Chapter 7

Some Other Related Results

7.1 Tarski's Undefinability of Truth

We show that the truth inside the standard model is not definable by an $\mathcal{L}_{\mathcal{A}}$-formula in the following sense:

Theorem 1.1: Tarski's undefinability theorem

There is no $\mathcal{L}_{\mathcal{A}}$-formula $\mathcal{T}_{truth.}(x_0)$ such that for any closed $\mathcal{L}_{\mathcal{A}}$-formula φ one has

$$\mathbb{N} \models \varphi \longleftrightarrow \mathcal{T}_{truth.}(\ulcorner \varphi \urcorner).$$

Proof of Theorem 1.1:

Towards a contradiction, we assume $\mathcal{T}_{truth.}(x_0)$ exists and consider some formula $\ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}(x_0)$ which satisfies:

$$\ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}(\ulcorner \varphi \urcorner) := \ulcorner \varphi \urcorner \in \mathcal{F}_{\checkmark x_0\ !free} \longrightarrow \neg \mathcal{T}_{truth.}(\ulcorner \varphi_{[\ulcorner \varphi \urcorner / x_0]} \urcorner) \ a.$$

We then consider the closed formula $\ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.\,[\ulcorner \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.} \urcorner / x_0]}$ and discuss whether

(1) $\mathbb{N} \models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.\,[\ulcorner \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.} \urcorner / x_0]}$ or (2) $\mathbb{N} \not\models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.\,[\ulcorner \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.} \urcorner / x_0]}$.

First, notice that since $\ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}(x_0)$ is some $\mathcal{L}_{\mathcal{A}}$-formula whose only free variable is x_0, we have $\mathbb{N} \models \ulcorner \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.} \urcorner \in \mathcal{F}_{\checkmark x_0\ !free}$. Therefore we also have

(1) $\mathbb{N} \models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}$

$\Rightarrow \mathbb{N} \models \neg\mathcal{T}_{ruth.}\left(\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}\rceil\right)$ *(by definition of $\ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}$)*

$\Rightarrow \mathbb{N} \not\models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}$ *(by definition of the $\mathcal{T}_{ruth.}$ predicate)*

(2) $\mathbb{N} \not\models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}$

$\Rightarrow \mathbb{N} \not\models \mathcal{T}_{ruth.}\left(\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}\rceil\right)$ *(by definition of the $\mathcal{T}_{ruth.}$ predicate)*

$\Rightarrow \mathbb{N} \models \neg\mathcal{T}_{ruth.}\left(\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}\rceil\right)$ *(by definition of the $\models$ relation)*

$\Rightarrow \mathbb{N} \models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}$ *(by definition of $\ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}$)*

We have obtained

$$\mathbb{N} \models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]} \iff \mathbb{N} \not\models \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}{}_{[\lceil \ddot{\mathcal{D}}_{iag.}\mathcal{T}_{r.}\rceil/x_0]}$$

which contradicts the existence of the formula $\mathcal{T}_{ruth.}(x_0)$.

□

[a] We recall that $\lceil\lceil\varphi\rceil\rceil$ stands for the term $\overbrace{S\ldots S}^{\lceil\varphi\rceil}\,0$.

7.2 Recursive Countable Models of Peano Arithmetic

Definition 2.1

A countable model of $\mathcal{P}eano$ is (up to isomorphism) some $\mathcal{L}_{\mathcal{A}}$-structure of the form

$$\mathcal{M} = \langle \mathbb{N}, 0^{\mathcal{M}}, S^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}} \rangle$$

that satisfies $\mathcal{M} \models \mathcal{P}eano$.
Such a model is *recursive* if the following functions are recursive.

- $S^{\mathcal{M}} : \mathbb{N} \to \mathbb{N}$
- $+^{\mathcal{M}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- $\cdot^{\mathcal{M}} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Theorem 2.1: Tennenbaum's theorem

The only[a] recursive countable model of $\mathcal{P}eano$ is the standard model.

[a] Up to isomorphism.

7.3 Gödel's 1st Incompleteness Theorem is Provable in RCA_0

Second order arithmetic is not a theory of second order logic, but rather a two-sorted first order theory. This means that in the language there are two different sorts of variables and terms: the numeric terms and the set terms. With respect to the semantic, the numeric variables and the set variables range on different sets of objects: numeric variables vary over integers (whether there are standard or non-standard); whereas set variables vary on sets of integers.

Definition 3.1: The language of second order arithmetic

The language of second order arithmetic $\mathcal{L}_{\mathcal{A}^2}$ is a two-sorted language: there are two kinds of terms.

numeric terms

- $x_0, x_1, \ldots$ are countably numeric variables that are numeric terms,
- 0 is a numeric term,
- if t, s are numeric terms, then the following are numeric terms
  - St
  - $t{+}s$
  - $t{\cdot}s$

set terms

- $X_0, X_1, \ldots$ are countably set variables that are set terms,

Definition 3.2: The formulas of second order arithmetic

- The atomic formulas are of the form
  - $t = s$
  - $t \in X$

  for t, s any numeric terms and X any set term[a].

- If φ, ψ are formulas, and x is a numeric variable and X is a set variable, then the following are formulas:

• atomic formulas	• $(\varphi \wedge \psi)$	• $(\varphi \longleftrightarrow \psi)$	• $\forall x \varphi$
• $\neg\varphi$	• $(\varphi \vee \psi)$	• $\exists x \varphi$	
	• $(\varphi \longrightarrow \psi)$	• $\exists X \varphi$	• $\forall X \varphi$

[a] Necessarily some set variable.

Definition 3.3: Semantic of second order arithmetic

An $\mathcal{L}_{\mathcal{A}^2}$-structure is of the form

$$\mathcal{M} = \langle M_1, M_2, 0^{\mathcal{M}}, S^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}} \rangle$$

such that

- M_1 is a non empty set,
- $M_2 \subseteq \mathcal{P}(M_1)$ is a non empty set (in case of full second order arithmetic one has exactly $\mathcal{P}(M_1) = M_2$)
- $0^{\mathcal{M}} \in M_1$
- $S^{\mathcal{M}} : M_1 \to M_1$
- $+^{\mathcal{M}} : M_1 \times M_1 \to M_1$
- $\cdot^{\mathcal{M}} : M_1 \times M_1 \to M_1$

Given any $\mathcal{L}_{\mathcal{A}^2}$-formula φ and any $\mathcal{L}_{\mathcal{A}^2}$-structure $\mathcal{M}$ as above, the definition of the satisfaction relation $\mathcal{M} \models \varphi$ is as usual for first order logic, except that numeric variables vary over M_1 while set variables vary over M_2.
In terms of the evaluation game $\mathbb{EV}(\mathcal{M}, \varphi)$, the rules become:

if φ is	*who plays*	*the game goes on with*
atomic formula	*no one*	*the game ends*
$\exists x\,\psi$	**V***erifier picks some* $a \in M_1$	$\psi_{[a/x]}$
$\forall x\,\psi$	**F***alsifier picks some* $a \in M_1$	$\psi_{[a/x]}$
$\exists X\,\psi$	**V***erifier picks some* $S \in M_2$	$\psi_{[S/X]}$
$\forall X\,\psi$	**F***alsifier picks some* $S \in M_2$	$\psi_{[S/X]}$
$(\varphi_1 \vee \varphi_2)$	**V***erifier chooses* φ_1 *or* φ_2	*the chosen subformula*
$(\varphi_1 \wedge \varphi_2)$	**F***alsifier chooses* φ_1 *or* φ_2	*the chosen subformula*
$\neg\psi$	**V***erifier and* **F***alsifier switch roles*	ψ

Except for the distinction between the two different sorts of variables, proofs in second order arithmetic behave as in first order logic.

Definition 3.4: $\mathbf{Z_2}$: the theory of full second order arithmetic

The Theory $\mathbf{Z_2}$ of full second order arithmetic is composed of the following axioms:

- $\mathcal{R}ob$.
- The second order induction scheme: for every formula $\varphi(x, X)$ *where* x *and* X *may occur freely*,

$$\forall X\Big(\big(\varphi(0/x, X) \wedge \forall x(\varphi(x, X) \longrightarrow \varphi(Sx/x, X))\big) \longrightarrow \forall x\ \varphi(x, X)\Big)$$

- The comprehension scheme: for every formula $\varphi(x)$ where other variables may occur freely, *but not the variable* X

$$\exists X \forall x\ \big(x \in X \longleftrightarrow \varphi(x)\big).$$

Most proofs that one encounters in Analysis can be conducted within $\mathbf{Z_2}$ + **DC** where **DC** (Dependent Choice) is a weak form of the **AC** (Axiom of Choice). The proof of Gödel's 1st incompleteness theorem only requires a fragment of $\mathbf{Z_2}$ – i.e., a theory whose axioms are all theorems of $\mathbf{Z_2}$ – known as $\mathbf{RCA_0}$.

Definition 3.5: The theory $\mathbf{RCA_0}$

The Theory $\mathbf{RCA_0}$ is a fragment of the full second order theory of arithmetic composed of the following axioms:

- $\mathcal{R}ob. + I\Sigma_1^0$
- The second order induction axiom

$$\forall X \Big(\big(0 \in X \wedge \forall x (x \in X \longrightarrow Sx \in X)\big) \longrightarrow \forall x \; x \in X \Big)$$

- The (recursive) comprehension scheme for Δ_0^0 formulas:
  given any Σ_1^0-formula $\varphi_\Sigma(x)$ and any Π_1^0-formula $\varphi_\Pi(x)$

$$\forall x \big(\varphi_\Sigma(x) \longleftrightarrow \varphi_\Pi(x)\big) \longrightarrow \exists X \forall x \; \big(x \in X \longleftrightarrow \varphi_\Sigma(x)\big).$$

The name $\mathbf{RCA_0}$ stands for "Recursive Comprehension Axiom for Δ_0^0-formulas" because all the sets of integers that $\mathbf{RCA_0}$ proves to exist are recursive.

In other words, $\mathbf{RCA_0}$ is too weak to prove the existence of non-recursive sets.

Proposition 3.1

Gödel's 1st incompleteness theorem is provable inside $\mathbf{RCA_0}$.

7.4 Presburger Arithmetic

Gödel's 1st incompleteness Theorem implies that the complete $\mathcal{L}_\mathcal{A}$-theory[1] of the standard model $\langle \mathbb{N}, 0, S, +, \cdot \rangle$ is undecidable.

If we consider the first order language whose signature is $\mathcal{L}'_\mathcal{A} = \{0, 1, +, \cdot, <\}$, it follows from Gödel's 1st incompleteness Theorem, that the complete $\mathcal{L}'_\mathcal{A}$-theory of the standard model $\langle \mathbb{N}, 0, 1, +, \cdot, < \rangle$ is also undecidable.

But if we remove the multiplication function symbol $\cdot$ from the language, then the complete theory of the standard model $\langle \mathbb{N}, 0, 1, +, < \rangle$ becomes decidable.

[1] Where $\mathcal{L}_\mathcal{A} = \{0, S, +, \cdot\}$.

Definition 4.1: Presburger Arithmetic

Let $\mathcal{L} = \{0, 1, +, <\}$, where $0, 1$ are constant symbols, $+$ is a binary function symbol, and $<$ is a binary relation symbol.

Presburger Arithmetic ($\mathcal{P}resb.$) is the complete $\mathcal{L}$-theory of the structure $\langle \mathbb{Z}, 0, 1, +, < \rangle$.
i.e.,

$$\mathcal{P}resb. = \{\varphi \text{ closed } \mathcal{L}\text{-formula } \mid \mathbb{Z} \models \varphi\}.$$

Theorem 4.1

Presburger Arithmetic is decidable.

i.e.,

The complete theory of the structure $\langle \mathbb{Z}, 0, 1, +, < \rangle$ is decidable.

The original proof of this result — due to Presburger himself — relies on the method of quantifier elimination which provides an algorithm that transforms any given formula into some quantifier free equivalent formula from which is then easy to decide [45, 9]. An other approach — due to the Swiss mathematician Julius Richard Büchi — to deciding Presburger arithmetic consists in constructing a finite-state automaton whose language mirror all satisfying assignments of a given formula [5].

Adding multiplication to Presburger Arithmetic makes it undecidable as was shown by Alonzo Church [7].

Theorem 4.2

The complete theory of the structure $\langle \mathbb{Z}, 0, 1, +, \cdot, < \rangle$ is undecidable.

7.5 Real Closed Fields

Definition 5.1: Real Closed Fields

Let $\mathcal{L}_{rcf} = \{0, 1, +, \cdot, <\}$, where $0, 1$ are constant symbols, $+, \cdot$ are a binary function symbols, and $<$ is a binary relation symbol. Let $\mathcal{R} = \langle |\mathcal{R}|, 0, 1, +, \cdot, < \rangle$ be any $\mathcal{L}_{rcf}$ -structure.

$\mathcal{R}$ is a real closed field if

$$\langle |\mathcal{R}|, 0, 1, +, \cdot, < \rangle \text{ is elementary equivalent to } \langle \mathbb{R}, 0, 1, +, \cdot, < \rangle .$$

We recall that two structures are elementary equivalent if they satisfy the same closed formulas. So, $\mathcal{R}$ is a real closed field if the complete $\mathcal{L}_{rcf}$-theories of $\mathcal{R}$ and $\mathbb{R}$ are exactly the same.

One can also define real closed fields in some other ways. For instance, by saying that a real closed field is any $\mathcal{L}_{rcf}$-structure $\mathcal{R} = \langle M, 0, 1, +, \cdot, < \rangle$ that satisfies both

(1) the field axioms:

- $\forall x \, \forall y \, \forall z \ (x+y)+z = x+(y+z)$ (associativity of addition)
- $\forall x \, \forall y \, \forall z \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)
- $\forall x \, \forall y \ x+y = x+y$ (commutativity of addition)
- $\forall x \, \forall y \ x \cdot y = x \cdot y$ (commutativity of multiplication)
- $\forall x \ x+0 = x$ (additive identity)
- $\forall x \ x \cdot 1 = x$ (multiplicative identity)
- $\forall x \, \exists y \ x+y = 0$ (additive inverses)
- $\forall x \neq 0 \ \exists y \ x \cdot y = 1$ (multiplicative inverses)
- $\forall x \, \forall y \, \forall z \ x \cdot (y+z) = (x \cdot y)+(x \cdot z)$ (distributivity of multiplication over addition)

(2) and any of the following equivalent conditions:

- $\mathcal{R}$ is not algebraically closed, but its algebraic closure is a finite extension.
- $\mathcal{R}$ is not algebraically closed but the field extension $\mathcal{R}(\sqrt{-1})$ is algebraically closed.
- $<^{\mathcal{R}}$ is a total order on $|\mathcal{R}|$ making it an ordered field such that, in this ordering, every positive element of $\mathcal{R}$ has a square root in $\mathcal{R}$ and any polynomial of odd degree with coefficients in $\mathcal{R}$ has at least one root in $\mathcal{R}$.

Theorem 5.1

Let $\mathcal{L}_{rcf} = \{0, 1, +, \cdot, <\}$ and $\mathcal{R} = \langle |\mathcal{R}|, 0, 1, +, \cdot, < \rangle$ be any real closed field.

The complete theory of $\mathcal{R}$ is decidable.

Alfred Tarski proved this important result by means of quantifier elimination methods [58]. This result is of course equivalent to the following one:

Theorem 5.2

The complete theory of $\langle \mathbb{R}, 0, 1, +, \cdot, < \rangle$ is decidable.

An immediate consequence of Church's undecidability of the complete theory of the structure $\langle \mathbb{Z}, 0, 1, +, \cdot, < \rangle$ (Theorem 4.2) is the following:

Corollary 5.1

Let $\mathcal{L}_{rcf} = \{0, 1, +, \cdot, <\}$ and $\mathbb{R} = \langle \mathbb{R}, 0, 1, +, \cdot, < \rangle$.

- There is no $\mathcal{L}_{rcf}$-formula $\varphi_{\mathbb{Z}}(x)$ such that for all real a $\mathbb{R} \models \varphi(a) \iff a \in \mathbb{Z}$
- There is no $\mathcal{L}_{rcf}$-formula $\varphi_{\mathbb{N}}(x)$ such that for all real n $\mathbb{R} \models \varphi(n) \iff n \in \mathbb{N}$.

7.6 Hilbert's 10$^{\text{th}}$ Problem

Hilbert's 10$^{\text{th}}$ problem is the tenth of a list of 23 problems that David Hilbert posed in 1900.

The original formulation of Hilbert's 10$^{\text{th}}$ problem was:

> *"Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: to devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers."*

A Diophantine equation is a polynomial equation with natural coefficients (in $\mathbb{Z}$) and usually several unknowns, such that the only solutions of interest are the integer ones (those where all unknowns take values inside $\mathbb{N}$).

The modern formulation of Hilbert's 10$^{\text{th}}$ problem is whether one can decide if one or more solutions exist given some Diophantine equation. In other words, does there exist an algorithm to check whether any given Diophantine equation has a solution.

Hilbert's 10$^{\text{th}}$ problem remained open for 70 years and was solved in 1970 [38, 46, 16, 19]. It received a negative answer known as Matiyasevich's theorem or the MRDP theorem (Yuri Matiyasevich, Julia Robinson, Martin Davis, Hilary Putnam).

Given a diophantine equation of the form $P(y_1, \ldots, y_n, x_1, \ldots, x_k) = 0$, one distinguishes, among the variables $x_1, \ldots, x_k, y_1, \ldots, y_n$, between the unknowns $x_1, \ldots, x_k$ and the parameters $y_1, \ldots, y_n$.

Definition 6.1: Diophantine set

A Diophantine set S is any subset $S \subseteq \mathbb{N}^n$ (any $n \in \mathbb{N}$) such that there exists some Diophantine equation $P(y_1, \ldots, y_n, x_1, \ldots, x_k) = 0$ that satisfies:

$$\forall y_1 \in \mathbb{N} \ldots \forall y_n \in \mathbb{N} \left((y_1, \ldots, y_n) \in S \longleftrightarrow \exists x_1 \in \mathbb{N} \ldots \exists x_k \in \mathbb{N}\, P(y_1, \ldots, y_n, x_1, \ldots, x_k) = 0 \right)$$

Matiyasevich-Robinson-Davis-Putnam Theorem 6.1

Given any integer n and $S \subseteq \mathbb{N}^n$,

$$S \text{ is a Diophantine set} \iff S \text{ is recursively enumerable.}$$

For a complete proof of the Matiyasevich-Robinson-Davis-Putnam Theorem theorem, see Matiyasevich's book: *Hilbert's tenth problem* [39].