Bounded Arithmetic in Free Logic

Yoriyuki Yamagata

CTFM, 2013/02/20

Buss's theories S_2^i

- Language of Peano Arithmetic + "#"
  - a # b = $2^{|a|\cdot|b|}$
- BASIC axioms
- PIND

$$\frac{A\left(\left\lfloor\frac{x}{2}\right\rfloor\right), \Gamma \to \Delta, A(x)}{A(0), \Gamma \to \Delta, A(t)}$$

where $A(x) \in \Sigma_i^b$, i.e. has i-alternations of bounded quantifiers $\forall x \le t, \exists x \le t$.

PH and Buss's theories S_2^i

$$S_2^1 = S_2^2 = S_2^3 = \ \ldots$$

Implies

$$P = \square(NP) = \square(\Sigma_2^p) = \ \ldots$$

We can approach (non) collapse of PH from (non) collapse of hierarchy of Buss's theories

(PH = Polynomial Hierarchy)

Our approach

- Separate S_2^i by Gödel incompleteness theorem
- Use analogy of separation of $I\Sigma_i$

Separation of $I\Sigma_i$

$$\vdots$$

$$I\Sigma_3 \vdash \mathrm{Con}(\mathrm{I}\Sigma_2)$$

$$\cup\!|$$

$$I\Sigma_2 \nvdash \mathrm{Con}(\mathrm{I}\Sigma_2)$$

$$\cup\!|$$

$$I\Sigma_1$$

Consistency proof inside S_2^i

- Bounded Arithmetics generally are not capable to prove consistency.
  - S_2 does not prove consistency of Q (Paris, Wilkie)
  - S_2 does not prove bounded consistency of S_2^1 (Pudlák)
  - S_2^i does not prove consistency the B_i^b fragement of S_2^{-1} (Buss and Ignjatović)

Buss and Ignjatović(1995)

$$\vdots$$

$$S_2^3 \nvdash B_3^{\mathrm{b}} - \mathrm{Con}(S_2^{-1})$$

$$\cup\!|$$

$$S_2^2 \nvdash B_2^{\mathrm{b}} - \mathrm{Con}(S_2^{-1})$$

$$\cup\!|$$

$$S_2^1 \nvdash B_1^{\mathrm{b}} - \mathrm{Con}(S_2^{-1})$$

Where…

- $B_i^b - Con(T)$
  - consistency of B_i^b −proofs
  - B_i^b −proofs : the proofs by B_i^b-formule
  - B_i^b:$\Sigma_0^b(\Sigma_i^b)$… Formulas generated from Σ_i^b by Boolean connectives and sharply bounded quantifiers.
- S_2^{-1}
  - Induction free fragment of S_2^i

If…

$$S_2^j \vdash B_\mathrm{i}^\mathrm{b} - \mathrm{Con}(S_2^{-1}), \mathrm{j} > \mathrm{i}$$

Then, Buss's hierarchy does not collapse.

Consistency proof of S_2^{-1} inside S_2^i

Problem

- No truth definition, because
- No valuation of terms, because
  - The values of terms increase exponentially
    - E.g. 2#2#2#2#2#...#2

In S_2^i world, terms do not have values *a priori*.

- Thus, we must prove the existence of values in proofs.
- We introduce the predicate E which signifies existence of values.

Our result(2012)

$\vdots$

$$S_2^5 \vdash 3 - \mathrm{Con}(S_2^{-1}E)$$

$\cup\!|$

$$S_2^4 \vdash 2 - \mathrm{Con}(S_2^{-1}E)$$

$\cup\!|$

$$S_2^3 \vdash 1 - \mathrm{Con}(S_2^{-1}E)$$

Where…

- $i - Con(T)$
  - consistency of i-normal proofs
  - i-normal proofs : the proofs by i-normal formulas
  - i-normal formulas: Formulas in the form:
  $\exists x_1 \leq t_1 \forall x_2 \leq t_2 \ldots Q x_i \leq t_i Q x_{i+1} \leq |t_{i+1}|. A(\ldots)$
  Where A is quantifier free

Where…

- $S_2^{-1}E$
  - Induction free fragment of $S_2^i E$
  - have predicate E which signifies existence of values
    - Such logic is called *Free logic*

$S_2^i E$ (Language)

Predicates

- $=, \leq, E$

Function symbols

- Finite number of polynomial functions

Formulas

- Atomic formula, negated atomic formula
- $A \vee B, A \wedge B$
- Bounded quantifiers

$S_2^i E$ (Axioms)

- E-axioms
- Equality axioms
- Data axioms
- Defining axioms
- Auxiliary axioms

Idea behind axioms…

$$\rightarrow a = a$$

Because there is no guarantee of Ea
Thus, we add Ea in the antecedent

$$Ea \rightarrow a = a$$

E-axioms

- $Ef(a_1, \dots, a_n) \rightarrow Ea_j$
- $a_1 = a_2 \rightarrow Ea_j$
- $a_1 \neq a_2 \rightarrow Ea_j$
- $a_1 \leq a_2 \rightarrow Ea_j$
- $\neg a_1 \leq a_2 \rightarrow Ea_j$

Equality axioms

- $Ea \rightarrow a = a$
- $Ef(\vec{a}), \vec{a} = \vec{b} \rightarrow f(\vec{a}) = f(\vec{b})$

Data axioms

- $\to E0$
- $Ea \to Es_0a$
- $Ea \to Es_1a$

Defining axioms

$$f(u(a_1), a_2, \ldots, a_n) = t(a_1, \ldots, a_n)$$

$u(a) = 0, a, s_0 a, s_1 a$

$$Ea_1, \ldots, Ea_n, Et(a_1, \ldots, a_n) \to$$
$$f(u(a_1), a_2, \ldots, a_n) = t(a_1, \ldots, a_n)$$

Auxiliary axioms

$$|a| = |b| \supset a\#c = b\#c$$

$$Ea\#c, Eb\#c, |a| = |b| \rightarrow a\#c = b\#c$$

PIND-rule

$$\frac{\Gamma \to \Delta, A(0) \quad A(a), \Gamma \to \Delta, A(s_0 a) \quad A(a), \Gamma \to \Delta, A(s_1 a)}{Et, \Gamma \to \Delta, A(t)}$$

where A is an Σ_i^b-formulas

Bootstrapping $S_2^i E$

I. $S_2^i E \vdash \mathrm{Tot}(f)$ for any f, $i \geq 0$

II. $S_2^i E \vdash \mathrm{BASIC}^*, (\text{equality axioms})^*$

III. $S_2^i E \vdash (\text{predicate logic})^*$

IV. $S_2^i E \vdash \Sigma_i^b - \mathrm{PIND}^*$

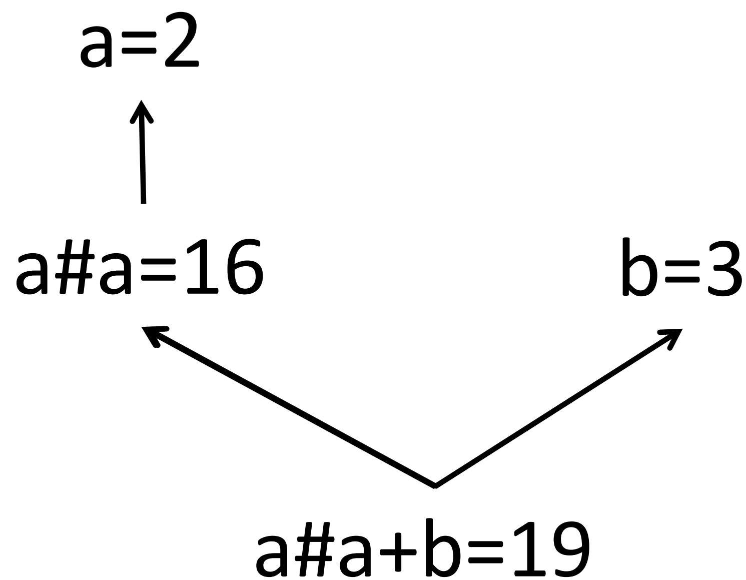
Theorem (Consistency)

$$S_2^{i+2} \vdash \mathrm{i} - \mathrm{Con}(S_2^{-1}E)$$

Valuation trees

ρ-valuation tree bounded by 19

ρ(a)=2, ρ(b)=3



$$v(\lceil a\#a + b \rceil, \rho) \downarrow_{19} 19$$

$v(\lceil t \rceil, \rho) \downarrow_u c$ is Σ_1^b

Bounded truth definition (1)

- $T(u, \lceil t_1 = t_2 \rceil, \rho) \Leftrightarrow_{\text{def}}$
  $\exists c \leq u, v(\lceil t_1 \rceil, \rho) \downarrow_u c \wedge v(\lceil t_1 \rceil, \rho) \downarrow_u c$
- $T(u, \lceil \phi_1 \wedge \phi_2 \rceil, \rho) \Leftrightarrow_{\text{def}}$
  $T(u, \lceil \phi_1 \rceil, \rho) \wedge T(u, \lceil \phi_2 \rceil, \rho)$
- $T(u, \lceil \phi_1 \vee \phi_2 \rceil, \rho) \Leftrightarrow_{\text{def}}$
  $T(u, \lceil \phi_1 \rceil, \rho) \vee T(u, \lceil \phi_2 \rceil, \rho)$

Bounded truth definition (2)

- $T(u, \lceil \exists x \leq t, \phi(x) \rceil, \rho) \Leftrightarrow_{\text{def}}$
$$\exists c \leq u, v(\lceil t \rceil, \rho) \downarrow_u c \land$$
$$\exists d \leq c, T(u, \lceil \phi(x) \rceil, \rho[x \mapsto d])$$
- $T(u, \lceil \forall x \leq t, \phi(x) \rceil, \rho) \Leftrightarrow_{\text{def}}$
$$\exists c \leq u, v(\lceil t \rceil, \rho) \downarrow_u c \land$$
$$\forall d \leq c, T(u, \lceil \phi(x) \rceil, \rho[x \mapsto d])$$

Remark: If ϕ is Σ_i^b, $T(u, \lceil \phi \rceil)$ is Σ_{i+1}^b

induction hypothesis

u: enough large integer
r: node of a proof of 0=1
$\Gamma_r \rightarrow \Delta_r$: the sequent of node r
ρ: assignment $\rho(a) \leq u$

$$\forall u' \leq u \ominus r, \{[\forall A \in \Gamma_r\, T(u', \lceil A \rceil, \rho)] \supset [\exists B \in \Delta_{\mathrm{r}}, T(u' \oplus r, \lceil B \rceil, \rho)]\}$$

Conjecture

- $S_2^{-1}E$ is weak enough
  - S_2^{i+2} can prove i-consistency of $S_2^{-1}E$
- While $S_2^{-1}E$ is strong enough
  - $S_2^{i}E$ can interpret S_2^{i}
- Conjecture

  $S_2^{-1}E$ is a good candidate to separate S_2^{i} and S_2^{i+2}.

Future works

- Long-term goal

$$S_2^i \vdash i\text{--}\mathrm{Con}(S_2^{-1}E)?$$

- Short-term goal
  - Simplify $S_2^i E$

Publications

- Bounded Arithmetic in Free Logic

  Logical Methods in Computer Science

  Volume 8, Issue 3, Aug. 10, 2012