Herbrand Consistency of $\mathrm{I}\Delta_0$ and $\mathrm{I}\Delta_0 + \Omega_1$

Saeed Salehi

University of Tabriz

http://SaeedSalehi.ir/

Logical Approaches to Barriers in Computing and Complexity

17–20 February 2010 || Greifswald, Germany

Outline

Bounded Induction

- Bounded Formula
- Bounded Arithmetic

Language of Arithmetic

- $\mathcal{L}_A = \langle 0, 1, +, \cdot, < \rangle$
- $\mathcal{L}_A = \langle 0, \mathrm{S}, +, \cdot, \leq \rangle$

$\mathrm{S}(x) = x + 1$	$x \leq y \iff x < y \vee x = y$
$1 = \mathrm{S}(0)$	$x < y \iff x \leq y \wedge x \neq y$

Terms $\Longleftrightarrow$ Polynomials

Bounded Quantifiers

- All $\exists x$ are in the form $\exists x \leq t$
- All $\forall y$ are in the form $\forall y \leq s$

t, s are $\cdots$ terms

Bounded Formula: all quantifiers are bounded.

- Relations definable by bounded formulas are
  - Decidable
  - Primitive Recursive
  - Recognizable in Linear Space [LinSpace $=$ Space $\in \mathcal{O}(n)$]
  - Recognizable in the Linear Time Hierarchy

Peano Arithmetic

Robinson's Arithmetic Q:

- $\mathrm{S}(x) = \mathrm{S}(y) \Rightarrow x = y$
- $x + 0 = x$
- $x \cdot 0 = 0$
- $x \leq y \iff \exists z(x + z = y)$
- $\mathrm{S}(x) \neq 0$
- $x + \mathrm{S}(y) = \mathrm{S}(x + y)$
- $x \cdot \mathrm{S}(y) = (x \cdot y) + x$
- $x \neq 0 \Rightarrow \exists y[x = \mathrm{S}(y)]$

Plus the Induction Axioms:

$$\varphi(0) \wedge \forall x[\varphi(x) \rightarrow \varphi(\mathrm{S}(x))] \Longrightarrow \forall y \varphi(y)$$

Bounded Induction

Definition

Q + Induction Axiom for Bounded Formulas $=$ $\mathrm{I}\Delta_0$

Theorem (*R.J. Parikh 1971*)

$\mathrm{I}\Delta_0 \vdash \forall\overline{x}\exists y\ \eta(\overline{x},y)\ \&\ \eta\in\Delta_0 \Longrightarrow \mathrm{I}\Delta_0 \vdash \forall\overline{x}\ \exists y\le t(\overline{x})\ \eta(\overline{x},y)$

$t-$*term*

Provably Recursive Functions of $\mathrm{I}\Delta_0$ are Polynomially Bounded

$$\mathrm{I}\Delta_0 \vdash \forall\overline{x}\exists y\ \underbrace{\eta(\overline{x},y)}_{\Delta_0} \Longrightarrow \mathrm{I}\Delta_0 \vdash \forall\overline{x}\ \underbrace{\exists y\le t(\overline{x})\eta(\overline{x},y)}_{\Delta_0}$$

Why Bounded Arithmetic ?

$x \mid y \equiv \exists z(x \cdot z = y)$ $\qquad$ $\mathtt{Prime}(x) \equiv \forall y(y \mid x \Rightarrow y = 1 \vee y = x)$

PA=Peano Arithmetic $\qquad$ $\mathrm{PA} \vdash \forall x \exists y \Big(y > x \wedge \mathtt{Prime}(y) \Big)$

Open Problem: $\qquad$ $\mathrm{I}\Delta_0 \vdash^{?} \forall x \exists y \Big(y > x \wedge \mathtt{Prime}(y) \Big)$

$\mathrm{Exp} = \forall x \exists y [y = 2^x]$ $\qquad$ $\text{“ } y = 2^x \text{ ”} \in \Delta_0$

$\mathrm{EA} = \mathrm{I}\Delta_0 + \mathrm{Exp}$ $\qquad$ $\mathrm{EA} \vdash \forall x \exists y \Big(y > x \wedge \mathtt{Prime}(y) \Big)$

Elementary Arithmetic

More Bounded Arithmetic

Definition

$$\begin{cases} \omega_0(x) = x^2 \\ \omega_{n+1}(x) = 2^{\omega_n(\log x)} \end{cases} \qquad \omega_1(x) = 2^{\log x \cdot \log x} \sim x^{\log x}$$

$$\text{polynomial}(x) \ll \omega_1(x) \ll \omega_2(x) \ll \cdots \ll 2^x$$

Definition

$$\Omega_m = \forall x \exists y [y = \omega_m(x)] \qquad \text{“ } y = \omega_m(x) \text{ ”} \in \Delta_0$$

$$\mathrm{I}\Delta_0 \subsetneqq \mathrm{I}\Delta_0 + \Omega_1 \subsetneqq \mathrm{I}\Delta_0 + \Omega_2 \subsetneqq \cdots \subsetneqq \mathrm{I}\Delta_0 + \mathrm{Exp}$$

Gödel's 2nd Incompleteness Theorem

- Π_1-Separation
- Herbrand Consistency

Unprovabilty of Consistency

$$\mathcal{Con}(\mathrm{T}) \;=\; \text{“ T is consistent ”} \;=\forall z\neg\underbrace{\mathtt{Proof}_{\mathrm{T}}}_{\Delta_0}(z,\ulcorner 0=1\urcorner)\in\Pi_1$$

Gödel's Second Incompleteness Theorem

$\mathrm{PA}\nvdash\mathcal{Con}(\mathrm{PA})$ $\qquad$ $\mathrm{ZFC}\vdash\mathcal{Con}(\mathrm{PA})$

$\mathrm{I}\Delta_0\nvdash\mathcal{Con}(\mathrm{I}\Delta_0)$ $\qquad$ $\mathrm{PA}\vdash\mathcal{Con}(\mathrm{I}\Delta_0)$

But $\mathrm{I}\Delta_0+\mathrm{Exp}\nvdash\mathcal{Con}(\mathrm{I}\Delta_0)$! $\qquad$ How $\mathrm{I}\Delta_0+\mathrm{Exp}\supsetneqq^{\Pi_1}\mathrm{I}\Delta_0$?

Open Problem: Π_1-Separating the Hierarchy $\{\mathrm{I}\Delta_0+\Omega_m\}_m$

Herbrand Consistency 1

- Skolemizing: $\exists y \rightsquigarrow$ eliminate $\exists$ & $[\mathfrak{f}(\overline{x}) \hookleftarrow y]$ $\mathfrak{f}$ new symbol
  $\overline{x}$ all the universal variables before y

then eliminating the remaining $\forall$ quantifiers

Examples:

- $\forall x \exists y \varrho(x, y) \longrightarrow^{\mathrm{Sk}} \longrightarrow \varrho(x, \mathfrak{f}(x))$
- $\exists y \forall u \exists z \rho(y, u, z) \longrightarrow^{\mathrm{Sk}} \longrightarrow \rho(\mathfrak{c}, u, \mathfrak{f}(u))$

- T is Consistent $\iff$ T^{Sk} is Consistent
  `First-Order` $\leftrightsquigarrow$ `Propositional`

Herbrand Consistency 2

Definition

Herbrand Consistency of T = Propositional Satisfiability of every finite set of (Skolem) instances of T

$$\mathrm{I}\Delta_0 + \mathrm{SupExp} \vdash \mathcal{HC}on(\mathrm{T}) \longleftrightarrow \mathcal{C}on(\mathrm{T})$$
$$\mathrm{I}\Delta_0 \nvdash \mathcal{HC}on(\mathrm{T}) \longleftrightarrow \mathcal{C}on(\mathrm{T})$$

$$\mathrm{I}\Delta_0 + \mathrm{Exp} \vdash \mathcal{HC}on(\mathrm{I}\Delta_0)$$

After 20 Years ... $\mathrm{I}\Delta_0 \nvdash \mathcal{HC}on(\mathrm{I}\Delta_0)$

Logarithmic Witnesses 1

Definition

$\log^n y = \log \cdots \log y$ ($n-$times) $\qquad \mathsf{LOG}^n = \{x \mid \exists y[x = \log^n y]\}$

Theorem (*Z. Adamowicz 2002*)

1 If $\theta \in \Delta_0$ & $m \geq 2$, then the Consistency of
$\mathcal{HC}\mathfrak{on}_{m-2}(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + (\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists \overline{x} \in \mathsf{LOG}^{m+1}\theta(\overline{x})$
implies the Consistency of $(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists \overline{x} \in \mathsf{LOG}^{m+2}\theta(\overline{x})$

where $\mathcal{HC}\mathfrak{on}_{m-2}$ is $\mathcal{HC}\mathfrak{on}$ restricted to the cut LOG^{m-2}.

Logarithmic Witnesses 2

Theorem (*Z. Adamowicz 2002*)

2 For any $m, n \geq 0$ there exists a $\eta(x) \in \Delta_0$ such that
$(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists x \in \mathsf{LOG}^n\ \eta(x)$ is Consistent, but
$(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists x \in \mathsf{LOG}^{n+1}\ \eta(x)$ is NOT Consistent

---

When $\mathcal{HC}\mathfrak{on}$ is Present
one can Shrink any LOG^m-witness *logarithmically*
But not always (when $\mathcal{HC}\mathfrak{on}$ is not present).

Two Theorems Again

Theorem (*Z. Adamowicz 2002*)

1 If $\theta \in \Delta_0$ & $m \geq 2$, then the Consistency of
$$\mathcal{HCon}_{m-2}(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + (\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists \overline{x} \in \mathsf{LOG}^{m+1}\theta(\overline{x})$$
implies the Consistency of $(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists \overline{x} \in \mathsf{LOG}^{m+2}\theta(\overline{x})$

Theorem (*Z. Adamowicz 2002*)

2 For any $m, n \geq 0$ there exists a $\eta(x) \in \Delta_0$ such that
$(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists x \in \mathsf{LOG}^n\ \eta(x)$ is Consistent, but
$(\mathrm{I}\Delta_0 + \Omega_\mathrm{m}) + \exists x \in \mathsf{LOG}^{n+1}\ \eta(x)$ is NOT Consistent

Proof of Unprovabilty

Thus $(n = m+1)$ $\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}} \nvdash \mathcal{HC}\mathfrak{on}_{m-2}(\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}})$ for $m \geq 2$:

Proof.

by 2, $\exists\eta$ s.t. (a) $\mathsf{Con}\Big((\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) + \exists x \in \mathsf{Log}^{m+1}\ \eta(x)\Big)$

but (b) $\neg\mathsf{Con}\Big((\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) + \exists x \in \mathsf{Log}^{m+2}\ \eta(x)\Big)$

If $\mathcal{HC}\mathfrak{on}_{m-2}(\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) + (\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) = (\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}})$,

then (a)+1 imply $\mathsf{Con}\Big((\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) + \exists x \in \mathsf{Log}^{m+2}\ \eta(x)\Big)$

contradiction with (b). □

In Particular $\mathrm{I}\Delta_0 + \Omega_2 \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0 + \Omega_2)$

Logarithmic Witnesses in $\mathrm{I}\Delta_0+\Omega_1$

Not Good for Π_1-Separating:

Theorem (*L.A. Kołodziejczyk 2006*)

$\bigcup_n(\mathrm{I}\Delta_0+\Omega_n) \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0+\Omega_m)$ for $m \geq 2$

Theorem (*S. Salehi 2002*)

1' The Consistency of the theory
$$\mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0+\Omega_1)+(\mathrm{I}\Delta_0+\Omega_1)+\exists\overline{x}\in\mathsf{Log}^2\theta(\overline{x})$$
implies the Consistency of
$$(\mathrm{I}\Delta_0+\Omega_1)+\exists\overline{x}\in\mathsf{Log}^3\theta(\overline{x})$$

Corollary $\mathrm{I}\Delta_0+\Omega_1 \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0+\Omega_1)$

New Results

- Pseudo-Logarithmic Cuts

Logarithmic Witnesses in $\mathrm{I}\Delta_0$

Definition

$$\mathcal{I} := \{x \mid \exists y[y = 2^{\omega_1^2(x)}]\} \qquad \mathcal{J} := \{x \mid \exists y[y = 2^{2^{x^4}}]\}$$

$$\omega_1^2(2^x) = \omega_1\left(2^{x^2}\right) = 2^{x^4} \longrightarrow 2^{\omega_1^2(2^x)} = 2^{2^{x^4}}$$

$$2^x \in \mathcal{I} \iff x \in \mathcal{J} \qquad \lhd\!\!-\!\!\rhd \qquad \mathcal{J} = \log \mathcal{I}$$

Theorem (*S. Salehi 2010*)

- The Consistency of the theory
$$\mathcal{HC}\mathrm{on}(\mathrm{I}\Delta_0+\Omega_0)+\mathrm{I}\Delta_0+\exists \overline{x}\in\mathcal{I}\theta(\overline{x})$$
implies the Consistency of
$$\mathrm{I}\Delta_0+\exists \overline{x}\in\mathcal{J}\theta(\overline{x})$$

recall $\Omega_0 = \forall x \exists y\left(y = x \cdot x\right)$!

Inside $\mathrm{I}\Delta_0$

Theorem (*S. Salehi 2010*)

2' There Exists a $\eta(x) \in \Delta_0$ such that
$\mathrm{I}\Delta_0 + \exists x \in \mathcal{I}\ \eta(x)$ is Consistent, but
$\mathrm{I}\Delta_0 + \exists x \in \mathcal{J}\ \eta(x)$ is NOT Consistent

Corollary $\mathrm{I}\Delta_0 = \mathrm{I}\Delta_0 + \Omega_0 \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0 + \Omega_0)$

$\Omega_0 = \forall x \exists y [y = \omega_0(x) = x^2]$ $\qquad$ ${\Omega_0}^{\mathrm{Sk}} \Longleftrightarrow \mathfrak{f}(x) = x^2$

$$\mathfrak{f}^n(\alpha) = (\ldots((\alpha^2)^2)^{\cdots})^2 = \underbrace{\alpha \cdot \alpha \cdot \alpha \ldots \alpha}_{2^n-\text{times}} = \alpha^{2^n}$$

$\ulcorner \mathfrak{f}^n(2) \urcorner \sim 2^n$ $\qquad$ $\mathfrak{f}^n(2) = 2^{2^n}$

Farewell

- Open Problems
- References

Future Works ?

Conjecture

1. $\bigcup_n(\mathrm{I}\Delta_0+\Omega_n) \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0+\Omega_1)$
2. $\bigcup_n(\mathrm{I}\Delta_0+\Omega_n) \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0+\Omega_0)$

Problems

1. $\bigcup_n(\mathrm{I}\Delta_0+\Omega_n) \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{I}\Delta_0)$ for a good definition of $\mathcal{HC}\mathfrak{on}$
2. Proving GST $\quad \mathrm{T} \nvdash \mathcal{HC}\mathfrak{on}(\mathrm{T}) \quad$ *nicely and neatly*
   for every $\mathrm{T} \supseteq Q-$Robinson's Arithmetic

References


Z. Adamowicz.
Herbrand Consistency and Bounded Arithmetic.
Fundamenta Mathematicae **171**, 279–292 (2002).


L.A. Kołodziejczyk.
On the Herbrand Notion of Consistency for Finitely Axiomatizable Fragments of Bounded Arithmetic Theories.
Journal of Symbolic Logic **71**, 624–638 (2006).


S. Salehi.
Herbrand Consistency in Arithmetics with Bounded Induction.
Ph.D. Dissertation, Inst. Math. Polish Academy Sci (2002).

Thank You!

Thanks to

The Participants . . . . . For Listening...

and

The Organizers . . . . For Taking Care of Everything...

SAEEDSALEHI.ir