WKL_0 and Finitistic Reductionism

Ke Gao

北京大学哲学系
PEKING UNIVERSITY PHILOSOPHY DEPARTMENT

November 6, 2016

Outline

Outline

Hilbert's Program

- The first step is to isolate the unproblematic, "finitistic" portion of mathematics (PRA). This part of mathematics is indispensable for all scientific reasoning and therefore needs no special validation.
- The second step is to reconstitute mathematics as a big, elaborate formal system. The big system contains unrestricted classical logic, infinite sets galore, and special variables ranging over natural numbers, functions from natural number to natural numbers, countable ordinals, etc.
- The last step is to give a finitistically correct consistency proof for the big system. It would then follow that any Π_1^0 sentence provable in the big system is finitistically true.

Main Question

- Gödel's incompleteness theorems imply that a wholesale realization of Hilbert's program is impossible. There is no hop of proving the consistency of set theory within PRA, nor is there any hope of showing that set theory is conservative over PRA for Π^0_1 sentences.
- In view of Gödel's limitative results, it is of interest to ask what part of Hilbert's program can be carried out. In other words, which portions of infinitistic mathematics can be reduced to finitism?
- The study of subsystems of second order arithmetic makes it possible to give a more precise formulation of this question: which interesting subsystems of Z_2 are conservative over PRA for Π^0_1 sentences?

Outline

Second-order Arithmetic Z_2

Definition 1

The language L_2 of second-order arithmetic is a two-sorted language with number variables x,y,z... intended to range over natural numbers and set variables X,Y,Z... intended to range over sets of natural numbers. In addition, the language include $+$, $\cdot$ as operation symbols, $0, 1$ as constants and $<$ as a relation symbol, with adding a binary relation $\in$ to relate the two sorts.

Second-order Arithmetic Z_2

Definition 1

The language L_2 of second-order arithmetic is a two-sorted language with number variables x,y,z... intended to range over natural numbers and set variables X,Y,Z... intended to range over sets of natural numbers. In addition, the language include $+$, $\cdot$ as operation symbols, $0, 1$ as constants and $<$ as a relation symbol, with adding a binary relation $\in$ to relate the two sorts.

Definition 2

A model for L_2 or an L_2-structure is an ordered 7-tuple

$$M = (|M|, \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$$

where $|M|$ is a set; $\mathcal{S}_M$ is a collection of subsets of $|M|$; $+_M$ and $\cdot_M$ are function from $|M| \times |M|$ into $|M|$; $<_M$ is a subset of $|M| \times |M|$; and 0_M and 1_M are distinguished elements of $|M|$.

Second-order Arithmetic Z_2

Definition 3

The axioms of second order arithmetic consist of universal closures of the following L_2-formulas:

1. Basic axioms, known as Robinson arithmetic (Q);
2. Induction axiom scheme:

$$(0 \in X \wedge \forall n(n \in X) \to n+1 \in X)) \to \forall n(n \in X)$$

3. Comprehension scheme:

$$\exists X \forall n(n \in X \leftrightarrow \varphi(n)),$$

where $\varphi(n)$ is any formula in which X does not occur freely.

Subsystems of Second-order Arithmetic

- The formal system RCA_0 consists of basic axioms, $I\Sigma^0_1$ and the schema of recursive comprehension axioms (RCA):

$$\forall n(\varphi(n) \leftrightarrow \psi(n)) \rightarrow \exists X \forall n(n \in X \leftrightarrow \varphi(n)),$$

  where φ and ψ are Σ^0_1 and Π^0_1 respectively.Intuitively, it asserts the existence of recursive sets.
- The system WKL_0 consists of RCA_0 and the weak könig's lemma, namely the statement that every infinite subtree of the full binary tree has an infinite path.

First-order Part of Z_2

Let L_1 be the language of first order arithmetic, i.e. L_1 is just L_2 with the set variables omitted. First order arithmetic is the formal system Z_1 whose language is L_1 and whose axioms are the basic axioms plus the first order induction scheme for all L_1-formulas $\varphi(n)$. In the literature of mathematical logic, first order arithmetic is sometimes known as Peano arithmetic. It is easy to see that every theorem of Z_1 is a theorem of Z_2. In model-theoretic terms, this means that for any model $(|M|, \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$ of Z_2, its first order part $(|M|, +_M, \cdot_M, 0_M, 1_M, <_M)$ is a model of Z_1.

First-order Part of Z_2

Let L_1 be the language of first order arithmetic, i.e. L_1 is just L_2 with the set variables omitted. First order arithmetic is the formal system Z_1 whose language is L_1 and whose axioms are the basic axioms plus the first order induction scheme for all L_1-formulas $\varphi(n)$. In the literature of mathematical logic, first order arithmetic is sometimes known as Peano arithmetic. It is easy to see that every theorem of Z_1 is a theorem of Z_2. In model-theoretic terms, this means that for any model $(|M|, \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$ of Z_2, its first order part $(|M|, +_M, \cdot_M, 0_M, 1_M, <_M)$ is a model of Z_1.

Theorem 4

An L_1-structure is the first order part of some model of RCA_0 if and only if it is a model of $\Sigma_1^0 - PA$, where $\Sigma_1^0 - PA$ is the L_1-theory consisting of the basic axioms plus the induction scheme for all Σ_1^0 L_1-formulas.

Primitive Recursive Arithmetic PRA

Definition 5

The language of PRA is a first order language with equality. In addition to the 2-place predicate symbol $=$, it contains a constant symbol $\underline{0}$, number variables $x_0, \ldots, x_n, \ldots (n < \omega)$, 1-place operation symbols $\underline{Z}$ and $\underline{S}$, k-place operation symbols $\underline{P}_i^k$ for each i and k with $1 \leq i \leq k < \omega$, and additional operation symbols which are introduced as follows. If $\underline{g}$ is an m-place operation symbol and $\underline{h}_1, \ldots, \underline{h}_m$ are k-place operation symbols, then $\underline{f} = C(\underline{g}, \underline{h}_1, \ldots, \underline{h}_m)$ is an k-place operation symbols. If $\underline{g}$ is a k-place operation symbol and $\underline{h}$ is a $(k+2)$-place operation symbol, then $\underline{f} = R(\underline{g}, \underline{f})$ is a $(k+1)$-place operation symbol. The operation symbols of the language of PRA are called primitive recursive function symbols.

Primitive Recursive Arithmetic PRA

The axioms of PRA are as follows. We have the usual axioms for equality. We have the usual axioms for $\underline{0}$ and the successor function:

$$\underline{Z}(x) = \underline{0}$$
$$\underline{S}(x) = \underline{S}(y) \to x = y$$
$$x \neq \underline{0} \leftrightarrow \exists y(\underline{S}(y) = x)$$

We have defining axioms for the projection functions:

$$\underline{P}_i^k(x_1, \ldots, x_k) = x_i$$

For each function $\underline{f} = C(\underline{g}, \underline{h}_1, \ldots, \underline{h}_m)$ given by composition, we have a defining axiom

$$\underline{f}(x_1, \ldots, x_k) = \underline{g}(\underline{h_1}(x_1, \ldots, x_k), \ldots, \underline{h}_m(x_1, \ldots, x_k)).$$

Primitive Recursive Arithmetic PRA

For each function $\underline{f} = R(\underline{g}, \underline{h})$ given by primitive recursion, we have defining axioms

$$\begin{aligned} \underline{f}(0, x_1, \dots, x_k) &= \underline{g}(x_1, \dots, x_k) \\ \underline{f}(\underline{S}(y), x_1, \dots, x_k) &= \underline{h}(y, \underline{f}(y, x_1, \dots, x_k), x_1, \dots, x_k) \end{aligned}$$

Finally we have the scheme of primitive recursive function:

$$(\theta(0) \wedge \forall x(\theta(x) \to \theta(\underline{S}(x)))) \to \forall x \theta(x)$$

where θ is any quantifier-free formula in language of PRA with a distinguished free variable x.

Canonical Interpretation

Definition 6

We define the canonical interpretation of the language of first order arithmetic, L_1, into the language of PRA. The constants 0 and 1 are interpreted as $\underline{0}$ and $\underline{1} \equiv \underline{S}(\underline{0})$ respectively. Addition and multiplication are interpreted as primitive recursive function given by

$$\begin{aligned} x + \underline{0} &= x, & x + \underline{S}(y) &= \underline{S}(x+y), \\ x \cdot \underline{0} &= \underline{0}, & x \cdot \underline{S}(y) &= (x \cdot y) + x \end{aligned}$$

We introduce predecessor and truncated subtraction, $\underline{P}$ and $\dot{-}$, as primitive recursive functions given by

$$\begin{aligned} \underline{P}(\underline{0}) &= 0, & \underline{P}(\underline{S}(y)) &= y, \\ x \dot{-} \underline{0} &= x, & x \dot{-} \underline{S}(y) &= \underline{P}(x \dot{-} y). \end{aligned}$$

We then interpret $t_1 < t_2$ as $t_1 \dot{-} t_2 \notin 0$.

Outline

The First-order Part of WKL_0

Theorem 7

Let M be any countable model of RCA_0. Then M is an ω-submodel of some countable model of WKL_0.

- The theorem above shows that the first part order part of WKL_0 is the same as that of RCA_0, particularly, namely $\Sigma^0_1 - \mathsf{PA}$.
- This is a previously unpublished result of Harrington.
- Our proof will employ kind of forcing argument in which the forcing conditions are trees.

Definition 8

Let M be a model of RCA_0.

1. We define $\mathcal{T}_M$ to be the set of all $T \in \mathcal{S}_M$ such that
$$M \models T \text{ is an infinite subtree of } 2^{<\mathbb{N}}.$$
For $T \in \mathcal{T}_M$ and $X \subseteq |M|$, we say that X is a path through T if, for all $b \in |M|$, $X[b] \in T$.Here $X[b] \in T$ means that there exists $\sigma \in |M|$ such that $M \models \sigma \in T$ and $lh(\sigma) = b$, and for all $a <_M b$, $a \in X$ if and only if $M \models \sigma(a) = 1$.
2. We say that $\mathcal{D} \subseteq \mathcal{T}_M$ is dense if for all $T \in \mathcal{T}_M$ there exists $T' \in \mathcal{D}$ such that $T' \subseteq T$. We say that $\mathcal{D}$ is M-definable if there exists a formula $\phi(X)$ with parameters from $|M| \cup \mathcal{S}_M$ and no free variables other than X, such that for all $T \in \mathcal{T}_M$, $M \models \phi(T)$ if and only if $T \in \mathcal{D}$.
3. We say that $G \subseteq |M|$ is $\mathcal{T}_M$-generic if for every dense, M-definable $D \subseteq \mathcal{T}_M$ there exists $T \in \mathcal{D}$ such that G is a path through T.

Lemma 9

Let M be a countable model of RCA_0. Given $T \in \mathcal{T}_M$, we can find a $\mathcal{T}_M$-generic $G \subseteq |M|$ such that a path through T.

Lemma 9

Let M be a countable model of RCA_0. Given $T \in \mathcal{T}_M$, we can find a $\mathcal{T}_M$-generic $G \subseteq |M|$ such that a path through T.

Proof.

Since M is a countable, the set of all dense M-definable sets $\mathcal{D} \subseteq \mathcal{T}_M$ is countable. Let $\langle \mathcal{D}_i : i < \omega \rangle$ be an enumeration of these dense sets. Given $T \in \mathcal{T}_M$, we can find a sequence of trees T_i, $i < \omega$, such that $T_0 = T$, $T_{i+1} \subseteq T_i$, and $T_{i+1} \in \mathcal{D}_i$ for all $i < \omega$. We are going to show that there is a unique G such that, for all $i < \omega$, G is a path through T_i. ❒

The First-order Part of WKL_0

Lemma 10

Let M be a model of RCA_0 and suppose that $G \subseteq |M|$ is $\mathcal{T}_M$-generic. Let M' be the L_2-structure with the same first order part as M and $\mathcal{S}_{M'} = \mathcal{S}_M \cup \{G\}$. Then M' satisfies Σ^0_1 induction.

Lemma 10

Let M be a model of RCA_0 and suppose that $G \subseteq |M|$ is $\mathcal{T}_M$-generic. Let M' be the L_2-structure with the same first order part as M and $\mathcal{S}_{M'} = \mathcal{S}_M \cup \{G\}$. Then M' satisfies Σ^0_1 induction.

Sketch of Proof:

- It suffices to prove that, for any $b \in |M|$ and any Σ^0_1 formula $\varphi(i, X)$ with parameters from $|M| \cup \mathcal{S}_M$ and no free variables other than i and X, the set $\{a : a <_M b \wedge M' \models \varphi(a, G)\}$ is M-finite.
- In order to prove this, assume first that $\varphi(i, X)$ is in normal form, i.e., $\varphi(i, X) \equiv \exists j \theta(i, X[j])$ where $\theta(i, \tau)$ is Σ^0_0 with parameters from $|M| \cup \mathcal{S}_M$.

- Let $\mathcal{D}_b$ be the set of $T \in \mathcal{T}_M$ such that, for each $a <_M b$, M satisfies either

  (i) $\forall \tau(\tau \in T \to \neg\theta(a, \tau))$, or

  (ii) $\exists k \forall \tau((\tau \in T \wedge lh(\tau) = k) \to \exists j \leq k \theta(a, \tau[j]))$,

  where $\tau[j]$ denotes the initial sequence of τ of length j. The motivation here is that if G is q path through T, then (i) gives $\neg\varphi(a, G)$ while (ii) gives $\varphi(a, G)$.
- We claim that $\mathcal{D}_b$ is dense in $\mathcal{T}_M$ and M-definable.
- By bounded Σ^0_1 comprehension i.e. $\forall n \exists X \forall i(i \in X \to (i < n \wedge \varphi(i)))$ where $\varphi(i)$ is Σ^0_1, we completes the proof.

Lemma 11

Let M be any L_2-structure which satisfies the basic axioms plus the Σ^0_1 induction scheme. Then M is an ω-submodel of some model of RCA_0.

The First-order Part of WKL_0

Lemma 11

Let M be any L_2-structure which satisfies the basic axioms plus the Σ^0_1 induction scheme. Then M is an ω-submodel of some model of RCA_0.

Lemma 12

Let M be a countable model of RCA_0. Given $T \in \mathcal{T}_M$, there exists a countable model M'' of RCA_0 such that M is an ω-submodel of M'', and $M'' \models T$ has a path.

Corollary 13

For any Π^1_1 sentence ψ, if ψ is a theorem of WKL_0 then ψ is already a theorem of RCA_0.

The First-order Part of WKL_0

Corollary 13

For any Π^1_1 sentence ψ, if ψ is a theorem of WKL_0 then ψ is already a theorem of RCA_0.

Corollary 14

The first order part of WKL_0 is the same as that of RCA_0, namely $\Sigma^0_1 - PA$.

Outline

Lemma 15

Any model of $\Sigma_1^0 - PA$ can be expanded to a model or PRA in a way which respects the canonical interpretation of L_1 into the language of PRA.

A Conservation Result for Hilbert's Program

Lemma 15

Any model of $\Sigma_1^0 - PA$ can be expanded to a model or PRA in a way which respects the canonical interpretation of L_1 into the language of PRA.

Theorem 16

Let θ be any L_1-formula. If θ is provable in PRA under the canonical interpretation, then θ is provable in $\Sigma_1^0 - PA$ (hence also in RCA_0).

A Conservation Result for Hilbert's Program

Lemma 15

Any model of $\Sigma_1^0 - PA$ can be expanded to a model or PRA in a way which respects the canonical interpretation of L_1 into the language of PRA.

Theorem 16

Let θ be any L_1-formula. If θ is provable in PRA under the canonical interpretation, then θ is provable in $\Sigma_1^0 - PA$ (hence also in RCA_0).

Having shown that PRA is essentially included in $\Sigma_1^0 - \mathrm{PA}$, we now turn to converse. We shall show that every Π_2^0 sentences which is provable in $\Sigma_1^0 - \mathrm{PA}$ (indeed WKL_0) is provable in PRA.

Definition 17

A formula in the language of PRA is said to be generalized Σ_0^0 if it is build from atomic formulas of the form $t_1 = t_2$ and $t_1 < t_2$, where t_1 and t_2 are terms in the language of PRA, by means of propositional connectives and bounded quantifiers.

Definition 17

A formula in the language of PRA is said to be generalized Σ_0^0 if it is build from atomic formulas of the form $t_1 = t_2$ and $t_1 < t_2$, where t_1 and t_2 are terms in the language of PRA, by means of propositional connectives and bounded quantifiers.

The following lemma tells us that every generalized Σ_0^0 formula is equivalent to an atomic formula.

Lemma 18

For any generalized Σ_0^0 formula $\theta(x_1, \ldots, x_k)$ with only the displayed free variables, we can find a k-place primitive recursive function symbol $\underline{f} = \underline{f}_\theta$ such that PRA proves

(1) $\underline{f}(x_1, \ldots, x_k) = \underline{1} \leftrightarrow \theta(x_1, \ldots, x_k)$

(2) $\underline{f}(x_1, \ldots, x_k) = \underline{0} \leftrightarrow \neg\theta(x_1, \ldots, x_k)$

Definition 19

Let M be a model of PRA.

1. An M-finite set is a set $X \subseteq |M|$ such that
$$X = \{a \in |M| : a <_M b \wedge R_M(a, c_1, ..., c_k)\}$$
for some primitive predicate symbol $\underline{R}$ and some parameters $b, c_1, ..., c_k \in |M|$.

2. If X is an M-finite set, the M-cardinality of X is the number of element of X as counted within M. Formally, the M-cardinality of X is defined as $card_M(X) = card_M(X, b)$ where $X \subseteq \{a : a <_M b\}$ and
$$\begin{aligned} card_M(X, 0) &= 0 \\ card_M(X, a+1) &= \begin{cases} card_M(X, a) + 1 & \text{if } a \in X, \\ card_M(X, a) & \text{if } a \notin X. \end{cases} \end{aligned}$$

Lemma 20

Let M be a model of PRA. Then for every M-finite set X, there is a unique $c \in |M|$ which encodes X. Furthermore $X \subseteq \{a : a <_M b\}$ if and only if $c <_M 2^b$.

Proof.

The code of X is $c = \sum_{a \in X} 2^a$. More formally, we define

$$c = code_M(X) = code_M(X, b)$$

where $X \subseteq \{a : a <_M b\}$ and

$$\begin{aligned} code_M(X, 0) &= 0 \\ code_M(X, a+1) &= \begin{cases} code_M(X, a) + 2^a & \text{if } a \in X, \\ code_M(X, a) & \text{if } a \notin X. \end{cases} \end{aligned}$$

□

Definition 21

Let M be a model of PRA.

1. A cut in M is a set $I \subseteq |M|$, $1_M \in I \neq |M|$, such that successor bounded and $c <_M b$, $b \in I$ imply $c \in I$.
2. If I is a cut in M, a set $X \subseteq I$ is said to be M-coded if there is an M-finite set X^* such that $X^* \cap I = X$. The set of all M-coded subsets of I is denoted $Coded_M(I)$. A set X is said to be bounded in I if $X \subseteq \{a : a <_M b\}$ for some $b \in I$.
3. A cut I is said to be semiregular if, for all M-finite sets such that $card_M(X) \in I$, $X \cap I$ is bounded in I.

Lemma 22

Let M be a model of PRA, and let I be a semiregular cut in M. Then

$$(I, Coded_M(I), +_M \restriction I, \cdot_M \restriction I, 0_M, 1_M, <_M \restriction I)$$

is a model of WKL_0.

Definition 23

Let M be a model of PRA. For $b, c \in |M|$, we write $b \ll_M c$ to mean that $f_M(b) <_M c$ for all 1-place primitive recursive function symbols $\underline{f}$.

Definition 23

Let M be a model of PRA. For $b, c \in |M|$, we write $b \ll_M c$ to mean that $f_M(b) <_M c$ for all 1-place primitive recursive function symbols $\underline{f}$.

Lemma 24

Let M be a countable model of PRA. Suppose that $b, c \in |M|$ are such that $b \ll_M c$. Then there is a semiregular cut I in M such that $b \in I$ and $c \notin I$.

A Conservation Result for Hilbert's Program

Theorem 25

Let ψ be a Π^0_2 sentence. If ψ is provable in WKL_0, the ψ is provable in PRA (under the canonical interpretation of L_1 into the language of PRA).

Outline

Summary

- Theorem above emerges as a key result toward a partial realization of Hilbert's program. The theorem shows that WKL_0 is conservative over PRA for Π^0_1 sentences (in fact Π^0_2 sentences). This conservation result implies that a significant part of mathematical practice is finitistically reducible, in the precise sense envisioned by Hilbert.
- Conjecture: Let ψ be a Π^0_2 sentence. If ψ is provable in RT^2_2, the ψ is provable in PRA (under the canonical interpretation of L_1 into the language of PRA).

References

W. W. Tait,
Finitism.
Journal of Philosophy, 1981, pp.524-546.

S. G. Simpson,
Partial Relazations of Hilbert's Program.
Journal of Symbolic Logic, 1988, pp.349-363.

S. G. Simpson,
Subsystems of Second Order Arithmetic.
Springer-Verlag, Berlin, 1999.

J. B. Paris, L. Harrington,
Amathematical incompletenes in Peano arithmetic.
In Handbook of mathematical logic, Springer-Verlag, Berlin, 1977.

The End

THANKS!