Bounded Arithmetic: Classic and Intuitionistic

Morteza Moniri

Department of Mathematics
Shahid Beheshti University

5th Annual Conference of the IAL, 2017

Outline

1 Bounded Arithmetic

Outline

1. Bounded Arithmetic

2. Buss's theories of Bounded Arithmetic

Bounded Arithmetic

- $\mathrm{I}\Delta_0 =$ Bounded Arithmetic

Bounded Arithmetic

- $\mathrm{I}\Delta_0 =$ Bounded Arithmetic
- $\mathrm{I}\Delta_0$ is obtained from PA by restricting Induction Scheme to bounded formulas.

Bounded Arithmetic

- $\mathrm{I}\Delta_0 =$ Bounded Arithmetic
- $\mathrm{I}\Delta_0$ is obtained from PA by restricting Induction Scheme to bounded formulas.
- $\mathrm{I}\Delta_0$ is a bounded theory (Π_1-axiomatized).

Bounded Arithmetic

- $\mathrm{I}\Delta_0 =$ Bounded Arithmetic
- $\mathrm{I}\Delta_0$ is obtained from PA by restricting Induction Scheme to bounded formulas.
- $\mathrm{I}\Delta_0$ is a bounded theory (Π_1-axiomatized).

Theorem

$\mathrm{I}\Delta_0$ *can prove every property of exp-function, except totality:*

$$\mathrm{I}\Delta_0 \nvdash \forall x \, \forall y \, \exists z \;\; x^y = z$$

Bounded Arithmetic

- $\mathrm{I}\Delta_0$ = Bounded Arithmetic
- $\mathrm{I}\Delta_0$ is obtained from PA by restricting Induction Scheme to bounded formulas.
- $\mathrm{I}\Delta_0$ is a bounded theory (Π_1-axiomatized).

Theorem

$\mathrm{I}\Delta_0$ can prove every property of exp-function, except totality:

$$\mathrm{I}\Delta_0 \nvdash \forall x\, \forall y\, \exists z \;\; x^y = z$$

Proof.

Let $a \in M \models \mathrm{I}\Delta_0$, non-standard

$$a^{\mathbb{N}} = \{b : \; b < a^n \text{ for some } n\} \models \Pi_1(\mathrm{I}\Delta_0) \qquad \square$$

Bounded Arithmetic

Theorem (Wilkie, Paris 1987)

- $\mathrm{I}\Delta_0 + exp \nvdash Con(\mathrm{I}\Delta_0)$ (Indeed, $\mathrm{I}\Delta_0 + exp \nvdash Con(\mathbb{Q})$)
- $\mathrm{I}\Delta_0 + exp + Con(\mathrm{I}\Delta_0) \nvdash Con(\mathrm{I}\Delta_0 + exp)$

Bounded Arithmetic

Theorem (Wilkie, Paris 1987)

- $\mathrm{I}\Delta_0 + \mathit{exp} \nvdash \mathit{Con}(\mathrm{I}\Delta_0)$ (Indeed, $\mathrm{I}\Delta_0 + \mathit{exp} \nvdash \mathit{Con}(\mathbb{Q})$)
- $\mathrm{I}\Delta_0 + \mathit{exp} + \mathit{Con}(\mathrm{I}\Delta_0) \nvdash \mathit{Con}(\mathrm{I}\Delta_0 + \mathit{exp})$

Theorem (Wilmers 1985)

$\mathrm{I}\Delta_0$ (and even IE_1) dose not have recursive model.

- Originally proved for PA by Tennenbaum (1959)

Bounded Arithmetic

Theorem (Paris, Kirby 1978)

$$\mathrm{I}\Sigma_n \equiv \mathrm{I}\Pi_n \equiv \mathrm{L}\Sigma_n \equiv \mathrm{L}\Pi_n$$

Bounded Arithmetic

Theorem (Paris, Kirby 1978)

$$\mathrm{I}\Sigma_n \equiv \mathrm{I}\Pi_n \equiv \mathrm{L}\Sigma_n \equiv \mathrm{L}\Pi_n$$

Theorem (Wilmers 1985)

$$\mathrm{IE}_n \equiv \mathrm{IU}_n \equiv \mathrm{LE}_n$$

Bounded Arithmetic

Theorem (Paris, Kirby 1978)

$$\mathrm{I}\Sigma_n \equiv \mathrm{I}\Pi_n \equiv \mathrm{L}\Sigma_n \equiv \mathrm{L}\Pi_n$$

Theorem (Wilmers 1985)

$$\mathrm{IE}_n \equiv \mathrm{IU}_n \equiv \mathrm{LE}_n$$

Questions (Wilmers)

$$\mathrm{IE}_1 \vdash^? \mathrm{LU}_1$$

Bounded Arithmetic

MRDP Theorem (Matitasevic 1971)

$$\Sigma_1^{\mathbb{N}} = \exists_1^{\mathbb{N}}$$

Bounded Arithmetic

MRDP Theorem (Matitasevic 1971)

$$\Sigma_1^{\mathbb{N}} = \exists_1^{\mathbb{N}}$$

$\Longrightarrow$ Negative answer to Hilbert's tenth problem (because $r.e. = \Sigma_1^{\mathbb{N}}$).

Bounded Arithmetic

MRDP Theorem (Matitasevic 1971)

$$\Sigma_1^{\mathbb{N}} = \exists_1^{\mathbb{N}}$$

$\Longrightarrow$ Negative answer to Hilbert's tenth problem (because $r.e. = \Sigma_1^{\mathbb{N}}$).

Theorem (Dimitracopoulos, Gaifman 1982)

$$\mathrm{I}\Delta_0 + exp \vdash \mathrm{MRDP}$$

Bounded Arithmetic

MRDP Theorem (Matitasevic 1971)

$$\Sigma_1^{\mathbb{N}} = \exists_1^{\mathbb{N}}$$

$\Longrightarrow$ Negative answer to Hilbert's tenth problem (because $r.e. = \Sigma_1^{\mathbb{N}}$).

Theorem (Dimitracopoulos, Gaifman 1982)

$$\mathrm{I}\Delta_0 + exp \vdash \mathrm{MRDP}$$

Questions

$$\mathrm{I}\Delta_0 \vdash^? \mathrm{MRDP}$$

Bounded Arithmetic

- $|x| =$ The length of code of x in base 2

Bounded Arithmetic

- $|x| =$ The length of code of x in base 2
- $\Omega_1 : \forall x \, \forall y \, \exists z \quad z = x^{\mathrm{Ln} y}$

Bounded Arithmetic

- $|x| =$ The length of code of x in base 2
- $\Omega_1 : \forall x \, \forall y \, \exists z \quad z = x^{\mathrm{Ln} y}$
- $\mathrm{I}\Delta_0 + \Omega_1$ is strong enough to formalize consistency

Bounded Arithmetic

- $|x| =$ The length of code of x in base 2
- $\Omega_1 : \forall x \, \forall y \, \exists z \quad z = x^{\mathrm{Ln} y}$
- $\mathrm{I}\Delta_0 + \Omega_1$ is strong enough to formalize consistency

Syntax: Lengths of words (cods) in any model of $\mathrm{I}\Delta_0 + \Omega_1$ is closed under multiplication. So, Polynomial Time computation can be formalized in this theory.

$$x \rightsquigarrow |x|$$

$$x^{|y|} \rightsquigarrow |y|.|x|$$

Bounded Arithmetic

Definition (Polynomial Hierachy)

$$\begin{cases} \Sigma_0^{\mathrm{P}} & = \mathrm{P} \\ \Sigma_{i+1}^{\mathrm{P}} & = \mathrm{NP}\ (\Sigma_i^{\mathrm{P}}) \end{cases}$$

Bounded Arithmetic

Definition (Polynomial Hierachy)

$$\begin{cases} \Sigma_0^{\mathrm{P}} & = \mathrm{P} \\ \Sigma_{i+1}^{\mathrm{P}} & = \mathrm{NP}\ (\Sigma_i^{\mathrm{P}}) \end{cases}$$

- LinH is defined similarly, changing P to L.

Bounded Arithmetic

Definition (Polynomial Hierachy)

$$\begin{cases} \Sigma_0^{\mathrm{P}} & = \mathrm{P} \\ \Sigma_{i+1}^{\mathrm{P}} & = \mathrm{NP}\ (\Sigma_i^{\mathrm{P}}) \end{cases}$$

- LinH is defined similarly, changing P to L.

Fact

$$\Delta_0(\mathbb{N}) = \mathrm{LinH}$$

Bounded Arithmetic

Theorem

$$\mathrm{I}\Delta_0 + \Omega_1 \vdash \text{MRDP} \implies \text{NP} = \text{co-Np}$$

Bounded Arithmetic

Theorem

$$\mathrm{I}\Delta_0 + \Omega_1 \vdash \text{MRDP} \implies \text{NP} = \text{co-Np}$$

Theorem

$$\mathrm{I}\Delta_0 + \Omega_1 \text{ finitely axiomatizable} \implies \text{PH collapses}$$

Buss's theories of Bounded Arithmetic

- Language $= \{0, s, +, \sharp, |x|, \lfloor \frac{1}{2} \rfloor, \leqslant\}$

  with the intended interpretations as follows:

$$
\begin{array}{ll}
|x| & \text{lenght of x (gratest y s.t. } 2^y \leqslant x) \\
\lfloor \dfrac{1}{2} \rfloor & \text{integer part of } \dfrac{x}{2} \\
x \sharp y & = 2^{|x| . |y|}
\end{array}
$$

Buss's theories of Bounded Arithmetic

- Language $= \{0, s, +, \sharp, |x|, \lfloor \frac{1}{2} \rfloor, \leqslant\}$
  with the intended interpretations as follows:

$$
\begin{array}{ll}
|x| & \text{lenght of x (gratest y s.t. } 2^y \leqslant x) \\
\lfloor \frac{1}{2} \rfloor & \text{integer part of } \frac{x}{2} \\
x \sharp y & = 2^{|x|.|y|}
\end{array}
$$

- BASIC : Expressing basic properties of the parameters.

Buss's theories of Bounded Arithmetic

- Language $= \{0, s, +, \sharp, |x|, \lfloor \frac{1}{2} \rfloor, \leqslant\}$
  with the intended interpretations as follows:

$\lvert x \rvert$	lenght of x (gratest y s.t. $2^y \leqslant x$)
$\lfloor \frac{1}{2} \rfloor$	integer part of $\frac{x}{2}$
$x \sharp y$	$= 2^{\lvert x \rvert . \lvert y \rvert}$

- BASIC : Expressing basic properties of the parameters.
- Polynomial Induction PIND:

$$[A(0) \wedge \forall x (A(\lfloor \frac{x}{2} \rfloor) \to A(x))] \to \forall x A(x)$$

.

Σ_i^b and Π_i^b

Definition

- $\Sigma_0^b = \Pi_0^b$ is the class of all sharply bounded formulas.
- The syntactic classes $\Sigma_{i+1}^b, \Pi_{i+1}^b$ of bounded formulas are defined by counting alternations of bounded quantifiers ignoring sharply bounded quantifiers.

Buss's theories of Bounded Arithmetic

$$S_2^i = \mathrm{BASIC} + \Sigma_i^b - \mathsf{PIND}$$
$$S_2 = \bigcup S_2^i$$

Buss's theories of Bounded Arithmetic

$$S_2^i = \mathrm{BASIC} + \Sigma_i^b - \mathsf{PIND}$$

$$S_2 = \bigcup S_2^i$$

Theorem (Buss 1985)

$$\Sigma_i^b(\mathbb{N}) = \Sigma_i^P$$

Σ_1-definable functions

Definition

Let T be an arithmetical theory. A function $f : \mathbb{N}^k \to \mathbb{N}$ is Σ_1-definable in T if there is a Σ_1-formula $\phi(\vec{x}, y)$ such that

1) $\phi(\vec{n}, f(\vec{n}))$ is true, $n \in \mathbb{N}$
2) $T \vdash \forall \vec{x}\ \exists y\ \phi(\vec{x}, y)$

Σ_1-definable functions

Definition

Let T be an arithmetical theory. A function $f : \mathbb{N}^k \to \mathbb{N}$ is Σ_1-definable in T if there is a Σ_1-formula $\phi(\vec{x}, y)$ such that

1) $\phi(\vec{n}, f(\vec{n}))$ is true, $n \in \mathbb{N}$
2) $T \vdash \forall \vec{x}\ \exists y\ \phi(\vec{x}, y)$

Theorem (Parsons, Takeuti, ... 1970)

Σ_1-definable functions of $\mathrm{I}\Sigma_1$ are exactly primitive recursive functions.

Buss's theories of Bounded Arithmetic

Theorem (Buss 1985)

1) Σ_1^b-definable functions of S_2^1 are Polynomial Time computable functions.
2) Δ_1^b-definable predicates of S_2^1 are exactly P-relations.

Buss's theories of Bounded Arithmetic

Theorem (Buss 1985)

1) Σ_1^b-definable functions of S_2^1 are Polynomial Time computable functions.
2) Δ_1^b-definable predicates of S_2^1 are exactly P-relations.

Theorem (Krajicek, Pudlak, Takeuti 1991)

$$\exists i \;\; S_2^i = S_2^{i+1} \implies \text{PH collapses}$$

$\mathrm{I}S^1_2(CU)$

Definitin (Cook, Urquhart 1989-1993)

$\mathrm{I}S^1_2(CU) =$ Intuitionistic theory axiomatized by
$\mathrm{BASIC} + \mathrm{PIND}(\Sigma^{b^+}_1)$

$\mathrm{I}S^1_2(CU)$

Definitin (Cook, Urquhart 1989-1993)

$\mathrm{I}S^1_2(CU) =$ Intuitionistic theory axiomatized by $\mathrm{BASIC} + \mathrm{PIND}(\Sigma^{b^+}_1)$

- $\Sigma^{b^+}_1$: Positive Σ^b_1 (without $\neg$, $\rightarrow$)

$\mathrm{I}S_2^1(CU)$

Definitin (Cook, Urquhart 1989-1993)

$\mathrm{I}S_2^1(CU)$ = Intuitionistic theory axiomatized by $\mathrm{BASIC} + \mathrm{PIND}(\Sigma_1^{b^+})$

- $\Sigma_1^{b^+}$: Positive Σ_1^b (without $\neg$, $\rightarrow$)
- They independently proved the main theorem of S_2^1 for $\mathrm{I}S_2^1(CU)$.

$\mathrm{I}S_2^1(B)$

Another intuitionistic version of S_2^1 intruduced by Buss himself.

Definitin

$\mathrm{I}S_2^1(B) =$ Intuitionistic theory axiomatized by all consequence of S_2^1 of the form $(B_1 \wedge \cdots \wedge B_m) \rightarrow B_{m+1}$ where B_i is $\mathrm{H}\Sigma_1^b + \mathsf{PIND}(\mathrm{H}\Sigma_1^b)$.

$\mathrm{I}S_2^1(B)$

Another intuitionistic version of S_2^1 intruduced by Buss himself.

Definitin

$\mathrm{I}S_2^1(B)$ = Intuitionistic theory axiomatized by all consequence of S_2^1 of the form $(B_1 \wedge \cdots \wedge B_m) \to B_{m+1}$ where B_i is $\mathrm{H}\Sigma_1^b + \mathrm{PIND}(\mathrm{H}\Sigma_1^b)$.

- $\mathrm{H}\Sigma_1^b$ = hereditavy Σ_1^b = the set of formulas A such that each subformula of A is Σ_1^b.

$\mathrm{I}S^1_2(B)$

Another intuitionistic version of S^1_2 intruduced by Buss himself.

Definitin

$\mathrm{I}S^1_2(B) =$ Intuitionistic theory axiomatized by all consequence of S^1_2 of the form $(B_1 \wedge \cdots \wedge B_m) \to B_{m+1}$ where B_i is $\mathrm{H}\Sigma^b_1 + \mathrm{PIND}(\mathrm{H}\Sigma^b_1)$.

- $\mathrm{H}\Sigma^b_1 =$ hereditavy $\Sigma^b_1 =$ the set of formulas A such that each subformula of A is Σ^b_1.

Theorem (Buss 1992)

$$\mathrm{I}S^1_2(B) = \mathrm{I}S^1_2(CU)$$

$\mathrm{I}S_2^n$

Generalizing $\mathrm{I}S_2^1$ to $\mathrm{I}S_2^n$:

- $\mathrm{I}S_2^n(B)$ (1986)
- $\mathrm{I}S_2^n(H)$ (Victor Harnic, JSL 1992)

$\mathrm{PV_n}$

$\mathrm{PV_n}$: Originally defined by Cook for level 1 and extended by Harnik for each n.

Definitin (Harnik)

- $\mathrm{I}S_2^n = \mathrm{BASIC} + \mathrm{PEM}(\Sigma_{n-1}^{\mathrm{b}} \cup \Pi_{n-1}^{\mathrm{b}}) + \mathrm{PIND}(\Sigma_n^{\mathrm{b}^+})$.
- $\mathrm{IPV_n} = \mathrm{I}S_2^n(\mathrm{PV_n})$
- $\mathrm{PV_n}$ = Equational theory for Π_n^{P}-functions (level n of the PH for functions)
- $\mathrm{CPV_n}$ = Classical version of $\mathrm{IPV_n}$.

$\mathrm{PV_n}$

Theorem (MM 2009)

1) If $\mathrm{CPV_n} \vdash \forall x \, \exists y \, A$ then $\mathrm{IPV_n} \vdash \forall x \, \exists y \, A$,
2) If $S_2^n \vdash \forall x \, \exists y \, A$ then $\mathrm{I}S_2^n \vdash \forall x \, \exists y \, A$.

where A is a positive Σ_n^b-formula.

Proof.

Use Jeremy Avigad's forcing method (Avigad 2002-2004). $\square$

CU

Definition (CU)

- $\mathrm{IPV} = \mathrm{I}S_2^1(\mathrm{PV})$
- $\mathrm{IPV}^+ = \mathrm{PV}+$ PIND over formulas of the form $(A(x) \vee B)$
- $\mathrm{IPV}^* = \mathrm{PV}+$ PIND $(\neg\neg A(x))$

$A(x)$ an NP-formula (of the form $\exists x \leq t\ (r = s)$)

CU

Definition (CU)

- $\mathrm{IPV} = \mathrm{I}S_2^1(\mathrm{PV})$
- $\mathrm{IPV}^+ = \mathrm{PV}+$ PIND over formulas of the form $(A(x) \vee B)$
- $\mathrm{IPV}^* = \mathrm{PV}+$ PIND $(\neg\neg A(x))$

$A(x)$ an NP-formula (of the form $\exists x \leq t\ (r = s)$)

Questions (CU 1993)

- $\mathrm{IPV} =^? \mathrm{IPV}^+$
- $\mathrm{IPV} =^? \mathrm{IPV}^*$

CU

Theorem (MM 2003)

Answer is 'probably' No

- $\mathrm{IPV}=\mathrm{IPV}^{+} \implies \mathrm{CPV}=\mathrm{PV} \implies$ PH collapses.
- $\mathrm{IPV}=\mathrm{IPV}^{*} \implies \mathrm{CPV}=\mathrm{PV} \implies$ PH collapses.

CU

Proof.

By using Kripke models of IPV. Note that

$$(\mathrm{IPV}^{+})^{c} = (\mathrm{IPV}^{*})^{c} = \mathrm{CPV}$$

CU

Proof.

By using Kripke models of IPV. Note that

$$(\mathrm{IPV}^+)^c = (\mathrm{IPV}^*)^c = \mathrm{CPV}$$

- For IPV^+ : Consider $M \models \mathrm{PV}$ and $M \not\models \mathrm{CPV}$. M can be Σ_1^b-elementary embeded in a model M' of CPV. Now consider two-node Kripke model M' above M. K forces IPV but not IPV^+.

CU

Proof.

By using Kripke models of IPV. Note that

$$(\mathrm{IPV}^{+})^{c} = (\mathrm{IPV}^{*})^{c} = \mathrm{CPV}$$

- For IPV^{+} : Consider $M \models \mathrm{PV}$ and $M \not\models \mathrm{CPV}$. M can be Σ_1^b-elementary embeded in a model M' of CPV. Now consider two-node Kripke model M' above M. K forces IPV but not IPV^{+}.
- For IPV^{*} : The union of the worlds in any linear Kripke model of IPV^{*}, satisfies CPV. Any chain of CPV-models is a K. M. of IPV^{*}. So, if $\mathrm{IPV}{=}\mathrm{IPV}^{*}$, the class of models of CPV is closed under union of chain. So, CPV world be $\forall_2$-axiomatized. Therefore, as CPV is $\forall_2$-conservative over PV, we have $\mathrm{CPV} = \mathrm{PV}$.

□

$\mathrm{I}S_2^i(B)$

We alredy defined $\mathrm{I}S_2^n(H)$.

- $\mathrm{I}S_2^n(B)$: The set of all consequences of S_n^i of the form $(A_1 \wedge \cdots \wedge A_n) \rightarrow B$ where $A_i, B \in \mathrm{H}\Sigma_n^b$ plus Polynomial Induction on $\mathrm{H}\Sigma_n^b$-formulas.
- $\mathrm{H}\Sigma_n^b$: The class of all formulas A such that all subformulas of A is Σ_n^b.

$\mathrm{I}S^i_2(B)$

Theorem (MM 2008)

$$\forall i \;\; \mathrm{I}S^i_2(B) = \mathrm{I}S^i_2(H)$$

Proof.

A generalization of Buss's proof using a sequent calculus ~~from~~ of $\mathrm{I}S^i_2$. □

form

Thank you for your attention