A Model Theoretic Characterization of
$I\Delta_0 + Exp + B\Sigma_1$

Ali Enayat

IPM Logic Conference

June 2007
• **Theorem** (MacDowell-Specker) *Every model of PA has an elementary end extension.*

• **Proof:**

(1) Construct an ultrafilter $\mathcal{U}$ on the parametrically definable subsets of $\mathcal{M}$ with the property that every definable map with bounded range is constant on a member of $\mathcal{U}$ (this is similar to building a $p$-point in $\beta\omega$ using CH).

(2) Let $\prod_{\mathcal{U}} \mathcal{M}$ be the Skolem ultrapower of $\mathcal{M}$ modulo $\mathcal{U}$. Then

$$\mathcal{M} \preceq_e \prod_{\mathcal{U}} \mathcal{M}.$$
Characterizing PA (2)

• For each parametrically definable $X \subseteq M$, and $m \in M$,

$$(X)_m = \{x \in M : \langle m, x \rangle \in X \}.$$

• $\mathcal{U}$ is an * iterable ultrafilter if for every $X \in \mathcal{B}$, \{m \in M : (X)_m \in \mathcal{U}\} is definable in $\mathcal{M}$.

• **Theorem** (Gaifman). Let $\mathcal{M}^*$ be the $\mathbb{Z}$-iterated ultrapower of $\mathcal{M}$ modulo an iterable nonprincipal ultrafilter $\mathcal{U}$. Then for some $j \in Aut(\mathcal{M}^*)$

$$fix(j) = M.$$
Characterizing PA (3)

- Given a language $\mathcal{L} \supseteq \mathcal{L}_A$, an $\mathcal{L}$-formula $\varphi$ is said to be a $\Delta_0(\mathcal{L})$-formula if all the quantifiers of $\varphi$ are bounded by terms of $\mathcal{L}$, i.e., they are of the form $\exists x \leq t$, or of the form $\forall x \leq t$, where $t$ is a term of $\mathcal{L}$ not involving $x$.

- *Bounded arithmetic*, or $I\Delta_0$, is the fragment of Peano arithmetic with the induction scheme limited to $\Delta_0$-formulae.

- $I$ is a *strong cut* of $\mathcal{M} \models I\Delta_0$, if for each function $f$ whose graph is coded in $M$, and whose domain includes $M$, there is some $s$ in $M$, such that for all $i \in I$,

  \[ f(i) \notin I \iff s < f(i). \]
Characterizing PA (4)

• **Theorem** (Kirby-Paris). *Strong cuts are models of PA.*

• **Theorem.** *If* $\mathcal{M} \models I\Delta_0$ *and* $j \in Aut(\mathcal{M})$ *with* $\text{fix}(j) \subsetneq e\mathcal{M}$, *then* $\text{fix}(j)$ *is a strong cut of* $\mathcal{M}$. 

• **Theorem.** *The following are equivalent for a model* $\mathcal{M} \models I\Delta_0$:

  (a) $\mathcal{M} \models PA$;

  (b) *There is some* $\mathcal{M}^* \supsetneq e\mathcal{M}$ *and some* $j \in Aut(\mathcal{M}^*)$ *such that* $\mathcal{M}^* \models I\Delta_0$ *and* $\text{fix}(j) = \mathcal{M}$. 
Set Theory and Combinatorics within $I\Delta_0$ (1)

- Bennett showed that the graph of the exponential function $y = 2^x$ can be defined by a $\Delta_0$-predicate in the standard model of arithmetic. This result was later fine-tuned by Paris who found another $\Delta_0$-predicate $Exp(x, y)$ which has the additional feature that $I\Delta_0$ can prove the usual algebraic laws about exponentiation for $Exp(x, y)$.

- One can use Ackermann coding to simulate finite set theory and combinatorics within $I\Delta_0$ by using a $\Delta_0$-predicate $E(x, y)$ that expresses “the $x$-th digit in the binary expansion of $y$ is 1”.

- $E$ in many ways behaves like the membership relation $\in$; indeed, it is well-known that $\mathcal{M}$ is a model of $PA$ iff $(M, E)$ is a model of $ZF\setminus\{\text{Infinity}\} \cup \{\neg\text{Infinity}\}$.
Set Theory and Combinatorics within $I\Delta_0$ (2)

- **Theorem** If $\mathcal{M} \models I\Delta_0(\mathcal{L})$, and $E$ is Ackermann’s $\in$, then $\mathcal{M}$ satisfies the following axioms:

(a) Extensionality;

(b) Conditional Pairing $[\forall x \forall y \text{ “if } x < y \text{ and } 2^y \text{ exists, then } \{x, y\} \text{ exists”}]$;

(c) Union;

(d) Conditional Power Set $[\forall x (\text{“If } 2^x \text{ exists, then the power set of } x \text{ exists”})]$;

(e) Conditional $\Delta_0(\mathcal{L})$-Comprehension Scheme: for each formula $\Delta_0(\mathcal{L})$-formula $\varphi(x, y)$, and any $z$ for which $2^z$ exists, $\{xEz : \varphi(x, y)\}$ exists.
Set Theory and Combinatorics within $I\Delta_0$ (3)

- $c_E := \{m \in M : m Ec\}$.

- $X \subseteq M$ is **coded** in $\mathcal{M}$, if for some $c \in M$ such that $X = c_E$.

- Given $c \in M$, $\overline{c} := \{x \in M : x < c\}$. Note that $\overline{c}$ is coded in a model of $I\Delta_0$ provided $2^c$ exists in $\mathcal{M}$.

- $SSy_I(\mathcal{M}) := \{c_E \cap I : c \in N\}$.

- Within $I\Delta_0$ one can define a **partial** function $Card(x) = t$, expressing “the cardinality of the set coded by $x$ is $t$”.

- $I\Delta_0$ can prove that $Card(x)$ is defined (and is well-behaved) if $2^x$ exists.
In light of the above discussion, finite combinatorial statements have reasonable arithmetical translations in models of bounded arithmetic provided “enough powers of 2 exist”.

We shall therefore use the Erdős notation $a \rightarrow (b)^n_d$ for the arithmetical translation of the set theoretical statement:

“if $\text{Card}(X) = a$ and $f : [X]^n \rightarrow d$, then there is $H \subseteq X$ with $\text{Card}(H) = b$ such that $H$ is $f$-monochromatic.”

Here $[X]^n$ is the collection of increasing $n$-tuples from $X$ (where the order on $X$ is inherited from the ambient model of arithmetic), and $H$ is $f$-monochromatic iff $f$ is constant on $[H]^n$. 
• We also write $a \rightarrow \ast (b)^n$ for the arithmetical translation of the following canonical partition relation:

if $\text{Card}(X) = a$ and $f : [X]^n \rightarrow Y$, then there is $H \subseteq X$ with $\text{Card}(H) = b$ which is $f$-canonical, i.e., $\exists S \subseteq \{1, \ldots, n\}$ such that for all sequences $s_1 < \cdots < s_n$, and $t_1 < \cdots < t_n$ of elements of $H$,

$$f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n) \iff \forall i \in S (s_i = t_i).$$

Note that if $S = \emptyset$, then $f$ is constant on $[H]^n$, and if $S = \{1, \ldots, n\}$, then $f$ is injective on $[H]^n$.

• $\text{Superexp}(0, x) = x$, and

$$\text{Superexp}(n + 1, x) = 2^{\text{Superexp}(n, x)}.$$
Set Theory and Combinatorics within $I\Delta_0$ (6)

- **Theorem.** For each $n \in \mathbb{N}^+$, the following is provable in $I\Delta_0$:

  (a) [Ramsey] $a \rightarrow (b)^n_c$, if $a = \text{Superexp}(2n, bc)$ and $b \geq n^2$;

  (b) [Erdős-Rado] $a \rightarrow * (b)^n$, if $a = \text{Superexp}(4n, b \cdot 2^{2n^2-n})$ and $b \geq 4n^2$. 
On $I \Delta_0 + \text{Exp}$

- By a classical theorem of Parikh, $I \Delta_0$ can only prove the totality of functions with a polynomial growth rate, hence

$$I \Delta_0 \nvdash \forall x \exists y \text{Exp}(x, y).$$

- $I \Delta_0 + \text{Exp}$ is the extension of $I \Delta_0$ obtained by adding the axiom

$\text{Exp} := \forall x \exists y \text{Exp}(x, y)$.

The theory $I \Delta_0 + \text{Exp}$ might not appear to be particularly strong since it cannot even prove the totality of the superexponential function, but experience has shown that it is a remarkably robust theory that is able to prove an extensive array of theorems of number theory and finite combinatorics.
On $B\Sigma_1$

• For $\mathcal{L} \supseteq \mathcal{L}_A$, $B\Sigma_1(\mathcal{L})$ is the scheme consisting of the universal closure of formulae of the form

$$[\forall x < a \exists y \varphi(x, y)] \rightarrow [\exists z \forall x < a \exists y < z \varphi(x, y)]$$

where $\varphi(x, y)$ is a $\Delta_0(\mathcal{L})$-formula.

• It has been known since the work of Parsons that there are instances of $B\Sigma_1$ that are unprovable in $I\Delta_0 + Exp$; indeed Parsons’s work shows that even strengthening $I\Delta_0 + Exp$ with the set of $\Pi_2$-sentences that are true in the standard model of arithmetic fails to prove all instances of $B\Sigma_1$.

• However, Harvey Friedman and Jeff Paris have shown, independently, that adding $B\Sigma_1$ does not increase the $\Pi_2$-consequences of $I\Delta_0 + Exp$. 
A Characterization of $I\Delta_0 + Exp + B\Sigma_1$

• $I_{fix}(j)$ is the largest initial segment of the domain of $j$ that is pointwise fixed by $j$

• **Theorem A.** The following two conditions are equivalent for a countable model $M$ of the language of arithmetic:

(1) $M \models I\Delta_0 + B\Sigma_1 + Exp$.

(2) $M = I_{fix}(j)$ for some nontrivial automorphism $j$ of an end extension $M^*$ of $M$ that satisfies $I\Delta_0$. 
Outline of the proof of $I_{fix}(j) \models Exp$

(1) If $a \in I_{fix}(j)$ and $2^a$ is defined in $M$, then $2^a \in I_{fix}(j)$.

The usual proof of the existence of the base 2 expansion for a positive integer $y$ can be implemented within $I\Delta_0$ provided some power of 2 exceeds $y$. Therefore, for every $y < 2^a$, there is some element $c$ that codes a subset of \{0, 1, ..., $a - 1$\} such that $y = \sum_{i \in E} 2^i$.

The next observation is that $j(c) = c$. This hinges on the fact that $E$ satisfies Extensionality, and that $iE_{c}$ implies $j(i) = i$ (since $a \in I_{fix}(j)$, and $iE_{c}$ implies that $i < a$).
Outline of the proof of $I_{fix}(j) \models Exp$, Cont’d

\[ j(y) = j(\sum_{i} Ec \cdot 2^i) = \sum_{i} E_j(c) \cdot 2^i = \sum_{i} Ec \cdot 2^i = y. \]

So every $y < 2^a$ is fixed by $j$ and therefore $2^a \in I_{fix}(j)$.

(2) $\{m \in M : m$ is a power of 2$\}$ is cofinal in $M$.

Now use (1) and (2) to prove that if $a \in I_{fix}(j)$, then $2^a$ is defined and is a member of $I_{fix}(j)$. 
Two Key Results

• **Theorem** (Wilkie-Paris). *Every countable model of $I\Delta_0 + \text{Exp} + B\Sigma_1$ has an end extension to a model of $I\Delta_0 + B\Sigma_1$."

• $\mathcal{F}$ is the family of all $M$-valued functions $f(x_1, \ldots, x_n)$ on $M^n$ (where $n \in \mathbb{N}^+$) such that for some $\Sigma_1$-formula $\delta(x_1, \ldots, x_n, y)$, $\delta$ defines the graph of $f$ in $M$ and for some term $t(x_1, \ldots, x_n)$, $f(a_1, \ldots, a_n) \leq t(a_1, \ldots, a_n)$ for all $a_i \in M$.

• **Theorem** (Dimitracopoulos-Gaifman). *If $M \models I\Delta_0 + B\Sigma_1$, then the expanded structure

$$M_{\mathcal{F}} := (M, f)_{f \in \mathcal{F}}$$

satisfies $I\Delta_0(\mathcal{L}_F) + B\Sigma_1(\mathcal{L}_F)$, where $\mathcal{L}_F$ is the result of augmenting the language of arithmetic with names for each $f \in \mathcal{F}$."


(A variant of) Paris-Mills Ultrapowers

• Suppose $\mathcal{M} \models I\Delta_0 + B\Sigma_1$, $I$ is a cut of $\mathcal{M}$ that satisfies $Exp$ and $c \in M \setminus I$ such that $2^c$ exists in $\mathcal{M}$ (such an element $c$ exists by $\Delta_0$-OVERSPILL).

• The index set is $\overline{c} = \{0, 1, \ldots, c - 1\}$.

• $\mathcal{F}_c$ is the family of all $M$-valued functions $f(x_1, \ldots, x_n)$ on $[c]^n$ (where $n \in \mathbb{N}$) obtained by restricting the domains of $n$-ary functions in $\mathcal{F}$ to $[c]^n$ ($n \in \mathbb{N}^+$).

• The family of functions used in the formation of the ultrapower is $\mathcal{F}_c$. The relevant Boolean algebra is denoted $\mathcal{B}_c$. 
Desirable Ultrafilters (1)

- \( \mathcal{U} \subseteq \mathcal{B}_c \) is canonically Ramsey if for every \( f \in \mathcal{F}_c \) with \( f : [\bar{c}]^n \rightarrow M \), there is some \( H \in \mathcal{U} \) such that \( H \) is \( f \)-canonical;

- \( \mathcal{U} \) is \( I \)-tight if for every \( f \in \mathcal{F}_c \) with \( f : [\bar{c}]^n \rightarrow M \), then there is some \( H \in \mathcal{U} \) such either \( f \) is constant on \( H \), or there is some \( m_0 \in M \setminus I \) such that \( f(x) > m_0 \) for all \( x \in [H]^n \).

- \( \mathcal{U} \) is \( I \)-conservative if for every \( n \in \mathbb{N}^+ \) and every \( M \)-coded sequence \( \langle K_i : i < c \rangle \) of subsets of \( [\bar{c}]^n \) there is some \( X \in \mathcal{U} \) and some \( d \in M \) with \( I < d \leq c \) such that \( \forall i < d \) \( X \) decides \( K_i \), i.e., either \( [X]^n \subseteq K_i \) or \( [X]^n \subseteq [\bar{c}]^n \setminus K_i \).
Desirable Ultrafilters (2)

- **Theorem.** \( \mathcal{B}_c \) carries a nonprincipal ultrafilter \( \mathcal{U} \) satisfying the following four properties:

  (a) \( \mathcal{U} \) is canonically Ramsey;

  (b) \( \mathcal{U} \) is \( I \)-tight;

  (c) \( \{\text{Card}^M(X) : X \in \mathcal{U}\} \) is downward cofinal in \( M \setminus I \);

  (d) \( \mathcal{U} \) is \( I \)-conservative.
Fundamental Theorem

• Theorem. Suppose $I$ is a cut closed exponentiation in a countable model of $I \Delta_0$, $\mathbb{L}$ is a linearly ordered set, and $\mathcal{U}$ satisfies the four properties of the previous theorem. One can use $\mathcal{U}$ to build a an elementary extension $M^*_\mathbb{L}$ of $M$ that satisfies:

(a) $I \subseteq e M_\mathbb{L}$ and $SSy_I(M_\mathbb{L}) = SSy_I(M)$.

(b) $\mathbb{L}$ is a set of indiscernibles in $M^*_\mathbb{L}$;

(c) Every $j \in Aut(\mathbb{L})$ induces an automorphism $\hat{j} \in Aut(M^*_\mathbb{L})$ such that $j \mapsto \hat{j}$ is a group embedding of $Aut(\mathbb{L})$ into $Aut(M^*_\mathbb{L})$;

(d) If $j \in Aut(\mathbb{L})$ is nontrivial, then $I_{fix}(\hat{j}) = I$;

(e) If $j \in Aut(\mathbb{L})$ is fixed point free, then $fix(\hat{j}) = M$. 