# From Hilbert's $10^{\text{th}}$ Problem to slim, Undecidable Fragments of Set Theory*

Domenico Cantone[0000−0002−1306−1166] 1, Eugenio G. Omodeo[0000−0003−3917−1942] 2, and Mattia Panettiere[1]

[1] Dept. of Mathematics and Computer Science, University of Catania, Italy
domenico.cantone@unict.it, mattia.panettiere@gmail.com
[2] Dept. of Mathematics and Earth Sciences, University of Trieste, Italy
eomodeo@units.it

**Abstract.** We revisit, deepen, and make more systematic, the study—undertaken ca. 1990—of reductions of Hilbert's tenth problem to fragments of set theory, whereby sublanguages of the Zermelo-Fraenkel axiomatic theory are shown to have an undecidable satisfiability problem.

**Key words:** Hilbert's 10th problem; Undecidability; ZF set theory; Satisfiability problem; Cartesian product; $(\forall\exists)_0$ formulas; Proof-checkers.

## Introduction

We show that the satisfiability problems for various fragments of ZF—the Zermelo-Fraenkel first-order set theory with regularity axiom—are *un*decidable. To wit, if $\boldsymbol{\Phi}$ is among those sublanguages of ZF, no algorithm can establish whether or not any given formula $\psi$ in $\boldsymbol{\Phi}$ becomes true under suitable assignments of sets to its free variables.

For each $\boldsymbol{\Phi}$ taken into account, the undecidability result stems from a uniform translation method which turns every instance $D = 0$ (with $D \in \mathbb{Z}[x_1, \ldots, x_m]$) of Hilbert's $10^{\text{th}}$ problem into a formula $\psi$ of $\boldsymbol{\Phi}$ so that $\psi$ is satisfiable if and only if the polynomial equation $D(x_1, \ldots, x_m) = 0$ has natural solutions. Through this translation, the algorithmic unsolvability of Hilbert's $10^{\text{th}}$ problem carries over to the satisfiability problem for $\boldsymbol{\Phi}$.

Some of the undecidable $\boldsymbol{\Phi}$'s are slight extensions of a core language consisting of all conjunctions of literals of the forms $x = y \cup z$, $x = y \otimes z$, $x \cap y = \varnothing$, and $|x| = |y|$, where $x, y, z$ stand for variables, $y \otimes z$ is a variant of Cartesian product consisting of singletons and unordered doubletons, and $|x| = |y|$ designates equinumerosity between $x$ and $y$. Additional conjuncts entering into play can be, e.g.: one literal of the form $\mathsf{Finite}(x)$, stating that $x$ has finitely many elements,

 We gratefully acknowledge partial support from project "STORAGE—Università degli Studi di Catania, Piano della Ricerca 2020/2022, Linea di intervento 2", and from INdAM-GNCS 2019 and 2020 research funds.

taken along with one literal of the form $x \neq \varnothing$. Another option would be to extend the said syntactic core by allowing three *negated* equinumerosity literals of the form $|x| \neq |y|$ to appear in the conjunction. Our interest in these, and similar, slim undecidable set-theoretic languages is increased by the fact that they lie extremely close to fragments of $\mathsf{ZF}$ which are either known [3, Sec.11.1], or conjectured [4, p. 239], to be decidable.

One can recast the undecidable fragments of $\mathsf{ZF}$ under study in a set-theoretic language entirely *devoid* of function symbols (such as $\cup, \otimes$, etc.), which only involves the relators $\in$ and $=$, propositional connectives, and also the constructs $\forall\, x \in y\ \varphi$ and $\exists\, x \in y\ \varphi$ involving bounded quantifiers, subject to a very restrained use. The fact that somewhat sophisticated notions like "being an ordinal", "being the first limit ordinal $\omega$", "having a finite cardinality", "being a hereditarily finite set", can be specified inside this collection of formulas, dubbed $(\forall\exists)_0$ formulas, gives evidence of the high expressive power of bounded quantification in the context of $\mathsf{ZF}$.

In a full-fledged language for set theory, $(\forall\exists)_0$ specifications are only seldom used in order to define mathematical notions. Hence, to support the correctness of the proposed $(\forall\exists)_0$-specifications of $\omega$, equinumerosity, and finitude, we have proved that they are equivalent to more direct and practical characterizations of the same notions. As we document at the `http://aetnanova.units.it/scenarios/SetTheoreticH10/`, this formal accomplishment was carried out with the aid of a proof-checker embodying a computational version of $\mathsf{ZF}$.

## 1 From Hilbert's 10$^{\text{th}}$ problem to unsolvable satisfiability problems in set theory

### 1.1 How to flatten instances of Hilbert's 10$^{\text{th}}$ problem

Consider a polynomial Diophantine equation

$$D(x_1, \ldots, x_m) = 0$$

to be solved in $\mathbb{N}$. By pulling out subterms of the polynomial $D$, we can flatten this equation into a system (viz., a conjunction) of equations of the forms

$$x = y + z\ ,\ \ x = y \cdot z\ ,\ \ x = 1\ ,\ \ x = y\ ,$$

where $x, y, z$ stand for variables, to be regarded—the new ones as well as the original ones, $x_1, \ldots, x_m$—as unknowns in $\mathbb{N}$ (cf. [10,1]). We can then eliminate each equation of the form $x = y$ by rewriting it as $x = y + \zeta$, where $\zeta$ is forced to assume the value 0 (see equations (5) below).

The flattening process can easily enforce that $x, y, z$ are distinct variables when they appear together in the same equation $x = y \star z$ (with $\star \in \{`+', `\cdot'\}$); moreover, we will keep a sole equation, $o = 1$, involving 1. The equi-solvability between the system $\Delta$ so obtained and the original equation will be obvious.

*Example 1. The equation (from [8, p. 4])*

$$4\,x_1^3\,x_2 - 2\,x_1^2\,x_3^3 \;-\; 3\,x_2^2\,x_1 \;+\; 5\,x_3 \;=\; 0 \tag{1}$$

*can be flattened into the following system $\Delta_1$ consisting of 26 equations in 28 unknowns, 3 of which are $x_1, x_2, x_3$, namely the original unknowns of* (1)*:*

$$\begin{array}{lll}
\zeta = \zeta_1 + \zeta_2\,, & \zeta_1 = \zeta_2 + \zeta\,, & \zeta_2 = \zeta + \zeta_1\,,\\
o = 1\,, & u_2 = u_1 + o\,, & u_4 = u_3 + o\,,\\
u_1 = o + \zeta\,, & u_3 = u_2 + o\,, & u_5 = u_4 + o\,,\\
P^1_{x_1} = x_1 + \zeta\,, & P^2_{x_1} = P^1_{x_1}\cdot x_1\,, & P^3_{x_1} = P^2_{x_1}\cdot x_1\,,\\
P^1_{x_2} = x_2 + \zeta\,, & P^2_{x_2} = P^1_{x_2}\cdot x_2\,, & \\
P^1_{x_3} = x_3 + \zeta\,, & P^2_{x_3} = P^1_{x_3}\cdot x_3\,, & P^3_{x_3} = P^2_{x_3}\cdot x_3\,,\\
M^1_1 = u_4\cdot P^3_{x_1}\,, & M_1 = M^1_1\cdot x_2\,, & M_4 = u_5\cdot x_3\,,\\
M^1_2 = u_2\cdot P^2_{x_1}\,, & M_2 = M^1_2\cdot P^3_{x_3}\,, & L = M_1 + M_4\,,\\
M^1_3 = u_3\cdot P^2_{x_2}\,, & M_3 = M^1_3\cdot x_1\,, & L = M_2 + M_3\,.
\end{array}$$

*By then replacing the equation $o = 1$ in $\Delta_1$ by the constraints $o \neq \zeta$ and*

$$o = o\cdot o'\,,\;\; o' = o + \zeta\,, \tag{2}$$

*(which are equisatisfiable with $o = o^2$ & $o \neq \zeta$ ), we get a system $\Delta$ which is equisolvable—in $\mathbb{N}$—with the initial equation* (1) *and consists of: 28 equations in 29 unknowns, of the forms*

$$x = y + z\,,\;\; x = y\cdot z\,, \tag{3}$$

*(where all compound terms $y \star z$ involve distinct variables) and one inequality*

$$o \neq \zeta\,. \tag{4}$$

$\dashv$

**Definition 1.** Systems that consist of flat equations of the forms (3) conjoined with the equations

$$\zeta = \zeta_1 + \zeta_2\,,\;\; \zeta_1 = \zeta_2 + \zeta\,,\;\; \zeta_2 = \zeta + \zeta_1 \tag{5}$$

and (2) and with the inequality (4), and inside which all terms of type $y + z$ and $y \cdot z$ involve distinct variables, are named CANONICAL DIOPHANTINE SYSTEMS.

*Remark 1. One can also express multiplication in terms of the* SQUARING *operation (see [6, p. 230]). Notice, in fact, that any equation of the form $x = y \cdot z$ is equisolvable in $\mathbb{N}$ with the flattened system of equations*

$$\begin{array}{lll}
p = y + z\,, & x' = x + \zeta\,, & \\
q = p^2\,, & f = y^2\,, & g = z^2\,,\\
k = x + x'\,, & h = f + g\,, & q = k + h\,,
\end{array}$$

*as can be seen from the identity*

$$\overbrace{(\underbrace{y+z}_{p})^2}^{q} = \overbrace{\underbrace{y\cdot z}_{x} + \underbrace{y\cdot z}_{x'}}^{k} + \overbrace{\underbrace{y^2}_{f} + \underbrace{z^2}_{g}}^{h} \,. \qquad \dashv$$

From a canonical Diophantine systems $\varDelta$, we will next get a conjunction $\widehat{\varDelta}$ of set-theoretic constraints of the forms:

| | | |
|---|---|---|
| $\cdot = \cdot \cup \cdot$ | UNION | (ternary relation) |
| $\cdot = \cdot \times \cdot$ | CARTESIAN PRODUCT | (ternary relation) |
| $\cdot \cap \cdot = \varnothing$ | DISJOINTNESS | (dyadic relation) |
| $\lvert\cdot\rvert = \lvert\cdot\rvert$ | EQUINUMEROSITY | (dyadic relation) |
| $\mathsf{Finite}(\cdot)$ | FINITUDE | (property) |
| $\cdot = \{\cdot\}$ | SINGLETON FORMATION | (dyadic relation) |
| $\cdot \neq \varnothing$ | NON-EMPTYNESS | (property) |
| $\lvert\cdot\rvert \neq \lvert\cdot\rvert$ | NON-EQUINUMEROSITY | (dyadic relation) |

Here, in light of the replaceability of multiplication by the squaring operation (as pointed out in Remark 1), we might only employ Cartesian square $y \times y$, without ever resorting to the product $y \times z$ with $y$ distinct from $z$.

### 1.2 How to translate a canonical Diophantine system $\boldsymbol{\varDelta}$ into unquantified fragments of set theory

Let $\varDelta$ be a Diophantine canonical system.

We translate each conjunct of $\varDelta$ according to the following rules:

$$\begin{array}{lll} x = y + z & \rightsquigarrow & u^{y,z} = y \cup z \;\;\&\;\; y \cap z = \varnothing \;\;\&\;\; \lvert u^{y,z} \rvert = \lvert x \rvert \,, \\ x = y \cdot z & \rightsquigarrow & w^{y,z} = y \times z \;\;\&\;\; \lvert w^{y,z} \rvert = \lvert x \rvert \,, \\ o \neq \zeta & \rightsquigarrow & \quad o \neq \varnothing \,, \end{array}$$

where each $u^{y,z}$ and each $w^{y,z}$ is a new variable. By also adding, for each variable $u$ in $\varDelta$, the conjunct $\mathsf{Finite}(u)$ (meaning that $\lvert u \rvert \in \mathbb{N}$), we obtain the set-theoretic counterpart $\widehat{\varDelta}$ of $\varDelta$.

Next we prove that the canonical system $\varDelta$ is satisfiable in $\mathbb{N}$ if and only if its set-theoretic counterpart $\widehat{\varDelta}$ is satisfiable in the universe of all sets. In view of the unsolvability of Hilbert's Tenth problem (see [8, Chapter 5]), we readily obtain the algorithmic unsolvability of the satisfiability problem for set-theoretic conjunctions of positive literals of the forms

$$x = y \cup z\,, \quad x = y \times z\,, \quad x \cap y = \varnothing\,, \quad \lvert x \rvert = \lvert y \rvert\,, \quad \mathsf{Finite}(x)\,,$$

plus a single inequality of the form $x \neq \varnothing$.

To carry out the first half of the proof, we observe that any set-assignment $v \mapsto Mv$ over the variables of $\widehat{\Delta}$ that satisfies $\widehat{\Delta}$ induces naturally the corresponding $\mathbb{N}$-assignment

$$v \mapsto |Mv| \tag{6}$$

over the variables of $\Delta$, and it is a simple matter to check that (6) satisfies $\Delta$. For instance, if $x = y + z$ is in $\Delta$, then the following conjuncts are in $\widehat{\Delta}$

$$\begin{array}{lll} u^{y,z} \ = \ y \cup z\,, & y \cap z \ = \ \varnothing\,, & |\, u^{y,z}\,| \ = \ |\, x\,|\ , \\ \mathsf{Finite}(x)\ , & \mathsf{Finite}(y)\ , & \mathsf{Finite}(z)\ . \end{array}$$

Hence, we have:

$$\begin{array}{lll} Mu^{y,z} \ = \ My \cup Mz\,, & My \cap Mz \ = \ \emptyset\,, & |\, Mu^{y,z}\,| \ = \ |\, Mx\,|\ , \\ |\, Mx\,| \in \mathbb{N}\,, & |\, My\,| \in \mathbb{N}\,, & |\, Mz\,| \in \mathbb{N}\,, \end{array}$$

so that

$$|\, Mx\,| = |\, Mu^{y,z}\,| = |\, My \cup Mz\,| = |\, My\,| + |\, Mz\,|\,,$$

proving that the $\mathbb{N}$-assignment (6) satisfies the equation $x \ = \ y + z$ .

Similarly, one can show that the $\mathbb{N}$-assignment (6) also satisfies all equations of the form $x \ = \ y \cdot z$ in $\Delta$ as well as the inequality $o \neq 0$.

For the converse proof, we will make use of the following notation, for every $k \in \mathbb{N}$ and $A \subseteq \mathbb{N}$:

$$[k] \coloneqq \{1, 2, \ldots, k\} \qquad \text{and} \qquad k + A \coloneqq \{k + a : a \in A\}\,.$$

Suppose that $v \mapsto \boldsymbol{v}$ is a solution to $\Delta$ in $\mathbb{N}$, and let $v_1, v_2, \ldots, v_\ell$ be the distinct variables in $\Delta$, in any fixed order. We define a set-assignment over the variables in $\widehat{\Delta}$ by putting:

- $Mv_j \coloneqq k_j + [\boldsymbol{v}_j]$, for $j = 1, \ldots, \ell$, where $k_j \coloneqq \sum_{r=1}^{j-1} \boldsymbol{v}_r$ (so that $k_1 = 0$);
- $Mu^{y,z} \coloneqq My \cup Mz$, for every literal $x \ = \ y + z$ in $\Delta$;
- $Mw^{y,z} \coloneqq My \times Mz$, for every literal $x \ = \ y \cdot z$ in $\Delta$.

We prove that the set-assignment $M$ so defined over the variables of $\widehat{\Delta}$ satisfies all of the conjuncts of $\widehat{\Delta}$.

- Let $x \ = \ y + z$ be in $\Delta$. By the definition of $M$, we have

  $$Mu^{y,z} = My \cup Mz\,,$$

  so that $M$ satisfies the conjunct $u^{y,z} = y \cup z$.

  Let $y$ and $z$ be the variables $v_i$ and $v_j$, respectively, where without loss of generality we are assuming $i < j$. Also, let $x$ be the variable $v_h$. Preliminarily, we show that

  $$Mv_i \cap Mv_j = \emptyset\,. \tag{7}$$

If $\emptyset \in \{Mv_i\,,\ Mv_j\}$, then (7) plainly holds. Otherwise, recalling that

$$Mv_i \coloneqq k_i + [\boldsymbol{v}_i] \qquad \text{and} \qquad Mv_j \coloneqq k_j + [\boldsymbol{v}_j]\,,$$

we get

$$\max Mv_i \;=\; k_i + \boldsymbol{v}_i \;=\; \sum_{r=1}^{i-1} \boldsymbol{v}_r + \boldsymbol{v}_i \;=\; \sum_{r=1}^{i} \boldsymbol{v}_r \;\leqslant\; \sum_{r=1}^{j-1} \boldsymbol{v}_r \;<\; \min Mv_j\,,$$

whence (7) follows in this case too. From (7), it follows that

$$\begin{aligned} |\,Mu^{y,z}\,| \;&=\; |\,My \cup Mz\,| \;=\; |\,My\,| + |\,Mz\,| \;=\; |\,Mv_i\,| + |\,Mv_j\,| \\ &=\; \boldsymbol{v}_i + \boldsymbol{v}_j \;=\; \boldsymbol{v}_h \;=\; |\,Mv_h\,| \;=\; |\,Mx\,|\;, \end{aligned}$$

proving that the set-assignment $M$ satisfies the conjunct $|\,Mu^{y,z}\,| \;=\; |\,Mx\,|$.

– It is even easier to prove that $M$ satisfies also the literals in $\widehat{\Delta}$ of the forms

$$w^{y,z} \;=\; y \times z\,, \qquad |\,w^{y,z}\,| \;=\; |\,x\,|\,,$$

resulting from the translation of equations of the form $x \;=\; y \cdot z$, and the only literal of the form $x \neq \varnothing$ in $\widehat{\Delta}$.

– To end, for each variable $u$ in $\Delta$, the assignment $M$ also satisfies $\mathsf{Finite}(u)$.

We have thus obtained that the set-assignment $M$ satisfies the conjunction $\widehat{\Delta}$, and hence conclude that the translation $\Delta \mapsto \widehat{\Delta}$ is satisfiability-preserving, namely:

**Theorem 1.** *A canonical Diophantine system $\Delta$ is solvable in $\mathbb{N}$* if and only if *the corresponding conjunction $\widehat{\Delta}$ is satisfied by some set-assignment.*

Consequently, from the undecidability of Hilbert's tenth problem we get:

**Lemma 1.** *The satisfiability problem for set-theoretic conjunctions of any number of positive literals of the forms*

$$x = y \cup z\,, \quad x = y \times z\,, \quad x \cap y = \varnothing\,, \quad |\,x\,| = |\,y\,| \tag{‡}$$

*and of the form* $\mathsf{Finite}(x)$*, plus* one *negative literal of the form $x \neq \varnothing$, is algorithmically unsolvable.*

Since finitude is $\subseteq$-hereditary, any conjunction $\bigwedge_{i \in I} \mathsf{Finite}(x_i)$ of finitude constraints can be replaced, without affecting satisfiability, by the conjunction $\mathsf{Finite}(F)$ *&* $\bigwedge_{i \in I} F = F \cup x_i$ containing a single finitude constraint, where $F$ is a newly introduced variable. The preceding undecidability result can hence be slightly strengthened into:

**Lemma 2.** *The satisfiability problem for set-theoretic conjunctions of any number of positive literals of the forms* (‡)*, plus* one *positive finitude literal,* $\mathsf{Finite}(x)$*, and* one *negative literal of the form $x \neq \varnothing$ is algorithmically unsolvable.*

*A fortiori*, we also have the following negative result:

**Lemma 3.** *The satisfiability problem for set-theoretic conjunctions of any number of positive literals of the forms* (‡)*, plus* one *positive finitude literal,* $\mathsf{Finite}(x)$ *, and* one *negative literal of the form* $|\,x\,| \neq |\,y\,|$ *is algorithmically unsolvable.*

The following claim gives us a way of expressing the finitude of sets:

**Proposition 1.** *A set with at least two members is finite if and only if it is the union of two sets whose cardinalities differ from its own cardinality.*

*Proof.* It suffices to note that, for an infinite set $s$ and any decomposition $s = s_1 \cup s_2$, we have (independently of whether $s_1 \cap s_2 = \varnothing$ or not) $|\,s\,| = \max(|\,s_1\,|, |\,s_2\,|)$.

Thus, without affecting satisfiability, any conjunction $\bigwedge_{i\in I} \mathsf{Finite}(x_i)$ of finitude literals can be replaced by the conjunction

$$F = F_1 \cup F_2 \ \ \& \ \ |\,F_1\,| \neq |\,F\,| \ \ \& \ \ |\,F_2\,| \neq |\,F\,| \ \ \& \ \ \bigwedge_{i\in I} F = F \cup x_i$$

containing no finitude literal, where $F, F_1, F_2$ are newly introduced variables.

In view of the preceding remark, Lemma 3 can be restated as follows.

**Lemma 4.** *The satisfiability problem for set-theoretic conjunctions of any number of positive literals of the forms* (‡)*, plus at most* three *negative literals of the form* $|\,x\,| \neq |\,y\,|$*, is algorithmically unsolvable.*

One can express finitude also in the following way:

**Proposition 2.** *A nonempty set is finite if and only if, by removing a member from it, one obtains a set of different cardinality.*

Therefore, we have:

**Lemma 5.** *The satisfiability problem for set-theoretic conjunctions of any number of positive literals of the forms* (‡)*, plus* two *positive literals of the form* $x = \{\,y\,\}$*, and* one *negative literal of the form* $|\,x\,| \neq |\,y\,|$*, is unsolvable.*

*Proof.* In view of Lemma 2, it is enough to observe that:

- a negative literal of the form $x \neq \varnothing$ can be expressed via a conjunction of the form $y' = \{\,x'\,\} \ \& \ x = x \cup y'$ where $x', y'$ are brand new variables;
- any conjunction $\bigwedge_{i\in I} \mathsf{Finite}(x_i)$ of finitude literals can be expressed by means of the conjunction

  $$F^* = \{\,f^*\,\} \ \& \ F = F \cup F^* \ \& \ F^- = F \setminus F^* \ \& \ \left|\,F^-\,\right| \neq |\,F\,| \ \ \& \ \bigwedge_{i\in I} F = F \cup x_i$$

  containing no finitude literal, where $F, F^*, F^-$ are new variables;
- a literal of the form $x = y \setminus z$ can be expressed by means of the conjunction

  $$y = x \cup x' \ \ \& \ \ x \cap x' = \varnothing \ \ \& \ \ x \cap z = \varnothing \ \ \& \ \ x' \cap y = \varnothing\,.$$

### 1.3 Undecidability results regarding unordered Cartesian product

Much the same reductions can be carried out when the operation $\otimes$ defined by

$$s \otimes t \ \coloneqq\ \big\{\{u,v\} : u \in s,\ v \in t\big\}\,.$$

(for sets $s, t$ whatsoever) supersedes the standard Cartesian product operator $\times$.

In order that Lemmas 1, 2, 3, 4, and 5 retain their validity with this *unordered product* operator $\otimes$ in place of $\times$, it suffices that the above-proposed translation rule for arithmetical constraints of the form $x = y \cdot z$ gets retouched as follows:

$$x = y \cdot z \ \rightsquigarrow\ w^{y,z} = y \otimes z \ \ \&\ \ y \cap z = \varnothing \ \ \&\ \ |\,w^{y,z}\,| = |\,x\,|\ .$$

## 2 Undecidability of a restrained collection of bounded-quantifier formulas in set theory

So far we have been designating various set-theoretic operations (e.g., dyadic union, Cartesian product, cardinality) and properties and relations (finitude, disjointness, etc.) by means of *ad hoc* signs ($\bullet \cup \bullet$, $\bullet \times \bullet$, $\mathsf{Finite}(\bullet)$, $\bullet \cap \bullet = \varnothing$, etc.) which, if adopted beforehand as primitives in the language supporting set theory, would make the undecidable fragments reviewed in Sec. 1 devoid of quantifiers.

Most often, set theories get formalized in a first-order language devoid of constants and function symbols, whose only relators are $\in$ and $=$. How complex then becomes the syntactic structure of the formulas lying in the undecidable fragments? As we will see next, a very modest usage of quantification is needed to state them: only bounded quantifiers, and just one quantifier alternation are needed, with (bounded) universal quantifiers in leading position.

### 2.1 The syntax of $(\forall\exists)_0$ formulas

Consider the first-order language $\mathcal{L}_\in$ endowed with:

- an infinite supply $\nu_0, \nu_1, \nu_2, \ldots$ of set variables;
- dyadic relators $\in, =$ designating membership and equality;
- the familiar propositional connectives $\neg$ (monadic) and $\&$, $\vee$, $\rightarrow, \leftrightarrow$ (dyadic);
- associated with each set variable $\nu_i$, the familiar quantifiers $\forall\,\nu_i$ and $\exists\,\nu_i$.

We enhance the usual syntax of formulas with two handy shortening devices:

**Definition 2.** Universal and existential BOUNDED QUANTIFIERS are introduced as follows:

$$(\forall\, x \in y)\varphi \ \leftrightarrow_{\mathrm{Def}}\ (\forall\, x)(x \in y \rightarrow \varphi)\,;$$
$$(\exists\, x \in y)\varphi \ \leftrightarrow_{\mathrm{Def}}\ (\exists\, x)(x \in y \ \&\ \varphi)\,.$$

**Definition 3.** We dub $(\forall\exists)_0$-FORMULA any conjunction $\Phi$ of the form

$$\bigwedge_{j=0}^{M} (\forall y_{j1} \in y'_{j1}) \cdots (\forall y_{jp_j} \in y'_{jp_j})\, (\exists x_{j1} \in x'_{j1}) \cdots (\exists x_{jq_j} \in x'_{jq_j})\, \varphi_j$$

where, for each $j$, the formula $\varphi_j$ is devoid of quantifiers and either $p_j > 0$, $q_j \geqslant 0$ or $p_j = q_j = 0$ holds.

## 2.2 $(\forall\exists)_0$ specifications

**Definition 4.** We dub $(\forall\exists)_0$ SPECIFICATION of an $m$-place relationship $R$ over sets a $(\forall\exists)_0$ formula $\Phi$ with free variables $a_1, \ldots, a_m, x_1, \ldots, x_\kappa$ (where $\kappa \geqslant 0$) such that, under the axioms of set theory (see below), one can prove:

$$R(a_1, \ldots, a_m) \;\leftrightarrow\; (\exists\, x_1\,, \ldots,\, x_\kappa)\; \Phi\,.$$

E.g., the right-hand sides of

$$\begin{aligned} a = b \setminus c \;&\leftrightarrow\; (\forall t \in a)(t \in b \;\&\; t \notin c) \;\&\; (\forall t \in b)(t \in c \vee t \in a)\,, \\ \mathsf{Sngl}(a) \;&\leftrightarrow\; (\exists\, x)\big(x \in a \;\&\; (\forall y \in a)(y = x)\big) \end{aligned}$$

are $(\forall\exists)_0$ specifications of the 3-place relationship $a = b \setminus c$ and, respectively, of the property "being a singleton set".

In the ongoing, our set-theoretic framework will be the theory $\mathsf{ZF}$, axiom of regularity included. First, in order to design a $(\forall\exists)_0$ specification of the property "being a finite set" (see Sec. 2.4), we will extend temporarily the signature of $\mathcal{L}_\in$ with a constant $\omega$ which is meant to designate the first limit ordinal; then we will figure out a $(\forall\exists)_0$ specification of the property "being the first limit ordinal" (see Sec. 2.5), thus ending in an impeccable $(\forall\exists)_0$ specification of *finitude*. Along the way, we will also specify the important *equinumerosity* predicate, which relates two sets when they have the same cardinality (see Sec. 2.4).

## 2.3 $(\forall\exists)_0$ specifications referring to disjointness, unionset, and weak Cartesian product

$$\boxed{\begin{aligned} x \cap y = \varnothing &\leftrightarrow (\forall\, v \in x)\big(\, v \notin y\,\big)\,, \\ x \subseteq \textstyle\bigcup y &\leftrightarrow (\forall\, x' \in x)(\exists\, y' \in y)\big(\, x' \in y'\,\big)\,, \\ \textstyle\bigcup f \subseteq v &\leftrightarrow (\forall p \in f)(\forall w \in p)(w \in v)\,, \\ \mathsf{Map_w}(f) &\leftrightarrow (\forall p \in f)(\forall x_1, x_2, x_3 \in p)\big(x_1 = x_2 \vee x_2 = x_3 \vee x_3 = x_1\big)\,, \\ f \subseteq x \otimes y &\leftrightarrow \mathsf{Map_w}(f) \quad \& \\ &\phantom{\leftrightarrow} (\forall p \in f)(\exists x' \in x)(\exists y' \in y)\big(\, x' \in p \;\&\; y' \in p\,\big) \quad \& \\ &\phantom{\leftrightarrow} (\forall p \in f)(\forall w \in p)\big(\, w \in x \vee w \in y\,\big)\,. \end{aligned}}$$

The explanation of the last of these is straightforward; here it is:

**No member of $f$ has more than two members:** $(\forall p \in f)\big(\, |p| \leqslant 2 \,\big)$,
where

$$|p| \leqslant 2 \leftrightarrow (\forall x_1, x_2, x_3 \in p)\big(\, x_1 = x_2 \vee x_2 = x_3 \vee x_3 = x_1 \,\big)\,.$$

**Each member of $f$ has the form $\{x', y'\}$ with $x' \in x$ and $y' \in y$:**

$$(\forall p \in f)(\exists x' \in x)(\exists y' \in y)\big(\, x' \in p \;\&\; y' \in p \,\big)\,.$$

**No member of a member of $f$ lies outside $x \cup y$:** $\bigcup f \subseteq x \cup y\,.$

### 2.4 $(\forall\exists)_0$ specifications of equinumerosity, squaring, and finitude

$$\boxed{\begin{aligned} \mathsf{1\text{-}1_w}(x, f, y) \leftrightarrow x \cap y = \varnothing \;\&\; f \subseteq x \otimes y \;\&\; x \subseteq \textstyle\bigcup f \;\&\; y \subseteq \textstyle\bigcup f \;\& \\ (\forall p\,,\, q \in f)(\forall v \in p)\big(\, v \in q \;\rightarrow\; p = q \,\big)\,. \end{aligned}}$$

**Meaning:**

$\mathsf{1\text{-}1_w}(x, f, y)$ can only hold if $x$ and $y$ are *disjoint* sets, in which case $f$ models a one-to-one mapping between $x$ and $y$ by means of *un*ordered pairs, in the sense that:

- $f$ consists of doubletons proper;
- each doubleton in $f$ pairs up a member of $x$ with one of $y$;
- $f$ pairs up exactly one member of $y$ with each member of $x$;
- $f$ pairs up exactly one member of $x$ with each member of $y$.

Stating that sets $x, y$ are of the *same cardinality* amounts to the statement that there is a set $y'$ such that

- $y'$ can be put in one-to-one correspondence with $x$,
- $y'$ can be put in one-to-one correspondence with $y$,
- $y'$ and $x$ are disjoint, and $y'$ and $y$ are disjoint.

Summing up, we have:

$$|x| = |y| \leftrightarrow (\exists\, y'\,,\; g\,,\; h\,)\big(\mathsf{1\text{-}1_w}(x, g, y') \;\&\; \mathsf{1\text{-}1_w}(y, h, y')\,\big)\,.$$

**Clue:** One way of concretizing $y'$, here, is by putting $y' = y \otimes \{y \cup x\}$.

Likewise, stating that the cardinalities $|x|\,, |y|$ are such that $|x| = |y|^2$ amounts to the statement that there are sets $y', x'$ such that

- $y'$ can be put in one-to-one correspondence with $y$,
- $x' = y \otimes y'$ and $x'$ can be put in one-to-one correspondence with $x$,
- $x'$ and $x$ are disjoint, and $y'$ and $y$ are disjoint.

Summing up, we have:

$$\begin{array}{rl}|x| = |y|^2 \leftrightarrow (\exists\, x', y', g, h)\big( \mathsf{Map_w}(x') & \&\quad \mathsf{1\text{-}1_w}(x', g, x) \;\& \\ & \mathsf{1\text{-}1_w}(y', h, y) \;\& \\ (\forall p \in x')(\exists u \in y)(\exists v \in y')( u \in p \;\&\; v \in p ) & \& \\ (\forall u \in y)(\forall v \in y')(\exists p \in x')( u \in p \;\&\; v \in p ) & \big)\,. \end{array}$$

**Clue:** The equality $x' = y \otimes y'$ follows from the conjunction of $\mathsf{Map_w}(x')$ with the last two conditions, thanks to the disjointness constraint $y' \cap y = \varnothing$ hidden inside $\mathsf{1\text{-}1_w}(y', h, y)$. A convenient way to instantiate $y'$ is, again, to put $y' = y \otimes \{y \cup x\}$.

A *finite* set is one that can be put in one-to-one correspondence with a cardinal preceding (i.e., belonging to) the first infinite ordinal, $\omega$:

$$\mathsf{Finite}(x) \leftrightarrow (\exists\, o)\big(o \in \omega \;\&\; |x| = |o|\big)\,.$$

More explicitly:

$$\mathsf{Finite}(x) \leftrightarrow (\exists\, o, x', g, h)\; \big(o \in \omega \;\&\; \mathsf{1\text{-}1_w}(x', g, x) \;\&\; \mathsf{1\text{-}1_w}(x', h, o)\big).$$

### 2.5 $(\forall\exists)_0$ specification of ordinals and of the first limit ordinal

A set $t$ is said to be *transitive* if $t \subseteq \mathscr{P}(t)$; equivalently, if $\bigcup t \subseteq t$. After John von Neumann and Raphael M. Robinson, *ordinal numbers* are those transitive sets within which any two different elements can be compared by membership:

$$\boxed{\begin{array}{ll}\mathsf{Ord}(o) \leftrightarrow (\forall y \in o)(\forall y' \in y)\; y' \in o & \& \\ \qquad (\forall o_1 \in o)(\forall o_2 \in o)(o_1 = o_2 \vee o_1 \in o_2 \vee o_2 \in o_1) & \end{array}}$$

Those ordinal numbers $o$ such that $o \neq \emptyset$ and $o = \bigcup o$ are called *limit ordinals*. Plainly, the property "being a limit ordinal" is $(\forall\exists)_0$-specifiable.

To characterize uniquely the first limit ordinal, $\omega$, among all sets, it will suffice to conjoin together the following conditions, where $z, a$, and $\mathfrak{s}$ are meant to represent, respectively: $\omega$ itself, an element of $\omega$, and the successor function (modeled as a set of doubletons, each one implicitly ordered by membership):

**$z$ is a non-null ordinal:**

$$a \in z \;\&\; \mathsf{Ord}(z) \tag{8}$$

**No member of $\mathfrak{s}$ has more than two members:**

$$\mathsf{Map_w}(\mathfrak{s}) \tag{9}$$

**Each member of $\mathfrak{s}$ is a doubleton $\{x, y\}$ with $x \in y \in z$:**

$$(\forall p \in \mathfrak{s})(\exists x, y \in p)\big( x \in y \;\&\; y \in z \big) \tag{10}$$

**$\mathfrak{s}$ is single-valued:**

$$(\forall p, q \in \mathfrak{s})(\forall x, y \in p)(\forall y' \in q)\big(\ (x \in y\ \&\ x \in y'\ \&\ x \in q) \rightarrow p = q\ \big) \tag{11}$$

**The domain of $\mathfrak{s}$ includes $z$:**

$$(\forall x \in z)(\exists p \in \mathfrak{s})(\exists y \in p)\big(\ x \in p\ \&\ x \in y\ \big) \tag{12}$$

**The multi-image of $\mathfrak{s}$ includes $z \setminus \{\emptyset\}$:**

$$(\forall y \in z)(\forall e \in y)(\exists p \in \mathfrak{s})(\exists x \in p)\big(\ y \in p\ \&\ x \in y\ \big) \tag{13}$$

Thus, one can prove (in $\mathsf{ZF}$ with regularity):

$$(\forall z)\big(\ z = \omega \leftrightarrow (\exists a)(\exists \mathfrak{s})\big((8)\ \&\ \cdots\ \&\ (13)\big)\ \big)\,.$$

In fact:

- by (10) and (12), the domain of $\mathfrak{s}$ equals $z$;
- (12) and (13) yield that $z$ has no largest element;
  consequently, by (8), $z$ is an ordinal such that $z \notin \omega$;
- if $z$ were such that $\omega \in z$ then, by (13), there should exist some $x \in z$ such that $\{x, \omega\} \in \mathfrak{s}$,
- which is untenable: for, since $\mathfrak{s}$ represents an increasing function, the immediate successor $x \cup \{x\}$ of $x$ would not be in the multi-image of $\mathfrak{s}$. From $z \notin \omega$ and $\omega \notin z$, we get $z = \omega$.

## Concluding remarks and open problems

We have revisited, deepened, and made more systematic, the study undertaken long ago with [2] (see also [3, pp. 161–165]).

Can we do more along the directions envisioned in the following excerpt from a historical paper?

> [$\cdots$] *the translation of a theorem of the appropriate form in some part of mathematics shows that the corresponding Diophantine equation has no solution. Hence whatever methods went into proving the theorem can in fact be used to show that a particular Diophantine equation has no solution. It is possible that the same methods can be used to show that a class of equations including perhaps an equation of interest in itself are unsolvable. Such an example providing a new tool for solving Diophantine equations would be a considerable breakthrough. In any case, any mathematical method that has been used to prove a theorem of the appropriate form has in fact been used to show that a particular Diophantine equation has no solution. Thus all mathematical methods can be tools in the theory of Diophantine equations and perhaps we should consciously attempt to exploit them.* ” [5, pp. 338–339]

The quest is open… It may be rewarding to:

– translate back into number theory decidability results regarding fragments of set theory;
– mimic the proofs of the theorems, dubbed DPR and DPRM in [7], concerning the exponential Diophantine representability and the polynomial Diophantine representability of any r.e. set, directly inside set theory (possibly making some technical aspects of those proofs more transparent).

**Open problems**

Let $\mathsf{BSTC}\otimes$ (Boolean Set Theory with Cardinality comparison and the unordered Cartesian product) be the collection of conjunctions of any number of positive literals of the forms

$$x = y \cup z\,, \quad x = y \otimes z\,, \quad x \cap y = \varnothing\,, \quad |\,x\,| = |\,y\,|\ .$$

In sight of the still in progress decidability result for $\mathsf{MLS}\otimes$ (multilevel syllogistic with the unordered Cartesian product), concerning a positive solution to the satisfiability problem for conjunctions of literals of the forms

$$x = y \cup z\,, \quad x = y \otimes z\,, \quad x \cap y = \varnothing\,, \quad x \in y\,,$$

to precisely locate the boundary between decidability and undecidability, one should attempt to find the decidability status of the satisfiability problem for the following collections of equalities:

– $\mathsf{BSTC}\otimes$-conjunctions plus *one* negative literal of the form $x \neq \varnothing$,
– $\mathsf{BSTC}\otimes$-conjunctions plus *two* literals of any of the following forms:

$$|\,x\,| \neq |\,y\,| \qquad \text{and} \qquad x = \{\,y\,\}\,.$$

**Acknowledgements**

We are grateful to Martin Davis for his encouragement. We thank the anonymous referees for their careful comments.

## References

1. J.L. Britton. Integer solutions of systems of quadratic equations. *Mathematical Proceedings of the Cambridge Philosophical Society*, 86(3):385–389, 1979.
2. D. Cantone, Vincenzo Cutello, and Alberto Policriti. Set-theoretic reductions of Hilbert's tenth problem. In Egon Börger, Hans Kleine Büning, and Michael M. Richter, editors, *CSL '89, 3rd Workshop on Computer Science Logic, Kaiserslautern, Germany, October 2-6, 1989, Proceedings*, volume 440 of *Lecture Notes in Computer Science*, pages 65–75. Springer, 1990.
3. D. Cantone, E. G. Omodeo, and A. Policriti. *Set Theory for Computing. From Decision Procedures to Declarative Programming with Sets.* Monographs in Computer Science. Springer, 2001.
4. Domenico Cantone and Pietro Ursino. Formative processes with applications to the decision problem in set theory: II. Powerset and singleton operators, finiteness predicate. *Information and Computation*, 237:215–242, 2014.
5. Martin Davis, Yuri Matijasevič, and Julia Robinson. Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution. In *Mathematical Developments Arising From Hilbert Problems*, volume 28 of *Proceedings of Symposia in Pure Mathematics*, pages 323–378, Providence, RI, 1976. American Mathematical Society. Reprinted in [9, p. 269ff.].

6. Yu. Matiyasevich. Existential arithmetization of Diophantine equations. *Annals of Pure and Applied Logic*, 253(2-3):225–233, 2009.
7. Yu. V. Matiyasevich. Martin Davis and Hilbert's tenth problem. In Eugenio G. Omodeo and Alberto Policriti, editors, *Martin Davis on Computability, Computational Logic, and Mathematical Foundations*, volume 10 of *Outstanding Contributions to Logic*, pages 35–54. Springer, 2016.
8. Yuri Vladimirovich Matiyasevich. *Hilbert's tenth problem.* The MIT Press, Cambridge (MA) and London, 1993.
9. Julia Robinson. *The collected works of Julia Robinson*, volume 6 of *Collected Works.* American Mathematical Society, Providence, RI, 1996. ISBN 0-8218-0575-4. With an introduction by Constance Reid. Edited and with a foreword by Solomon Feferman. xliv+338 pp.
10. Thoralf Skolem. Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen. *Fundamenta Mathematicae*, 23:150–161, 1934.