Bounded finite set theory

Laurence Kirby

Baruch College, City University of New York

JAF 37, Florence, 2018

Arithmetic and finite set theory

The correspondence — does it work for bounded arithmetic?

$$\mathsf{FST} : \mathsf{PA} \quad = \quad ? : I\Delta_0$$

$$\begin{aligned}\mathsf{FST} &= \text{Finite Set Theory} \\ &= \mathsf{ZF} - \mathsf{Inf} + \neg\mathsf{Inf}\ (+\,\mathsf{TC}\,)\end{aligned}$$

$$\mathsf{TC} = \text{Axiom of Transitive Containment}$$

Arithmetic and finite set theory

The correspondence via Ackermann's interpretation

Let $x \in_{Ack} y$ be the predicate expressing that the coefficient of 2^x in the binary expansion of y is 1. Then

- $\langle \mathbb{N}, \in_{Ack} \rangle \cong \langle V_\omega, \in \rangle$.
- If $M \models \mathsf{PA}$, then $Ack_M =_{df} \langle M, \in^M_{Ack} \rangle \models \mathsf{FST}$ and its ordinals are isomorphic to M.

Arithmetic and finite set theory

The correspondence via induction

- Adjunction: $x; y = x \cup \{y\}$
- Work in the language $\mathcal{L}(0;)$
- $\in$ is definable: $y \in x \leftrightarrow x; y = x$
- PS_0 consists of:

$$0; x \neq 0$$

$$[x; y]; y = x; y$$

$$[x; y]; z = [x; z]; y$$

$$[x; y]; z = x; y \leftrightarrow x; z = x \lor z = y$$

Arithmetic and finite set theory

The correspondence via induction

Tarski-Givant induction:

$$\varphi(0) \ \wedge \ \forall x \forall y(\varphi(x) \wedge \varphi(y) \rightarrow \varphi(x; y)) \ \rightarrow \ \forall x \varphi(x).$$

PS consists of PS_0 together with induction for each first order φ (with parameters). (Previale)

- PS is logically equivalent to $\mathsf{ZF} - \mathsf{Inf} + \neg\mathsf{Inf} + \mathsf{TC}$

$I\Sigma_1 S$

is enough to Ackermannize

$$\mathsf{PS} : \mathsf{PA} \quad = \quad I\Sigma_1 S : I\Sigma_1$$

- If $M \models I\Sigma_1$, then $Ack_M \models I\Sigma_1 S$ and the ordinals of Ack_M, together with the restrictions of addition and multiplication to them, are isomorphic to M.
- Parsons' Theorem transfers to set theory: the primitive recursive set functions are those provably total in $I\Sigma_1 S$, where...

The primitive recursive set functions

are obtained from the initial functions

- the constant function $\tilde{0}(\vec{x}) = 0$,
- projections, and
- adjunction $x; y$,

by closing under

- *substitutions* $f(\vec{x}) = g(h_1(\vec{x}), \cdots, h_k(\vec{x}))$
- and *recursion* of form

$$\begin{aligned} f(0, \vec{z}) &= g(\vec{z}) \\ f([a; p], \vec{z}) &= h(a, p, f(a, \vec{z}), f(p, \vec{z}), \vec{z}) \end{aligned}$$

The primitive recursive set functions

include set-theoretic operators such as P, $\cup$, $\bigcup$, $|x|$ = cardinality of x, $\mathsf{TC}(x)$ = transitive closure of x, V_n, and ordinal arithmetic operations $+, \cdot, x^y$.

$I\Delta_0 S(\cup)$ means: $I\Delta_0 S$ plus "$\cup$ is total".
Or equivalently: $I\Delta_0 S$ in language expanded by a function symbol $\cup$ and axioms:

$$x \cup 0 = x \quad \text{and} \quad x \cup [y; z] = (x \cup y); z$$

and similarly for other primitive recursive functions.

$\mathcal{L}(0\,;<)$

"Bounded with respect to what?" — a transitive relation is needed

so we add $<$ to our language, intended to mean the transitive closure of the $\in$ relation.
Let $\mathsf{PS}_0^<$ be the result of adding to PS_0:

$$x \not< 0 \quad \text{and} \quad x < y; z \leftrightarrow x < y \ \vee \ x \leq z$$

Then we define the class of Δ_0 formulæ in the expanded language by allowing bounded quantification of form $\forall y < t$, $\exists y < t$ where t is a term. And we define $I\Delta_0 S$ to be $\mathsf{PS}_0^<$ together with induction for Δ_0 formulæ in the expanded language.

PS : PA $=$ $I\Delta_0 S : I\Delta_0$?

Proposition. Suppose $V \models I\Delta_0 S$ and W is a transitive subset of V closed under adjunction. Then Δ_0 formulæ are absolute between V and W, and $W \models I\Delta_0 S$.

- Q1: Which axioms of set theory are provable in $I\Delta_0 S$?
- Q2: Given $M \models I\Delta_0$, is there a model of $I\Delta_0 S$ whose ordinal arithmetic is isomorphic to M?

Which axioms of ZF are provable in $I\Delta_0 S$?

- $I\Delta_0 S \vdash$ the Pair Set Axiom, Extensionality, $\neg\mathsf{Inf}$, and the Axiom of Foundation.
- $I\Delta_0 S(\mathsf{TC}, \mathsf{P}) \vdash \bigcup$, i.e. the Union Axiom. This is because $\bigcup x \in \mathsf{P}(\mathsf{TC}(x))$.
- $I\Delta_0 S(\mathsf{P}) \vdash \Delta_0$-Comprehension.
- Does $I\Delta_0 S \vdash \Delta_0$-Comprehension? ... If so, and if the answer to Q2 is positive, then $I\Delta_0 \vdash \Delta_0 PHP$. This is because $I\Delta_0 S$ proves a pigeon hole principle for functions which are sets.

Submodels of Ack_M

for $M \models I\Sigma_1$

- For $I \subseteq_e M$: $V_I = \bigcup_{i \in I} V_i$.
- $V_I \models I\Delta_0 S(\bigcup, \mathsf{TC}, \mathsf{P})$.
- H_i is the set of all elements of $V_M = Ack_M$ whose transitive closure has cardinality $< i$, i.e. all sets of hereditary cardinality $< i$.
- If I is closed under $+$, then $H_I \models I\Delta_0 S(\bigcup, \mathsf{TC})$.
- $H_I \models \mathsf{P}$ iff I is closed under exponentiation.

Submodels of Ack_M

for $M \models I\Sigma_1$

- $C_i = \{x \in V_M \mid V_M \models \forall y \leq x\, |y| < i\}$.
- Let $e_0 = 1$, $e_{n+1} = 2^{e_n}$.
- *Theorem:*
  (1) $V_I \cap C_J \models I\Delta_0 S$.
  (2) $V_I \cap C_J \models \cup$ iff $J \geq e_I$ or J is closed under addition.
  (3) $V_I \cap C_J \models \bigcup$ iff $J \geq e_I$ or J is closed under multiplication.

  (5) $V_I \cap C_J \models \mathsf{P}$ iff $J \geq e_I$ or J is closed under exponentiation.

Submodels of Ack_M

for $M \models I\Sigma_1$

- (4)(i) Suppose I is closed under addition. Then $V_I \cap C_J \models \mathsf{TC}$ iff $J \geq e_I$ or $J^I = J$.

  (4)(ii) $V_I \cap C_J \models \mathsf{TC}$ iff $J \geq e_I$ or $\exists i \in I(J^{I-i} = J \wedge e_i \in J)$.
- This theorem provides examples to show that e.g. $I\Delta_0 S(\bigcup) \nvdash \mathsf{TC}$.
- Does $I\Delta_0 S(\mathsf{TC}) \vdash \bigcup$?

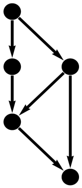
Sets as digraphs

(Aczel)

Each HF set x is uniquely specified by the extensional acyclic digraph with a single source

$G(x) =$ the membership relation restricted to $\mathsf{TC}(x)$; x

e.g. $a = \{\{\{0\}\}, \{0, \{0\}\}\}$



The ordinals of a model of $I\Delta_0 S$

It depends which ordinals …

- Q2: Given $M \models I\Delta_0$, is there a model of $I\Delta_0 S$ whose ordinal arithmetic is isomorphic to M?

Von Neumann ordinals (1923) (Zermelo, Mirimanoff): $n+1 = n; n = n \cup \{n\}$

Zermelo ordinals (1908): $(n+1)_z = 0; n_z = \{n_z\}$

They can differ, e.g. in $V_I \cap C_J$ with $J < I$, the von Neumann ordinals are J but the Zermelo ordinals are I.

Zermelo ordinals are simpler

in setbuilder notation

Zermelo: $6_z = \{\{\{\{\{\{\}\}\}\}\}\}$

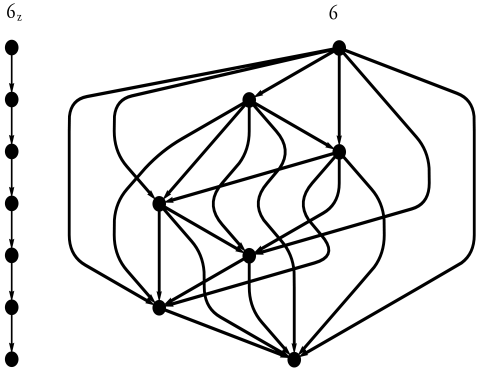
Von Neumann:

$$
\begin{aligned}
6 = & \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \\
& \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}\}, \\
& \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \\
& \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}\}
\end{aligned}
$$

Exponential growth in the length of the representation for n means that you can't multiply in polynomial time!

Zermelo ordinals are simpler

as digraphs



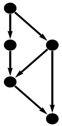
This time, only polynomially so.

Models of $I\Delta_0 + \mathsf{Exp}$ are expandable

Q2: Given $M \models I\Delta_0$, is there a model of $I\Delta_0 S$ whose ordinal arithmetic is isomorphic to M?

Yes if M has an end extension to a model of $I\Sigma_1$.

Theorem: Yes if $M \models \mathsf{Exp}$.
Idea: Code sets by their digraph representations, e.g.



$a = \{\{\{0\}\}, \{0, \{0\}\}\}$ = the "pair of deuces" is represented by $s^* = \langle \{0\}, \{1\}, \{0, 1\}, \{2, 3\} \rangle$ which is represented in turn by $s = \langle 1, 2, 3, 12 \rangle$.

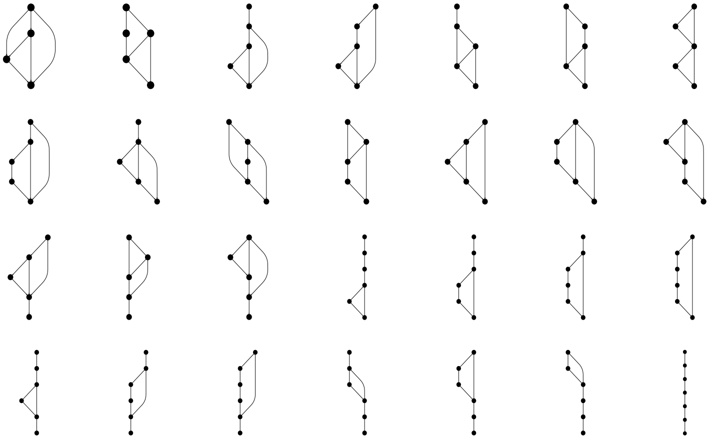
Models of $I\Delta_0 + \mathsf{Exp}$ are expandable

Definition: A *σ-sequence* in M is a strictly increasing sequence $s = \langle s_1, \dots, s_n \rangle$ such that for each i, $0 < s_i < 2^i$.

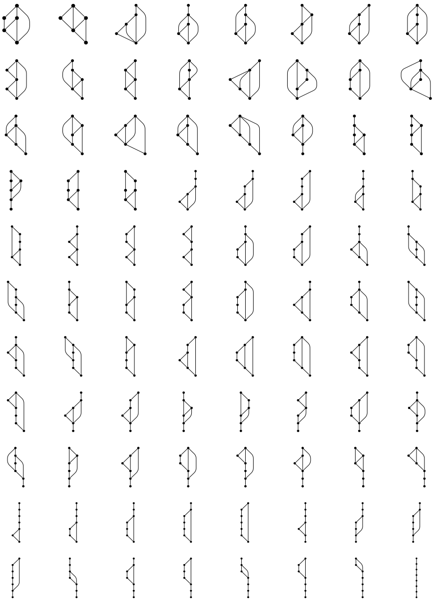
If s is a σ-sequence, define $s_i^* = \{j < i \mid j \in_{Ack} s_i\}$ and s^* to be the corresponding sequence $\langle s_1^*, \dots, s_n^* \rangle$. Then $s_i^* \subseteq \{0, \dots, i-1\}$ and the s_i^* are distinct and non-empty.

The idea is to use the sequence s to represent the set whose digraph has nodes $0, \dots, n$ with an edge from j to i just when $i \in s_j^*$.

The 28 sets whose graphs have 6 edges



The 88 sets whose graphs have 7 edges



a^a

in the Zermelo arithmetic where a is the "pair of deuces"