}
\]
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss's bounded arithmetic
Cook and Urquhart's PV
Separation of Buss's hierarchy
Main result: $S^2_2 \vdash \text{Con}(PV^-)$
Proof
Conclusion

Transformation for substitution

\[
\vdash \pi_1 \\
\frac{t(x) = u(x)}{t(s) = u(s)}
\]

\[
\tau_0 \vdash \langle u(x), [s/x] \rho \rangle \downarrow v, \alpha \\
\|\|\tau_0\|\| \leq \|\|\sigma\|\| + \|\|\pi_1\|\| + \|\|t(s)\|\|
\]
Consistency proof inside a bounded arithmetic

Yoriyuki Yamagata

Buss’s bounded arithmetic
Cook and Urquhart’s PV
Separation of Buss’s hierarchy

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

Proof

Conclusion

Transformation for substitution

\[
\vdash \pi_1 \\
\begin{align*}
t(x) &= u(x) \\
t(s) &= u(s)
\end{align*}
\]

\[
\tau \vdash \langle u(s), \rho \rangle \downarrow \nu, \alpha \\
|||\tau||| \leq |||\sigma||| + |||\pi_1||| + |||t(s)||| + |||u(s)|||
\]
Consistency proof inside a bounded arithmetic
Yoriyuki Yamagata

Buss's bounded arithmetic
Cook and Urquhart's PV
Separation of Buss's hierarchy

Main result:
$S_2^2 \vdash \text{Con}(PV^-)$

Proof

Conclusion

Theorem

$S_2^2 \vdash \text{Con}(PV^-)$

Conclusion
Future works

**Question**

\[ S_2 \vdash \text{Con}(\text{PV}_p^-(d)) \, ? \]

**Question**

\[ S_2 \vdash \text{Con}(\text{PV}_p^-(d) + \text{BASIC}) ? \]

**Remark**

*The last statement may imply \( S_2^1 \subsetneq S_2 \)*