Peano Arithmetic and Finite Zermelo Fraenkel Set Theory II

Zuzana Haniková

Institute of Computer Science of the Czech Academy of Sciences

Logika v souvislostech a aplikacích
Dpt. of Logic, Faculty of Arts, CUni
Feb & March 2024

Outline

- Natural numbers and Peano arithmetic.
- Notions of finiteness.
- Theories of finite sets and axioms.
- Ackermann interpretation of ZF_{fin} in PA.
- Theories of finite sets and classes.

Main source:

Richard Kaye, Tin Lok Wong: On Interpretations of Arithmetic and Set Theory. *Notre Dame J. Formal Logic* 48, 2007.

First-order theory in logic with equality.

Language: $\{0, S, +, \cdot\}$.

Axioms:

(Q1) $S(x) \neq \bar{0}$

(Q2) $S(x) = S(y) \to x = y$

(Q3) $x \neq \bar{0} \to (\exists y)(x = S(y))$

(Q4) $x + \bar{0} = x$

(Q5) $x + S(y) = S(x + y)$

(Q6) $x \cdot \bar{0} = \bar{0}$

(Q7) $x \cdot S(y) = (x \cdot y) + x$

(Q8) $x \leq y \leftrightarrow (\exists v)(v + x = y)$

(Ind) $\varphi(\bar{0}) \,\&\, (\forall x)(\varphi(x) \to \varphi(S(x))) \to (\forall x)\varphi(x)$

$\mathrm{ZF}_{\mathrm{fin}}$ and TC

$\mathrm{ZF}_{\mathrm{fin}}$:

(extensionality) $\forall x, y\, (\forall z\, (z \in x \leftrightarrow z \in y) \rightarrow x = y)$

(empty set) $\exists x\, \forall y\, \neg(y \in x)$

(pair) $\forall x, y\, \exists z\, \forall u\, (u \in z \leftrightarrow u = x \vee u = y)$

(union) $\forall x\, \exists y\, \forall z\, (z \in y \leftrightarrow \exists u\, (z \in u \wedge u \in x))$

(power set) $\forall x\, \exists y\, \forall z (z \in y \leftrightarrow \forall u\, (u \in z \rightarrow u \in x))$

(separation) $\forall x\, \exists y\, \forall z (z \in y \leftrightarrow z \in x \,\&\, \varphi(z))$
(φ any formula, y not free in φ)

(replacement)
$\forall x\, [\forall u \in x\, \exists! v\, \varphi(u, v) \rightarrow \exists y\, \forall v\, (v \in y \leftrightarrow \exists u \in x\, \varphi(u, v))]$
(φ any formula, y not free in φ)

(regularity) $\forall x\, (x \neq \emptyset \rightarrow \exists y\, (y \in x \wedge y \cap x = \emptyset))$

$\neg$(infinity) $\neg \exists x\, (\emptyset \in x \,\&\, \forall y \in x\, (y \cup \{y\} \in x))$

transitive closure:

(TC) $\forall x\, \exists y\, (x \subseteq y \,\&\, \mathrm{Trans(y)})$

The notion of an interpretation

Let T and S be first-order theories in languages $\mathcal{L}_T$ and $\mathcal{L}_S$ resp.

The pair $(\alpha, ^\star)$ is a translation of $\mathcal{L}_T$ to $\mathcal{L}_S$ provided that:
(i) α is a formula of $\mathcal{L}_S$ with one free variable;
(ii) the map * assigns to each

- n-ary fct. symbol F of $\mathcal{L}_T$ an n-ary fct. symbol $F^\star$ of $\mathcal{L}_S$;
- n-ary pred. symbol P of $\mathcal{L}_T$ an n-ary pred. symbol $P^\star$ of $\mathcal{L}_S$ ($=$ translates to itself);
- for φ atomic of $\mathcal{L}_T$, $\varphi^\star$ of $\mathcal{L}_S$ is obtained by replacing each F or P of $\mathcal{L}_T$ with its *-image;

(iii) * commutes with logical connectives;
(iv) * relativizes quantifiers: for φ of $\mathcal{L}_T$,

- $(\forall x \varphi(x))^\star$ is $\forall x(\alpha(x) \to \varphi^\star(x))$;
- $(\exists x \varphi(x))^\star$ is $\exists x(\alpha(x) \,\&\, \varphi^\star(x))$.

Extend * to each formula of $\mathcal{L}_T$ by induction on formula structure.

The notion of an interpretation – cont'd

Let T and S be first-order theories in languages $\mathcal{L}_T$ and $\mathcal{L}_S$ resp.

S interprets T iff there is a (conservative) extension by definitions S' of S and a translation $(\alpha, ^\star)$ of $\mathcal{L}_T$ to $\mathcal{L}_{S'}$ such that

(i) $S' \vdash \exists x \alpha(x)$;

(ii) if F is n-ary in $\mathcal{L}_T$, then
$S' \vdash \forall x_1, \ldots, x_n(\alpha(x_1), \ldots, \alpha(x_n) \rightarrow \alpha(F^*(x_1, \ldots, x_n)))$

(iii) $S' \vdash \varphi^\star$ for each axiom φ of T.

If T is interpreted in S, we have $S \vdash \varphi^\star$ for any theorem φ of T.

Relative consistency

Assume S interprets T.

Suppose T is inconsistent: i.e., $T \vdash \varphi$ and $T \vdash \neg\varphi$ for some φ (and hence, for every φ) of $\mathcal{L}_T$.

Then also S is inconsistent, since by assumption S proves both $\varphi^\star$ and $\neg(\varphi^\star)$.

By contraposition, if S is consistent, then so is T.
In such a case we say that T is consistent relative to S.

In case T is consistent relative to S,
and S is consistent relative to T,
then T and S are said to be equiconsistent.

NB. Role of metatheory. Relative consistency or equiconsistency are meaningful if one cannot prove the consistency of T or of S.

Example: the "ordinal" intp. of PA in $\mathrm{ZF}_{\mathrm{fin}}$ (+TC)

A set is an ordinal number iff is transitive and totally ordered by $\in$.

Let On denote the class of ordinals.

As usual, $\emptyset \in \mathrm{On}$ and $\emptyset$ has no predecessor;
$\alpha \in \mathrm{On}$ implies $\alpha \cup \{\alpha\} \in \mathrm{On}$ and the latter is immediate successor of α within On.

The interpretation $(o, {}^{\mathsf{o}})$ is given as follows:

$o(x)$ is $x \in \mathrm{On}$;
$S(x)^{\mathsf{o}}$ is interpreted as $x \cup \{x\}$;
$(x + y)^{\mathsf{o}}$ is interpreted as ordinal addition of x and y;
$(x \cdot y)^{\mathsf{o}}$ is interpreted as ordinal multiplication
within $\mathrm{ZF}_{\mathrm{fin}}$ (+TC).

Then $(o, {}^{\mathsf{o}})$ is an interpretation of PA in $\mathrm{ZF}_{\mathrm{fin}}$.
(We have already mentioned this. It also works in ZF.)

Binary numerals

Let $n \in N$.
Write n_2 for the binary numeral representing n.

In other words, we have

$$n = \sum_{i=0}^{k-1} p_i 2^i$$

for some k, with $p_i \in \{0, 1\}$ and $p_{k-1} = 1$.
Also $k = \lfloor \log_2(n) \rfloor + 1$.

Then n_2 is $p_k \, p_{k-1} \ldots p_1 \; p_0$.

E.g., n is 26.

We have $26 = 16 + 8 + 2$, i.e., $26 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$.

So 26_2 is 11010.

“Membership” on N

Define ε on N, using binary representations.

Let $m, n \in N$. Let n_2 be $p_{k-1}\, p_{k-2} \ldots p_1\ p_0$ with $k = \lfloor \log_2(n) \rfloor + 1$.

Define

$$m \,\varepsilon\, n \quad \text{if and only if} \quad m\text{-th digit in } n_2 \text{ is } 1$$

...	...	...	...	...	...	...	...	...	...
...	0	0	0	1	1	0	1	0	26
...	...	...	...	...	...	...	...	...	...
...	0	0	0	0	1	0	1	0	10
...	0	0	0	0	1	0	0	1	9
...	0	0	0	0	1	0	0	0	8
...	0	0	0	0	0	1	1	1	7
...	0	0	0	0	0	1	1	0	6
...	0	0	0	0	0	1	0	1	5
...	0	0	0	0	0	1	0	0	4
...	0	0	0	0	0	0	1	1	3
...	0	0	0	0	0	0	1	0	2
...	0	0	0	0	0	0	0	1	1
...	0	0	0	0	0	0	0	0	0
...	7	6	5	4	3	2	1	0	

"Membership" on N – cont'd

Running example: 26_2 is 11010.

Therefore $26 = \{4, 3, 1\}$.

A coding of finite sets:

$$a(\sum_{i=0}^{k-1} p_i 2^i) = \{a(i) \mid p_i = 1\}$$

Example:

- binary unions and intersections;
- singletons and pairs;
- successors.

Work in PA or fragment.

1. the formula α, delimiting the "domain", will be just $x = x$.
Comment: within N, every number stands for some set, as we have seen.

2. Further we define the translation $\mathfrak{a}$ of the symbol $\in$.
(Our definition of intp. stipulates that $=$ translates to itself.
In other words, set-theoretic $=$ translates to arithmetical $=$.)

$(x \in y)^{\mathfrak{a}}$ is

$$\exists w < y\, \exists p \leq y\, \exists r < p\, (p = 2^x \,\&\, y = (2w + 1)p + r)$$

Notice that if $n = \sum_{i=0}^{k-1} p_i 2^i$, then n can be written as

$$(p_{k-1}2^{l-1} + p_{k-2}2^{l-2} + \cdots + p_{k-l+1}2 + 1)2^{k-l} + r$$

where $r < 2^{k-l}$ if and only if $p_{k-l} = 1$ in n_2.

3. It remains to define $p = 2^x$.
Exponentiation is not available in the language of PA.

A suitable formula $\mathrm{Pow}(y, x)$ that represents "y is the x-th power of 2".

Properties: $\mathrm{Pow}(1, 0)$ and $\mathrm{Pow}(y, x) \to \mathrm{Pow}(2y, x + 1)$
and $\mathrm{Pow}(v, x) \,\&\, \mathrm{Pow}(w, x) \to v = w$.

The formula says, in plain words, there is the (code of the) sequence

$$\langle 0, 2, 4, 8, \ldots y\rangle$$

of length $x + 1$ and with the recursive property.

Then PA proves $\forall x \exists y \mathrm{Pow}(y, x)$.
(In fact already $\mathrm{I}\Sigma_1$.)

Ackermann interpretation of $\mathrm{ZF}_{\mathrm{fin}}$ in PA – cont'd

Theorem: [Ackermann] $(\alpha, {}^{\mathfrak{a}})$ defines an interpretation of $\mathrm{ZF}_{\mathrm{fin}}$ in PA.

Proof: consists in verifying that the formula $\varphi^{\mathfrak{a}}$ is provable in PA whenever φ is an axiom of $\mathrm{ZF}_{\mathrm{fin}}$.

NB. We cannot "reason in the standard model",
since we need to establish provability of the translations
(i.e., validity in all models).

[Kaye-Wong] remark that one can prove translations of
extensionality, empty set, union, foundation, and some others, in $\mathrm{I}\Delta_0$.

Provided 2^x is total, one can prove existence of singletons
(and pairing and power).
Notice that $a^{-1}(\{x\})$ is coded by $2^{(a^{-1}(x))}$.

Ackermann interpretation of ZF_{fin} in PA – cont'd

Moreover [Kaye–Wong] also show:

Lemma:
Let $(\alpha, {}^{\mathfrak{a}})$ be the Ackermann interpretation of ZF_{fin} in PA.
Then $I\Delta_0 \vdash TC^{\mathfrak{a}}$.

Proof sketch:
Consider an arbitrary model M of $I\Delta_0$ and its element x,
obtained by "subtracting 1" from the smallest power of 2 that is bigger than x.
Existence: Δ_0-induction gives a least u s.t. $\exists z \leq x(2^u = z)$ no longer holds.

Then if $(u \in v)^{\mathfrak{a}} \,\&\, (v \in y)^{\mathfrak{a}}$, we have $u < v < y$ so u-th digit in y_2 is 1.

However $ZF_{fin} \nvdash TC$, as discussed.

Inverse Ackermann interpretation:
working in $\mathrm{ZF}_{\mathrm{fin}}$+TC, define $\mathfrak{b}$ by recursion:

$$\mathfrak{b}(y) = \Sigma(\{2^{\mathfrak{b}(x)} \in \mathrm{On} \mid x \in y\})$$

where Σ is ordinal addition.

This is a bijection from V to On.

Taking β again to be $x = x$ and
equipped with ordinal arithmetic on the range of $\mathfrak{b}$, this gives

$(\beta, {}^{\mathfrak{b}})$ is an interpretation of PA in $\mathrm{ZF}_{\mathrm{fin}}$+TC.

Then they obtain
$\mathrm{PA} \vdash \varphi \leftrightarrow ((\varphi^{\mathfrak{b}})^{\mathfrak{a}})$
$\mathrm{ZF}_{\mathrm{fin}}+\mathrm{TC} \vdash \psi \leftrightarrow ((\psi^{\mathfrak{a}})^{\mathfrak{b}})$
for arithmetical sentences φ and sentences ψ in language of set theory.

(More) analysis of provability from fragments.

Every model of $\mathrm{ZF}_{\mathrm{fin}}$ has a transitive submodel of $\mathrm{ZF}_{\mathrm{fin}}$+TC with the same ordinals.