Logarithmic Witnesses in Bounded Induction

SAEED SALEHI

University of Tabriz

http://SaeedSalehi.ir/

IPM Logic Seminar
December 30–31, 2009

Outline

1. Bounded Induction
   - Bounded Formulae
   - Bounded Arithmetic
2. Gödel's 2nd Incompleteness Theorem
   - Π_1-Separation
   - Herbrand Consistency
3. New Results
   - Pseudo-Logarithmic Cuts
   - Computations
4. Farewell

Logarithmic Witnesses in Bounded Induction IPM Logic Seminar, Dec. 31' 2009

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 $\iff$ 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:

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

Bounded Induction

Definition

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

Theorem

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

$t-$*term*

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

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

Why Bounded Arithmetic?

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

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

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

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

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

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

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

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

Unprovability of Consistency

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

$\mathbf{PA} \nvdash \texttt{Con}(\mathbf{PA})$ $\mathbf{ZFC} \vdash \texttt{Con}(\mathbf{PA})$

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

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

Herbrand Consistency

- Skolemizing: $\exists y \rightsquigarrow$ eliminate $\exists$ & $[f(\overline{x}) \hookleftarrow y]$ f new symbol
  $\overline{x}$ all the universal variables before y
  - T is Consistent $\iff$ T^{Sk} is Consistent

Definition

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

$$\mathrm{I}\Delta_0 + \mathrm{SupExp} \vdash \mathtt{HCon}(\mathbf{T}) \longleftrightarrow \mathtt{Con}(\mathbf{T})$$
$$\mathrm{I}\Delta_0 \nvdash \mathtt{HCon}(\mathbf{T}) \longleftrightarrow \mathtt{Con}(\mathbf{T})$$

$\mathrm{I}\Delta_0 + \mathrm{Exp} \vdash \mathtt{HCon}(\mathrm{I}\Delta_0)$ $\mathrm{I}\Delta_0 \nvdash \mathtt{HCon}(\mathrm{I}\Delta_0)$?

$\mathrm{I}\Delta_0 + \mathrm{Exp} \nvdash \mathtt{Con}(\mathrm{I}\Delta_0)$ ✓

Logarithmic Witnesses 1

Definition

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

Theorem

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

where $\texttt{HCon}_{m-2}$ is $\texttt{HCon}$ restricted to the cut $\textsc{Log}^{m-2}$.

Logarithmic Witnesses 2

Theorem

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

---

When `HCon` is Present
one can Shrink any $\textsc{Log}^m-$witness *logarithmically*
But not always (when `HCon` is not present)

Proof of Unprovability

Thus ($n = m+1$) $\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}} \nvdash \mathtt{HCon}_{m-2}(\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}})$ for $m \geq 2$:

Proof.

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

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

If $\mathtt{HCon}_{m-2}(\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) + (\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}}) = (\mathrm{I}\Delta_0 + \Omega_{\mathrm{m}})$,

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

contradiction with (b). $\square$

In Particular $\mathrm{I}\Delta_0 + \Omega_2 \nvdash \mathtt{HCon}(\mathrm{I}\Delta_0 + \Omega_2)$

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

Not Good for Π_1-Separating:

Theorem

$\bigcup_n(\mathrm{I}\Delta_0 + \Omega_\mathrm{n}) \nvdash \mathtt{HCon}(\mathrm{I}\Delta_0 + \Omega_\mathrm{m})$ for $m \geq 2$

Theorem

1' The Consistency of the theory

$$\mathtt{HCon}(\mathrm{I}\Delta_0 + \Omega_1) + (\mathrm{I}\Delta_0 + \Omega_1) + \exists \overline{x} \in \mathsf{Log}^2 \theta(\overline{x})$$

implies the Consistency of

$$(\mathrm{I}\Delta_0 + \Omega_1) + \exists \overline{x} \in \mathsf{Log}^3 \theta(\overline{x})$$

Corollary $\mathrm{I}\Delta_0 + \Omega_1 \nvdash \mathtt{HCon}(\mathrm{I}\Delta_0 + \Omega_1)$

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

Definition

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

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

$$2^x \in \mathcal{I} \iff x \in \mathcal{J} \qquad\qquad \mathcal{J} = \log \mathcal{I}$$

Theorem

- The Consistency of the theory
  $$\mathtt{HCon}(\mathbb{I}\triangle_0) + \mathrm{I}\Delta_0 + \exists \overline{x} \in \mathcal{I} \theta(\overline{x})$$
  implies the Consistency of $\mathrm{I}\Delta_0 + \exists \overline{x} \in \mathcal{J} \theta(\overline{x})$

where $\mathbb{I}\triangle_0 \ = \ \mathrm{I}\Delta_0 \ + \ \forall x \exists y[y = x \cdot x]$!

Inside $\mathrm{I}\Delta_0$

Theorem

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 $\mathrm{I}\Delta_0 \nvdash \mathtt{HCon}(\mathbb{I}\triangle_0)$

$\mathbb{I}\triangle_0 = \mathrm{I}\Delta_0 + \Omega_0$

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

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

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

Some Dirty Computations

$$p(x) \ll x^{\log^2 x} \ll \omega_1(x) \ll \omega_2(x) = 2^{2^{\log^2 x \cdot \log^2 x}} \ll \cdots \ll 2^x$$

$\ulcorner\langle\alpha\rangle\urcorner \leq 9(\ulcorner\alpha\urcorner + 1)^2$ $\ulcorner A \frown B \urcorner$ $(\ulcorner A \cup B \urcorner) \leq 64 \cdot (\ulcorner A \urcorner \cdot \ulcorner B \urcorner)$

$\mathtt{length}(A)$ $(|A|) \leq (\log \ulcorner A \urcorner)$ $\ulcorner p \urcorner \leq \mathcal{P}\Big(\omega_1(\ulcorner\Lambda\urcorner)\Big)$ $\prod_{t,s\in\Lambda} \ulcorner t \urcorner \cdot \ulcorner s \urcorner =$

$\prod_{t\in\Lambda} (\ulcorner t \urcorner)^{2|\Lambda|} = (\prod_{t\in\Lambda} \ulcorner t \urcorner)^{2|\Lambda|} \leq \mathcal{P}(\ulcorner\Lambda\urcorner)^{2\log\ulcorner\Lambda\urcorner} \leq \mathcal{P}(\ulcorner\Lambda\urcorner^{\log\ulcorner\Lambda\urcorner})$

$\ulcorner\Lambda\urcorner^{\log\ulcorner\Lambda\urcorner} \leq \exp(\log\ulcorner\Lambda\urcorner)^{\log\ulcorner\Lambda\urcorner} = \exp\left((\log\ulcorner\Lambda\urcorner)^2\right) = \omega_1(\ulcorner\Lambda\urcorner)$ $\Lambda^{\langle 0 \rangle} = \Lambda$

$$\Lambda^{\langle k+1 \rangle} = \Lambda^{\langle k \rangle} \cup \{f(t_1, \ldots, t_m) \mid f \in \mathcal{L} \ \& \ t_1, \ldots, t_m \in \Lambda^{\langle k \rangle}\}$$

$$\cup \{\mathfrak{f}_{\exists x \psi(x)}(t_1, \ldots, t_m) \mid \ulcorner\psi\urcorner \leq k \ \& \ t_1, \ldots, t_m \in \Lambda^{\langle k \rangle}\}$$

$|\Lambda^{\langle n \rangle}| \leq \mathcal{P}\left((n!)^{n!}|\Lambda|^{n!}\right)$ $\ulcorner\Lambda^{\langle n \rangle}\urcorner \leq \mathcal{P}\left(\left(\ulcorner\Lambda\urcorner\right)^{|\Lambda|^{(n+1)!}}\right)$

$$2(j+1)! \leq 2^{2^j} \leq \log^2\ulcorner\Lambda\urcorner$$

$$\ulcorner\Lambda^{\langle j \rangle}\urcorner \leq \mathcal{P}\left(\left(\ulcorner\Lambda\urcorner\right)^{|\Lambda|^{(j+1)!}}\right) \leq \mathcal{P}\left(\left(2^{\log\ulcorner\Lambda\urcorner + 1}\right)^{(\log\ulcorner\Lambda\urcorner)^{(j+1)!}}\right) \leq$$

$$\mathcal{P}\left(\exp\left((\log\ulcorner\Lambda\urcorner)^{2(j+1)!}\right)\right) \leq \mathcal{P}\left(\exp\left(\omega_1(\log\ulcorner\Lambda\urcorner)\right)\right)$$

Next Talk:

Logical Approaches to Barriers in Computing and Complexity

The DVMLG, the PTLiFN, the ACiE and the EACSL jointly organize a workshop on Logical Approaches to Barriers in Computing and Complexity. The workshop is sponsored by the Stiftung Alfried Krupp Kolleg Greifswald and the DFG, and takes place at the Alfried Krupp Wissenschaftskolleg in the city of Greifswald in Germany.

Date of the Workshop: 17 - 20 February 2010

http://www.cs.swan.ac.uk/greifswald2010/

Programme Committee

- Zofia Adamowicz (Warsaw, Poland)
- Franz Baader (Dresden, Germany)
- Arnold Beckmann (**chair**; Swansea, Wales)
- Sam Buss (La Jolla CA, U.S.A.)
- Manfred Droste (Leipzig, Germany)
- Christine Gaßner (Greifswald, Germany)
- Peter Koepke (Bonn, Germany)
- Benedikt Löwe (Amsterdam, The Netherlands)
- Johann Makowsky (Haifa, Israel)
- Elvira Mayordomo (Zaragoza, Spain)
- Damian Niwinski (Warsaw, Poland)
- Wolfgang Thomas (Aachen, Germany)
- Martin Ziegler (Darmstadt, Germany)

Future Works ?

Conjecture

1. $\bigcup_n (\mathrm{I}\Delta_0 + \Omega_\mathrm{n}) \nvdash \texttt{HCon}(\mathrm{I}\Delta_0 + \Omega_1)$
2. $\bigcup_n (\mathrm{I}\Delta_0 + \Omega_\mathrm{n}) \nvdash \texttt{HCon}(\mathrm{I}\Delta_0 + \Omega_0) = \texttt{HCon}(\mathbb{I}\triangle_0)$

Problems

1. $\bigcup_n (\mathrm{I}\Delta_0 + \Omega_\mathrm{n}) \nvdash \texttt{HCon}(\mathrm{I}\Delta_0)$ for a good definition of $\texttt{HCon}$
2. Proving GST $\mathrm{T} \nvdash \texttt{HCon}(\mathrm{T})$ *nicely and neatly*
   for every $\mathrm{T} \supseteq Q$–Robinson's Arithmetic

Thank You!

Thanks to the

Participants

and The Organizers of the

IPM Logic Seminar
December 30–31, 2009

SAEEDSALEHI.ir