Reductions of Hilbert's 10th problem to undecidable fragments of set theory *

Domenico Cantone,
Eugenio G.Omodeo,
Mattia Panettiere

JAF 39
celebrating Yuri Gurevich's 80th birthday
Fontainebleau, France
18–20/05/2020

*The authors acknowledge support from GNCS–INdAM 2019 research funds.

Overview

1. Hilbert's 10^{th} problem and how to 'flatten' its instances
2. From Hilbert's 10^{th} to unsolvable cases of the set-sat problem
3. How far outside a decidable fragment of ZF do our unsolvable prob's lie ?

Overview

4. Recasting the undecidable fragments of ZF via $(\forall\exists)_0$ formulae
5. Validation by means of a proof-checker of the proposed $(\forall\exists)_0$ specs

Overview

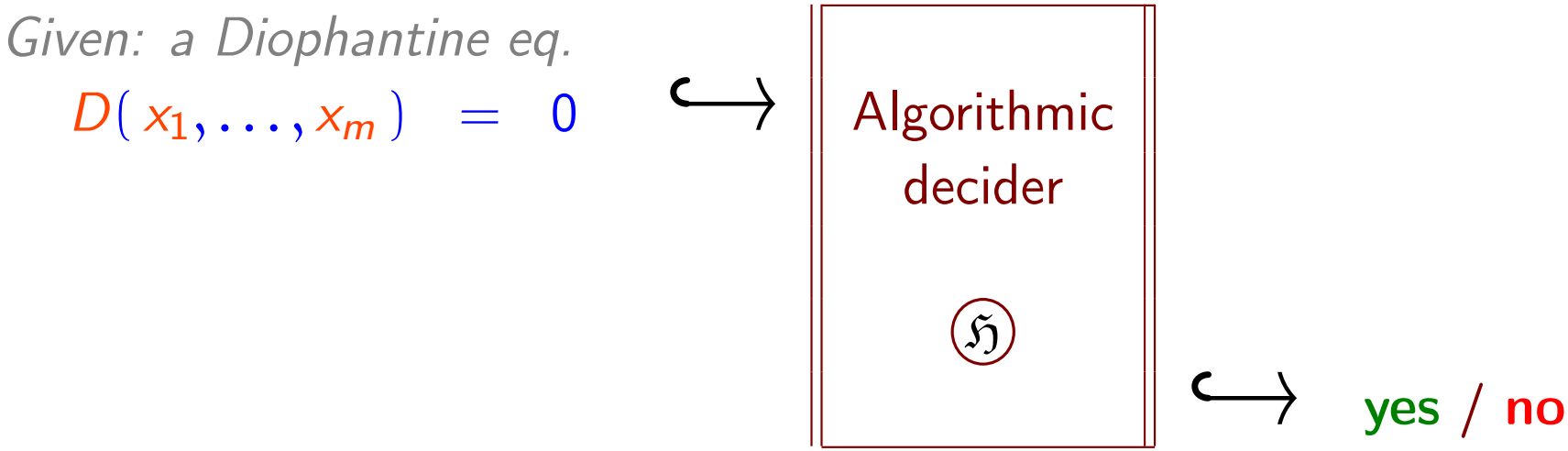
6. Any deeper links between set theory and Diophantine arithmetic ?

Overview

1. Hilbert's 10^{th} problem and how to 'flatten' its instances
2. From Hilbert's 10^{th} to unsolvable cases of the set-sat problem
3. How far outside a decidable fragment of $\mathtt{ZF}$ do our unsolvable prob's lie ?
4. Recasting the undecidable fragments of $\mathtt{ZF}$ via $(\forall\exists)_0$ formulae
5. Validation by means of a proof-checker of the proposed $(\forall\exists)_0$ specs
6. Any deeper links between set theory and Diophantine arithmetic ?
7. Bibliographic references

Hilbert's 10^{th} problem and how to 'flatten' its instances

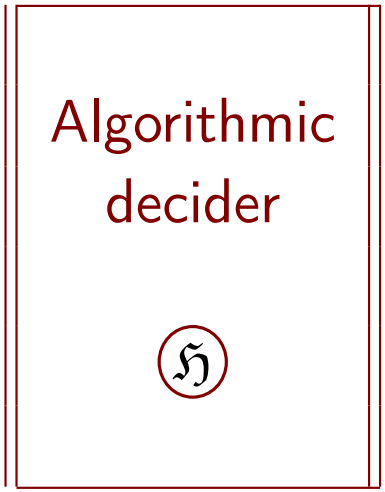
Hilbert's $10^{\underline{\text{th}}}$ problem (1900)



Scheme of a *hypothetical* solver for the $10^{\underline{\text{th}}}$ problem. The answer:

Hilbert's $10^{\underline{\text{th}}}$ problem (1900)

Given: a Diophantine eq.

$D(x_1, \ldots, x_m) = 0$ ↪ 

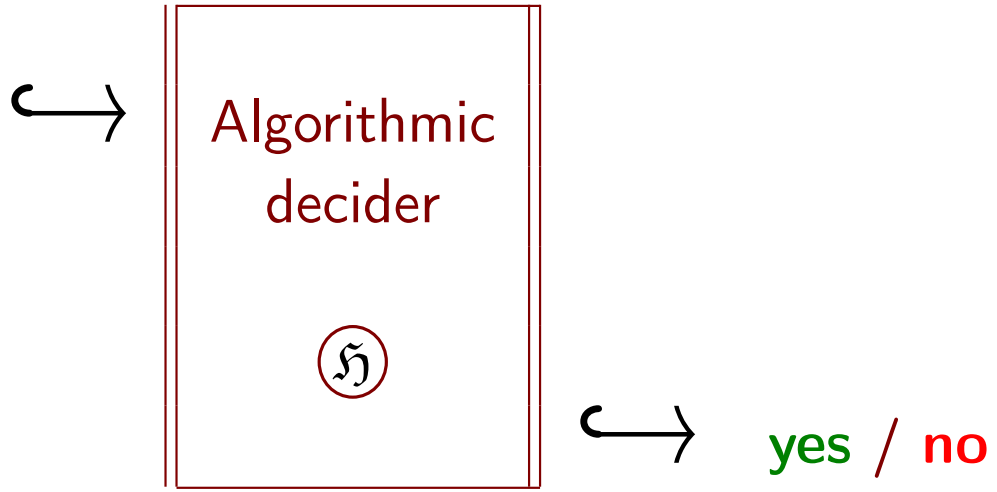
↪ yes / no

Scheme of a *hypothetical* solver for the $10^{\underline{\text{th}}}$ problem. The answer: "**no**" should indicate that there exist no solutions;

Hilbert's $10^{\underline{\text{th}}}$ problem (1900)

Given: a Diophantine eq.

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



Scheme of a *hypothetical* solver for the $10^{\underline{\text{th}}}$ problem. The answer:

"**yes**" should indicate that the equation has *at least one* solution

$$\begin{cases} x_1 = \boldsymbol{v}_1 \\ \vdots \quad \vdots \quad \vdots \\ x_m = \boldsymbol{v}_m \end{cases}$$

where each $\boldsymbol{v}_i$ is an integer (positive, negative, or null).

An adaptation of Hilbert's $10^{\underline{\text{th}}}$ problem to $\mathbb{N}$

Establishing whether or not, any given equation

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

(where D is a polynomial with coefficients in $\mathbb{Z}$),

admits a solution

1. in $\mathbb{Z}$
2. in $\mathbb{N}$

are problems translatable into each other.

This presentation will refer **H10** to $\mathbb{N}$

Theorem DPRM (1970)

Hilbert's problem **H10** is algorithmically unsolvable

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 (=conjunction) of equations of the forms

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

The ***equisolvability*** between the system Δ thus obtained and the equation given at the outset will be obvious.

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 (=conjunction) of equations of the forms

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

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 $\mathbb{N}$. We will manage that x, y, z are *distinct* when they appear in the same equation $x = y \star z$. The ***equisolvability*** between the system Δ thus obtained and the equation given at the outset will be obvious.

Example of how to flatten a Diophantine eq.

The equation[†]

$$4\,x_1^3\,x_2 - 2\,x_1^2\,x_3^3 - 3\,x_2^2\,x_1 + 5\,x_3 = 0$$

in 3 unknowns can be flattened into the following system in 22 unknowns (19 are 'temporaries'):

$$\begin{array}{lcllcllcl}
o & = & 1\,, & o_1 & = & o\,, & u_2 & = & o + o_1\,, \\
p_1 & = & u_2 \cdot x_1\,, & p_2 & = & p_1 \cdot x_1\,, & p_3 & = & p_2 \cdot x_1\,, \\
q_1 & = & u_2 \cdot x_2\,, & q_2 & = & q_1 + x_2\,, & q_3 & = & q_2 \cdot x_2\,, \\
s_1 & = & x_3\,, & s_2 & = & s_1 \cdot x_3\,, & s_3 & = & s_2 \cdot x_3\,, \\
r_1 & = & s_1 + x_3\,, & r_2 & = & r_1 + x_3\,, & r_3 & = & r_1 + r_2\,, \\
t_1 & = & p_3 \cdot q_1\,, & t_2 & = & p_2 \cdot s_3\,, & t_3 & = & q_3 \cdot x_1\,, \\
 & & & w & = & t_1 + r_3\,, & w & = & t_2 + t_3\,.
\end{array}$$

[†]Cf. [Mat93, p. 4]

Example of how to flatten a Diophantine eq.

The equation[†]

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

in 3 unknowns can be flattened into the following system in 25 unknowns (22 are 'temporaries'):

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl}
\zeta & = & \zeta_1 + \zeta_2\,, & \zeta_1 & = & \zeta_2 + \zeta\,, & \zeta_2 & = & \zeta + \zeta_1\,, \\
 & & & o_1 & = & o + \zeta\,, & u_2 & = & o + o_1\,, \\
o & \neq & \zeta\,, & o_1' & = & o + \zeta\,, & o & = & o_1 \cdot o_1'\,, \\
p_1 & = & u_2 \cdot x_1\,, & p_2 & = & p_1 \cdot x_1\,, & p_3 & = & p_2 \cdot x_1\,, \\
q_1 & = & u_2 \cdot x_2\,, & q_2 & = & q_1 + x_2\,, & q_3 & = & q_2 \cdot x_2\,, \\
s_1 & = & x_3 + \zeta\,, & s_2 & = & s_1 \cdot x_3\,, & s_3 & = & s_2 \cdot x_3\,, \\
r_1 & = & s_1 + x_3\,, & r_2 & = & r_1 + x_3\,, & r_3 & = & r_1 + r_2\,, \\
t_1 & = & p_3 \cdot q_1\,, & t_2 & = & p_2 \cdot s_3\,, & t_3 & = & q_3 \cdot x_1\,, \\
 & & & w & = & t_1 + r_3\,, & w & = & t_2 + t_3\,.
\end{array}$$

[†]Cf. [Mat93, p. 4]

Trick to avoid equations between variables

We have just seen how to eliminate equations of the form $x = y$ (with x, y distinct var's) during flattening, thanks to a new var. ζ which (in concert with others) gets the value $\mathbf{0}$. To enforce this, three constraints suffice:

Trick to avoid equations between variables

We have just seen how to eliminate equations of the form $x = y$ (with x, y distinct var's) during flattening, thanks to a new var. ζ which (in concert with others) gets the value $\mathbf{0}$. To enforce this, three constraints suffice:

$$\underbrace{\zeta = \zeta_1 + \zeta_2\,,\quad \zeta_1 = \zeta_2 + \zeta\,,\quad \zeta_2 = \zeta + \zeta_1\,,}$$
$$\zeta \leqslant \zeta_1 \leqslant \zeta_2 \leqslant \zeta \quad \therefore \quad \zeta = \zeta_1 = \zeta_2 = \mathbf{0}$$

Figure: The three variables ζ, ζ_1, ζ_2 are thus forced to take the value $\mathbf{0}$

How to employ squaring instead of product

We can also rewrite each equation of the form

$$x = y \cdot z$$

as a system involving only squaring and addition. In fact we can replace it, in light of the identity

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

by the following equations:

We can also rewrite each equation of the form

$$x = y \cdot z$$

as a system involving only squaring and addition. In fact we can replace it, in light of the identity

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

by the following equations:

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

where f, g, h, k, p, q and x' are new and, as before, $\zeta = 0$.

From Hilbert's 10^{th} problem to undecidable fragments of ZF

From arithmetic to set theory

From Δ (a flat Diophantine system) we'll get a conjunction, $\hat{\Delta}$, of set-theoretic constraints of the forms:

$\cdot = \cdot \cup \cdot$	union	(dyadic operation)
$\cdot = \cdot \times \cdot$	Cartesian product	(dyadic operation)
$\cdot \cap \cdot = \varnothing$	disointness	(dyadic relation)
$\lvert\cdot\rvert = \lvert\cdot\rvert$	equinumerosity	(dyadic relation)
$\mathsf{Finite}(\cdot)$	finitude	(property)
$\cdot = \{\cdot\}$	singleton formation	(monadic operation)
$\cdot \neq \varnothing$	non-emptyness	(property)
$\lvert\cdot\rvert \neq \lvert\cdot\rvert$	non-equinumerosity	(dyadic relation)

From Δ (a flat Diophantine system) we'll get a conjunction, $\hat{\Delta}$, of set-theoretic constraints of the forms:

$\cdot = \cdot \cup \cdot$	union	(dyadic operation)
$\cdot = \cdot \times \cdot$	Cartesian product	(dyadic operation)
$\cdot \cap \cdot = \varnothing$	disointness	(dyadic relation)
$\lvert\cdot\rvert = \lvert\cdot\rvert$	equinumerosity	(dyadic relation)
$\mathrm{Finite}(\cdot)$	finitude	(property)
$\cdot = \{\cdot\}$	singleton formation	(monadic operation)
$\cdot \neq \varnothing$	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 above), we might only employ Cartesian square $y \times y$, without ever resorting to the product $y \times z$ with y distinct from z .

Translate each conjunct of Δ, on the basis of its form:

$$x = y + z \quad \Rightarrow \quad |x| = |u_{y,z}| \ \& \ u_{y,z} = y \cup z$$
(where $u_{y,z}$ is a new var.);

$$x = y \cdot z \quad \Rightarrow \quad |x| = |w_{y,z}| \ \& \ w_{y,z} = y \times z$$
(where $w_{y,z}$ is a new var.);

$$o = 1 \quad \Rightarrow \quad o = \{\cdot\}$$
('$\cdot$' either new or the same as ζ).

By also adding the constraint

- $y \cap z = \varnothing$ for each pair y, z of distinct var's in Δ,
- Finite (v) for each variable v occurring in Δ,

we get the set-theoretic counterpart, $\hat{\Delta}$, of Δ.

Translate each conjunct of Δ, on the basis of its form:

$$x = y + z \quad \Rightarrow \quad |x| = |u_{y,z}| \ \& \ u_{y,z} = y \cup z$$
(where $u_{y,z}$ is a new var.);

$$x = y \cdot z \quad \Rightarrow \quad |x| = |w_{y,z}| \ \& \ w_{y,z} = y \times z$$
(where $w_{y,z}$ is a new var.);

$$o \neq \zeta \quad \Rightarrow \quad \text{either } o \neq \varnothing \text{ or } |o| \neq |\zeta| .$$

By also adding the constraint

- $y \cap z = \varnothing$ for each pair y, z of distinct var's in Δ ,
- Finite (v) for each variable v occurring in Δ ,

we get the set-theoretic counterpart, $\hat{\Delta}$, of Δ .

If $\hat{\Delta}$ has a solution $v \mapsto \boldsymbol{v}$ over sets, then it is plain that by restricting the function $v \mapsto |\boldsymbol{v}|$ to the unknowns of Δ we will get a solution to Δ in $\mathbb{N}$.

If $\widehat{\Delta}$ has a solution $v \mapsto \boldsymbol{v}$ over sets, then it is plain that by restricting the function $v \mapsto |\boldsymbol{v}|$ to the unknowns of Δ we will get a solution to Δ in $\mathbb{N}$.

Conversely, suppose that $v \mapsto \boldsymbol{v}$ is a solution to Δ in $\mathbb{N}$. Let us fix an order $v_1, \ldots, v_\ell$ of the distinct variables of Δ, and put

$$\widehat{\boldsymbol{v}}_i \quad =_{\mathsf{Def}} \quad \left\{ \textstyle\sum_{j=0}^{i-1} \boldsymbol{v}_j \,, \ldots, \; \boldsymbol{v}_i - 1 + \sum_{j=0}^{i-1} \boldsymbol{v}_j \right\}$$

for $i = 0, \ldots, \ell$, so that the sets $\widehat{\boldsymbol{v}}_1, \ldots, \widehat{\boldsymbol{v}}_\ell$ are p.w. disjoint and each of them satisfies $|\widehat{\boldsymbol{v}}_i| = \boldsymbol{v}_i$. Then put, for the variables $u_{y,z}$ and $w_{y,z}$:

$$\widehat{\boldsymbol{u}}_{y,z} \quad = \quad \widehat{\boldsymbol{y}} \cup \widehat{\boldsymbol{z}} \,, \qquad \widehat{\boldsymbol{w}}_{y,z} = \widehat{\boldsymbol{y}} \times \widehat{\boldsymbol{z}} \,;$$

we will thus get a *hereditarily finite* solution $v \mapsto \widehat{\boldsymbol{v}}$ for $\widehat{\Delta}$.

The equisatisfiability between Δ and $\hat{\Delta}$, just seen, along with the DPRM theorem, gives us:

Theorem CCP (Cantone–Cutello-Policriti, 1990)

> When referred to conjunctions of constraints of the forms shown in the previous table, the set-theoretic satisfiability problem is algorithmically unsolvable.

Remark (One may prefer to avoid Cartesian product)

If one, while building a flat Δ in arithmetic, uses squaring instead of product, then the conjuncts of $\hat{\Delta}$ which involve $\times$ can be superseded by literals of the form $|\cdot| = |\cdot|^2$, via the translation

$$x = y^2 \quad \Rightarrow \quad |x| = |y|^2 \ .$$

Remark (Cartesian product can be weakened)

The role of $\times$ can be superseded, in the reduction of **H10** to sets, by the following weaker operation:

$$y \otimes z \quad =_{\mathsf{Def}} \quad \left\{ \{u, v\} : u \in y,\ v \in z \right\} .$$

Remark (One negative constraint suffices)

Altogether, at most one constraint of any of the three forms

$$o = \{\cdot\}, \quad o \neq \varnothing, \quad |o| \neq |\zeta|$$

is needed to ensure the set-theoretic analogue of DPRM.

Remark (One negative constraint suffices)

Altogether, at most one constraint of any of the three forms

$$o = \{\cdot\}, \quad o \neq \varnothing, \quad |o| \neq |\zeta|$$

is needed to ensure the set-theoretic analogue of DPRM.

Instead of any of those, one could exploit $\in$. E.g.:

$$o = \{\zeta\} \rightsquigarrow \zeta \in o \ \& \ |o| = |o|^2$$

Finitude vs negative constraints

Remark (One finiteness constraint suffices)

$$\bigwedge_{i=1}^{\ell} \mathsf{Finite}\,(v_i) \rightsquigarrow \mathsf{Finite}\,(\phi) \;\&\; \bigwedge_{i=1}^{\ell} \phi \supseteq v_i$$

Finitude vs negative constraints

Remark (One finiteness constraint suffices)

$$\bigwedge_{i=1}^{\ell} \mathsf{Finite}\,(v_i) \rightsquigarrow \mathsf{Finite}\,(\phi) \;\&\; \bigwedge_{i=1}^{\ell} \big(\, \phi \supseteq v_i \;=\; v_i \cup v_i' \,\big)$$

W.l.o.g., we may require that this finite 'container' ϕ be at least

DOUBLETON:

$$\mathsf{Finite}\,(\phi) \rightsquigarrow \phi = \phi_1 \cup \phi_2 \;\&\; |\phi| \neq |\phi_2| \;\&\; |\phi| \neq |\phi_1|$$

REMARK (ONE FINITENESS CONSTRAINT SUFFICES)

$$\bigwedge_{i=1}^{\ell} \mathrm{Finite}\,(v_i) \rightsquigarrow \mathrm{Finite}\,(\phi) \;\&\; \bigwedge_{i=1}^{\ell} \phi \supseteq v_i$$

W.l.o.g., we may require that this finite 'container' ϕ be at least

SINGLETON:

$$\mathrm{Finite}\,(\phi) \rightsquigarrow \phi = \phi_1 \cup \phi_2 \;\&\; \phi_2 = \{\cdot\} \;\&\; |\phi| \neq |\phi_1|$$

DOUBLETON:

$$\mathrm{Finite}\,(\phi) \rightsquigarrow \phi = \phi_1 \cup \phi_2 \;\&\; |\phi| \neq |\phi_2| \;\&\; |\phi| \neq |\phi_1|$$

Hence one can do without finiteness constraints

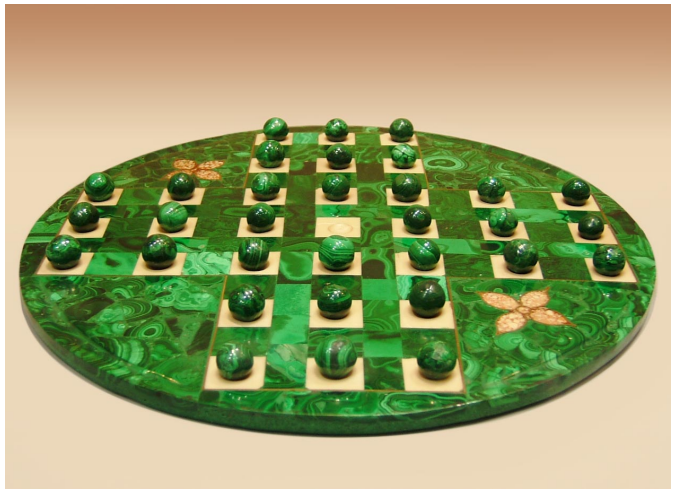
in the $\Delta \Rrightarrow \hat{\Delta}$ translation,

and still resort to at most two or three negative constraints.

How far away
from decidability
does $\widehat{\Delta}$ lie ?

One can algorithmically test for satisfiability over sets any conjunction of literals of the following forms [FOS80]:

$$x = y \setminus z\,, \quad x = y \cap z\,, \quad x = y \cup z\,,$$
$$x \neq y\,, \quad x \subseteq y\,, \quad x \not\subseteq y\,,$$
$$x = \varnothing\,, \quad x = \{y\}\,,$$
$$x \in y\,, \quad x \notin y$$



By combining MLSS with the unquantified sublanguage of Presburger's additive arithmetic [Pre30], one *does not disrupt* decidability. In its most essential form, the problem at hand is the one of satisfying conjunctions of equations of the forms

$$\begin{array}{rcl|rcl} \varnothing & = & y \cap z & h & = & |x| \\ x & = & y \cup z & h & = & i + j \\ x & = & \{y\} & h & = & 1 \end{array}$$

over *hereditarily finite sets* and *natural numbers*.

By combining MLSS with the unquantified sublanguage of Presburger's additive arithmetic [Pre30], one *does not disrupt* decidability. In its most essential form, the problem at hand is the one of satisfying conjunctions of equations of the forms

$$\begin{array}{lcl|lcl} \varnothing & = & y \cap z & h & = & |x| \\ x & = & y \cup z & h & = & i + j \\ x & = & \{y\} & h & = & 1 \end{array}$$

over *hereditarily finite sets* and *natural numbers*.

Hence:

> 'Main' culprit of undecidability, in what precedes, is:
> Cartesian $\times$ / Cartesian squaring / card. squaring
> when paired with equinumerosity

By dropping from the the language of $\hat{\Delta}$ the "equinumerosity" and the "finitude" constraints, one obtains the language MLSS×:

$\cdot = \cdot \cup \cdot$	union	(dyadic operation)
$\cdot = \cdot \times \cdot$	Cartesian product	(dyadic operation)
$\cdot \cap \cdot = \varnothing$	disointness	(dyadic relation)
$\cdot = \{\cdot\}$	singleton formation	(monadic operation)
$\cdot \neq \varnothing$	non-emptyness	(property)

By dropping from the the language of $\hat{\Delta}$ the "equinumerosity" and the "finitude" constraints, one obtains the language MLSS×:

$\cdot = \cdot \cup \cdot$	union	(dyadic operation)
$\cdot = \cdot \times \cdot$	Cartesian product	(dyadic operation)
$\cdot \cap \cdot = \varnothing$	disointness	(dyadic relation)
$\cdot = \{\cdot\}$	singleton formation	(monadic operation)
$\cdot \neq \varnothing$	non-emptyness	(property)

(By replacing the operator × in MLSS× by the weakened operator ⊗, one obtains the language MLSS⊗.)

By dropping from the the language of $\hat{\Delta}$ the "equinumerosity" and the "finitude" constraints, one obtains the language MLSS$\times$:

$\cdot = \cdot \cup \cdot$	union	(dyadic operation)
$\cdot = \cdot \times \cdot$	Cartesian product	(dyadic operation)
$\cdot \cap \cdot = \varnothing$	disointness	(dyadic relation)
$\cdot = \{\cdot\}$	singleton formation	(monadic operation)
$\cdot \neq \varnothing$	non-emptyness	(property)

(By replacing the operator $\times$ in MLSS$\times$ by the weakened operator $\otimes$, one obtains the language MLSS$\otimes$.)

Using the formative processes approach (cf. [CU18]),
Cantone & Ursino are currently well under way in proving that the set-theoretic satisfiability problem for MLSS$\otimes$ is solvable.
It is expected that the satisfiability problem for MLSS$\times$ will turn out to be solvable as well, much by the same approach.

$(\forall\exists)_0$-recasting of our undecidable fragments of ZF

Henceforth, we *expunge* from primitive constructs all constants (such as $\varnothing$ and $\mathbb{N}$) and all function symbols (such as $\cup$, $\cap$, $\otimes$, $|\cdot|$). *Only $\in$ and $=$ are retained as primitive relators*. All other needed constructs must be specified as handy shortening devices.

Henceforth, we *expunge* from primitive constructs all constants (such as $\varnothing$ and $\mathbb{N}$) and all function symbols (such as $\cup$, $\cap$, $\otimes$, $|\cdot|$). *Only $\in$ and $=$ are retained as primitive relators*. All other needed constructs must be specified as handy shortening devices.

UNIVERSAL AND EXISTENTIAL *bounded quantifiers*

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

Definition

We dub $(\forall\exists)_0$-***formula*** any conjunction Φ 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 φ_j is devoid of quantifiers and either $p_j > 0$, $q_j \geqslant 0$ or $p_j = q_j = 0$ holds.

DEFINITION

We dub $(\forall\exists)_0$ ***specification*** of an m-place relationship R over sets a $(\forall\exists)_0$ formula Φ such that, under the axioms of set theory (to wit, ZF with regularity and global choice), one can prove:

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

EXAMPLE

The right-hand sides of

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

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

Can $(\forall\exists)_0$ specs *compete* with the definition mechanisms of a full-fledged set theory ?

$$
\begin{array}{rcl}
\mathcal{P}(S) & =_{\mathsf{Def}} & \{\, y : y \subseteq S \,\} \\
\bigcup S & =_{\mathsf{Def}} & \{\, y : x \in S\,,\ y \in x \,\} \\
\mathsf{Finite}\,(F) & \leftrightarrow_{\mathsf{Def}} & \Big(\forall\, g \in \mathcal{P}(\mathcal{P}(F)) \setminus \{\varnothing\} \;\Big|\; \big(\exists\, m \mid g \cap \mathcal{P}(m) = \{m\}\big)\Big) \\
\mathsf{HerFin}\,(F) & \leftrightarrow_{\mathsf{Def}} & \mathsf{Finite}\,(F) \;\;\&\;\; \Big(\forall\, x \in F \;\Big|\; \mathsf{HerFin}\,(x)\Big) \\
I^{+} & =_{\mathsf{Def}} & I \cup \{\, I \,\} \\
\mathsf{nat}(I, S) & =_{\mathsf{Def}} & \mathbf{arb}\Big(\big\{\, \mathsf{nat}^{+}(\mathsf{j}, \mathsf{S}) : \mathsf{j} \in \mathsf{I} \;\big|\; \mathsf{I} = \{\mathsf{j}\} \cap \mathsf{S} \,\big\}\Big) \\
\mathbb{N} & =_{\mathsf{Def}} & \{\, \mathsf{nat}(i, \mathbf{s}_{\infty}) : i \in \mathbf{s}_{\infty} \,\} \\
\mathsf{Trans}(T) & \leftrightarrow_{\mathsf{Def}} & T \supseteq \bigcup T \\
\mathsf{Ord}(O) & \leftrightarrow_{\mathsf{Def}} & \mathsf{Trans}(O) \;\&\; \Big(\forall\, x \in O\,,\ y \in O \setminus \{x\} \;\Big|\; x \in y \;\vee\; y \in x\Big) \\
\mathsf{rank}\,(x) & =_{\mathsf{Def}} & \bigcup \big\{\, \mathsf{rank}^{+}(y) : y \in x \,\big\}
\end{array}
$$

Figure:
ÆtnaNova definitions can rely on: set abstraction terms, $\in$-recursion, a global choice operator **arb** , a constant $\mathbf{s}_{\infty}$ designating an infinite set

Plain $(\forall\exists)_0$ specs

Specifying basic properties or relations in the $(\forall\exists)_0$ format tends to be *unwildy* or even *undoable*, but some straightforward cases exist:

$$T \cap S = \varnothing \quad \leftrightarrow \quad (\,\forall x \in T\,)\; x \notin S$$

$$T \supseteq \bigcup S \quad \leftrightarrow \quad (\,\forall x \in S\,)(\forall y \in x)\; y \in T$$

$$T \subseteq \bigcup S \quad \leftrightarrow \quad (\,\forall x \in T\,)(\exists y \in S)\; x \in y$$

$$\mathsf{Map}_w(M) \quad \leftrightarrow \quad (\,\forall p \in M\,)(\forall x_1, x_2, x_3 \in p)(\,x_1 = x_2 \vee x_2 = x_3 \vee x_1 = x_3\,)$$

$$\mathsf{Ord}(O) \quad \leftrightarrow \quad O \supseteq \bigcup O \;\;\&\;\; (\,\forall x \in O\,)(\,\forall y \in O\,)(\,x \in y \;\vee\; y \in x \;\vee\; x = y\,)$$

$$\mathsf{LimOrd}(L) \quad \leftrightarrow \quad (\,\exists a\,)\Big(\, a \in L \;\&\; \mathsf{Ord}(L) \;\&\; L \subseteq \bigcup L \,\Big)$$

Can we likewise specify that $\mathbb{N}$ is *the least* limit ordinal ?

Slightly clumsier $(\forall\exists)_0$ specs

$$\begin{aligned}\text{1-1}_w(D, F, R) \leftrightarrow\ & \mathrm{Map}_w(F) \ \&\ D \subseteq \bigcup F \ \&\ R \subseteq \bigcup F \ \&\ \boxed{D \cap R = \varnothing} \ \& \\ & (\forall p, q \in F)(\forall w \in p)(w \in q \rightarrow p = q) \ \& \\ & (\forall p \in F)(\exists u \in D)(\exists v \in R)(u \in p \ \&\ v \in p)\end{aligned}$$

$$|x| = |y| \leftrightarrow (\exists z, f, g)\big(\text{1-1}_w(z, f, x) \ \&\ \text{1-1}_w(z, g, y)\big)$$

$$\begin{aligned}|x| = |y|^2 \leftrightarrow (\exists x', y', f, g)\big(&\text{1-1}_w(x', f, x) \ \&\ \text{1-1}_w(y', g, y) \\ &\&\ x' = y \otimes y'\big)\end{aligned}$$

Here (since $y' \cap y = \varnothing$), the constraint $x' = y \otimes y'$ is rewritable as:

$$\begin{aligned}&\mathrm{Map}_w(x') \ \& \\ &(\forall p \in x')(\exists u \in y)(\exists v \in y')(u \in p \ \&\ v \in p) \ \& \\ &(\forall u \in y)(\forall v \in y')(\exists p \in x')(u \in p \ \&\ v \in p) \ .\end{aligned}$$

Two stressful $(\forall\exists)_0$ specs

$$\mathcal{Z} = \mathbb{N} \quad \leftrightarrow \quad (\,\exists\, a\,,\ s\,)\,\big(\ (1)\ \&\ \cdots\ \&\ (5)\ \big)$$

(1) $\quad a \in \mathcal{Z} \quad \& \quad \mathrm{Ord}(\mathcal{Z}) \quad \& \quad \mathrm{Map}_w(s)$,

(2) $\quad (\forall p \in s)(\exists x, y \in p)\big(\ \ x \in y \,\&\, y \in \mathcal{Z}\ \ \big)$,

(3) $\quad (\forall p, q \in s)(\forall x, y \in p)(\forall y' \in q)\big((x \in y \,\&\, x \in y' \,\&\, x \in q) \ \rightarrow\ p = q\big)$,

(4) $\quad (\forall x \in \mathcal{Z})(\exists p \in s)(\exists y \in p)\big(\ \ x \in p \quad \& \quad x \in y\ \ \big)$,

(5) $\quad (\forall y \in \mathcal{Z})(\forall e \in y)(\exists p \in s)(\exists x \in p)\big(\ \ y \in p \quad \& \quad x \in y\ \ \big)$.

Two stressful $(\forall\exists)_0$ specs

$$\boxed{\mathcal{Z} = \mathbb{N} \quad \leftrightarrow \quad (\exists\, a,\, s)\big(\,(1)\,\&\,\cdots\,\&\,(5)\,\big)}$$

(1) $\quad a \in \mathcal{Z} \quad \& \quad \mathrm{Ord}(\mathcal{Z}) \quad \& \quad \mathrm{Map}_w(s)$,

(2) $\quad (\forall p \in s)(\exists x, y \in p)\big(\quad x \in y \,\&\, y \in \mathcal{Z} \quad\big)$,

(3) $\quad (\forall p, q \in s)(\forall x, y \in p)(\forall y' \in q)\big((x \in y \,\&\, x \in y' \,\&\, x \in q) \;\rightarrow\; p = q\big)$,

(4) $\quad (\forall x \in \mathcal{Z})(\exists p \in s)(\exists y \in p)\big(\quad x \in p \quad \& \quad x \in y \quad\big)$,

(5) $\quad (\forall y \in \mathcal{Z})(\forall e \in y)(\exists p \in s)(\exists x \in p)\big(\quad y \in p \quad \& \quad x \in y \quad\big)$.

$$\boxed{\mathcal{Z} = \mathbb{N} \;\&\; \mathrm{HerFin}(F) \;\leftrightarrow\; (\exists\, a,\, s, t,\, h)\big((1)\,\&\,\cdots\,\&\,(5)\,\&\,(1')\,\&\,\cdots\,\&\,(5')\big)}$$

(1′) $\quad F \in t \quad \& \quad \mathcal{Z} \notin t \quad \& \quad t \supseteq \bigcup t \quad \& \quad \mathrm{Map}_w(h)$,

(2′) $\quad (\forall p \in h)(\exists\, w, m \in p)(\exists x \in t)\big(\quad x \in w \quad \& \quad \mathcal{Z} \in w \quad \& \quad m \in a \quad\big)$,

(3′) $\quad (\forall p \in h)(\forall w \in p)(\forall x_1, x_2 \in w)\big(\mathcal{Z} \in w \rightarrow x_1 = x_2 \vee x_2 = \mathcal{Z} \vee x_1 = \mathcal{Z}\big)$,

(4′) $\quad (\forall p,\, q \in h)(\forall v \in p)\big(\quad v \in q \quad \rightarrow \quad p = q \quad\big)$,

(5′) $\quad (\forall x \in t)(\exists p \in h)(\exists w \in p)\big(\quad x \in w \quad \& \quad \mathcal{Z} \in w \quad\big)$.

Corollary of CCP (Cantone–Cutello-Policriti, 1990)

When referred to $(\forall\exists)_0$ formulae, the set-theoretic satisfiability problem is algorithmically unsolvable.

Validation by means of a proof assistant of the proposed $(\forall\exists)_0$ specs

Formal experiments with ÆtnaNova

In late 2019, the equivalence between the 'official' definitions of

$$\text{equinumerosity}, \quad \mathbb{N}, \quad \text{finitude},$$

and the corresponding $(\forall\exists)_0$ specs has been formally proved, and checked by means of the ÆtnaNova proof assistant (see [SCO11]).

ÆtnaNova takes in input bodies of text, called *scenarios*, and checks whether they constitute a valid sequence of definitions and theorems. Proofs are sequences of statements of the form:

$$\langle \text{HINT} \rangle \implies \langle \text{ASSERTION} \rangle$$

Where the assertion is a first-order formula and the hint is one of several inferential mechanism used to derive the former. Examples

ÆtnaNova takes in input bodies of text, called *scenarios*, and checks whether they constitute a valid sequence of definitions and theorems. Proofs are sequences of statements of the form:

$$\langle \text{HINT} \rangle \implies \langle \text{ASSERTION} \rangle$$

Where the assertion is a first-order formula and the hint is one of several inferential mechanism used to derive the former. Examples of hints are:

- ELEM — Elementary set theoretic reasoning.
- Suppose_not — Starts a proof by contradiction.
- Suppose — Opens a context in which the assertion is supposed. Closed by Discharge statement.
- $(e_1, \ldots, e_n) \hookrightarrow \mathit{Stat}$ — Replaces bound variables in the statement Stat by terms $e_1, \ldots, e_n$.
- Loc_def — Defines a symbol in the local context.

Under assumption that

$$\text{1-1}_w(D, F, R)$$

holds, the following basic results, along with some more technical ones, have been proved and verified.

$$\begin{aligned}
& & & \text{1-1}_w(R, F, D) \\
D = \emptyset \ \vee \ R = \emptyset & & \rightarrow & \quad F = D = R = \emptyset \\
\{a, b\} \in F \ \& \ a \in D \ \& \ b \in R & & \rightarrow & \quad \text{1-1}_w\big(D \setminus \{a\},\ F \setminus \big\{\{a, b\}\big\},\ R \setminus \{b\}\big) \\
x \in D & & \rightarrow & \quad \Big(\exists y \in R \mid \{x, y\} \in F\Big) \\
y \in R & & \rightarrow & \quad \Big(\exists x \in D \mid \{x, y\} \in F\Big)
\end{aligned}$$

* all (seemingly) free variables are universally quantified

In sight of showing the rightness of a specification of equinumerosity, we had to prove three more claims (henceforth referred to as `TrestrQuant14a`, `TrestrQuant13`, and `TrestrQuant14b`):

$$\text{1-1}_w\big(X,\ \big\{\big\{a,\{a,X\cup Y\}\big\} : a\in X\big\},\ X\otimes\{X\cup Y\}\big)$$

$\text{1-1}_w(D,G,R)\ \&\ F=\{[u,v] : p\in G, u\in p\cap D, v\in p\cap R\}$ implies:
F is an injection from D onto R.

F is an injection from D onto R implies:
$$\text{1-1}_w\big(D,\big\{\big\{x,\{F\,x,R\cup D\}\big\} : x\in D\big\},R\otimes\{R\cup D\}\big)$$

In the ongoing, we will see that these three claims yield a convenient $(\forall\exists)_0$ specification of equinumerosity between sets.

The theorem claims that the following conditions imply each other:

1. $(\exists f \mid \text{1-1}(f) \ \& \ \text{domain}(f) = D \ \& \ \text{range}(f) = R)$
2. $(\exists z, g, h \mid \text{1-1}_w(D, g, z) \ \& \ \text{1-1}_w(R, h, z))$

All proofs, in ÆtnaNova, are carried out by contradiction; hence our first statement is:

$$\text{Suppose\_not}(d_0, r_0) \implies \text{AUTO}$$

which negates the claim statement on $D = d_0$ and $R = r_0$.

We proceed by deriving (2) from (1) through the construction of two unordered one-one maps g_0 and h_0 that map d_0 and r_0 to the same set z_0.

Suppose $\Longrightarrow$ Stat1: $(\exists f \mid \text{1-1}(f) \ \& \ \text{domain}(f) = d_0 \ \& \ \text{range}(f) = r_0)$ &
Stat2: $(\nexists z, g, h \mid \text{1-1}_w(d_0, g, z) \ \& \ \text{1-1}_w(r_0, h, z))$

$f_0 \hookrightarrow$ Stat1 $\Longrightarrow$ $\text{1-1}(f_0)$ & $\text{domain}(f_0) = d_0$ & $\text{range}(f_0) = r_0$

Loc_def $\Longrightarrow$ $z_0 = r_0 \otimes \{r_0 \cup d_0\}$

Loc_def $\Longrightarrow$ $g_0 = \{\{x, \{f_0\, x, r_0 \cup d_0\}\} : x \in d_0\}$

Loc_def $\Longrightarrow$ $h_0 = \{\{y, \{y, r_0 \cup d_0\}\} : y \in r_0\}$

$(r_0, d_0) \hookrightarrow$ `TrestrQuant14a` $\Longrightarrow$ **AUTO**

$(f_0, d_0, r_0) \hookrightarrow$ `TrestrQuant14b` $\Longrightarrow$ **AUTO**

EQUAL $\Longrightarrow$ $\text{1-1}_w(r_0, h_0, z_0) \ \& \ \text{1-1}_w(d_0, g_0, z_0)$

$(z_0, g_0, h_0) \hookrightarrow$ Stat2 $\Longrightarrow$ **false**

Discharge $\Longrightarrow$ Stat3: $(\exists z, g, h \mid \text{1-1}_w(d_0, g, z) \ \& \ \text{1-1}_w(r_0, h, z))$ &
Stat4: $(\nexists f \mid \text{1-1}(f) \ \& \ \text{domain}(f) = d_0 \ \& \ \text{range}(f) = r_0)$

Next we must prove the implication (2) $\rightarrow$ (1) (Stat3 amounts to its negation); by instantiation of the existential variables, we get:

$$(z_1, g_1, g_2) \hookrightarrow \text{Stat3} \implies 1\text{-}1_w(d_0, g_1, z_1) \ \& \ 1\text{-}1_w(r_0, g_2, z_1)$$

Since domain and range of unordered bijections commute (`TunrdOneOne_2`), we get:

$$(r_0, g_2, z_1) \hookrightarrow \texttt{TunrdOneOne\_2} \implies 1\text{-}1_w(z_1, g_2, r_0)$$

We now put:

$$\mathit{Loc\_def} \implies f_1 = \left\{[u, v] : p \in g_1, u \in p \cap d_0, v \in p \cap z_1\right\} \ \& \\ f_2 = \left\{[u, v] : p \in g_2, u \in p \cap z_1, v \in p \cap r_0\right\}$$

By one of the lemmas—recalled above—on weak bijections between disjoint sets, we have:

$$(d_0, g_1, z_1, f_1) \hookrightarrow \texttt{TrestrQuant13} \implies \text{1-1}(f_1)\ \&\ \text{domain}(f_1) = d_0\ \&\ \text{range}(f_1) = z_1$$

$$(z_1, g_2, r_0, f_2) \hookrightarrow \texttt{TrestrQuant13} \implies \text{1-1}(f_2)\ \&\ \text{domain}(f_2) = z_1\ \&\ \text{range}(f_2) = r_0$$

Since the map product of two bijections is a bijection (`Tcomposition_3`) with the domain of the second and range of the first (`Tcomposition_5a`), we readily get the sought contradiction:

$$(f_2, f_1) \hookrightarrow \texttt{Tcomposition\_3} \implies \text{1-1}(f_2 \circ f_1)$$

$$(f_1, f_2) \hookrightarrow \texttt{Tcomposition\_5a} \implies \text{domain}(f_2 \circ f_1) = d_0\ \&\ \text{range}(f_2 \circ f_1) = r_0$$

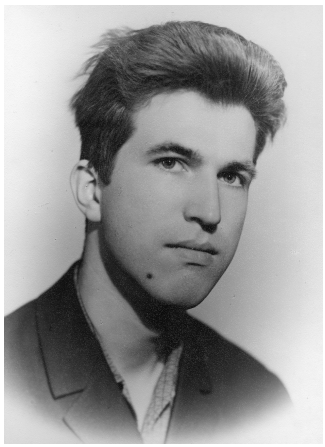
$$(f_2 \circ f_1) \hookrightarrow \text{Stat4} \implies \textbf{false}$$

$$\text{Discharge} \implies \textbf{QED}$$

Are there any deeper links between set theory and Diophantine arithmetic ?

“[· · ·] *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. ” [DMR76]



Can we do more along the directions envisioned by [DMR76]? 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 DPR and of DPRM *directly inside* set theory (possibly making the techniques more transparent).

Can we do more along the directions envisioned by [DMR76]? 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 DPR and of DPRM *directly inside* set theory (possibly making the techniques more transparent).

Bibliographic references

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.

Domenico Cantone and Pietro Ursino.

An Introduction to the Technique of Formative Processes in Set Theory.

Springer International Publishing, 2018.

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 [Rob96, p. 269ff.].

A. Ferro, E. G. Omodeo, and J. T. Schwartz.

Decision procedures for elementary sublanguages of set theory. I: Multi-level syllogistic and some extensions.

Comm. Pure Appl. Math., XXXIII:599–608, 1980.


Yuri Vladimirovich Matiyasevich.
Hilbert's tenth problem.
The MIT Press, Cambridge (MA) and London, 1993.


Mojżesz Presburger.
Über die Völlständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt.
Comptes-rendus du premier Congrès des mathematiciens des Pays Slaves, Warsaw:92–101,395, 1930.


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.


Jacob T. Schwartz, Domenico Cantone, and Eugenio G. Omodeo.
Computational Logic and Set Theory - Applying Formalized Logic to Analysis.
Springer, London, 2011.
Foreword by Martin Davis.

Replaceability of singleton by membership

In light of Kuratowski's definition of the ordered pair, the members of the Cartesian product $y \times z$ are precisely the sets of the form

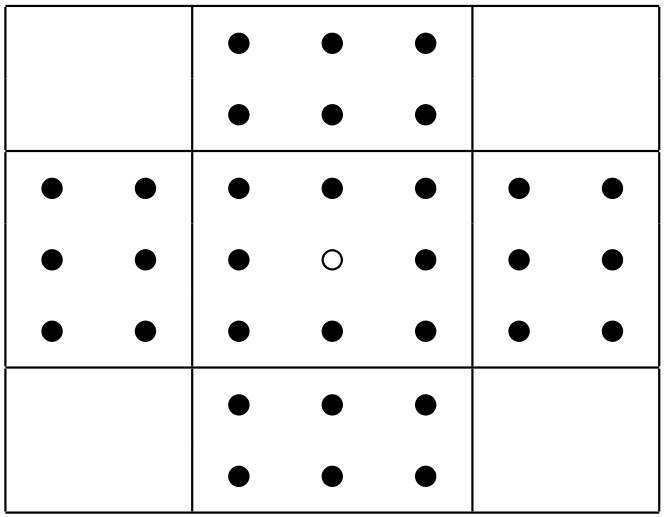
$$\big\{\{t\},\{t,t'\}\big\}\,, \quad \text{with} \quad t \in y \quad \text{and} \quad t' \in z \quad .$$

Hence—as we postulate that $\in$ does not form cycles—the equivalences

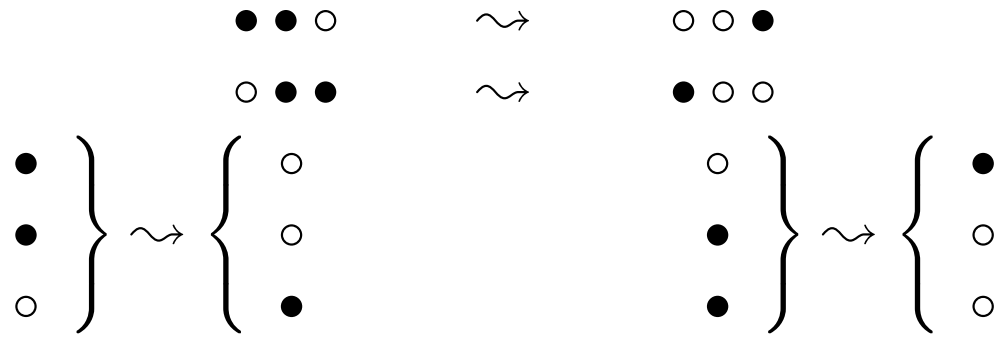
$$s = \{\,t\,\} \iff \exists\, d\, \exists\, p \Big(t \in s \in d \in p \in d \times d \;\&\; t \in d \;\&\; s \in p \Big)\,,$$
$$s = \{\,t\,\} \iff \exists\, d \quad \Big(t \in s \in d \quad \in d \otimes d \;\&\; t \in d \;\&\; s \in d \otimes d \Big)$$

hold: they enable us to replace every equation of the form $s = \{\,t\,\}$ appearing in $\widehat{\Delta}$ by a constraint conjoining either:

- one eq'n of the form $w = d \times d$ with 6 membership literals; or
- one eq'n of the form $w = d \otimes d$ with 5 membership literals.



Moves :



		1	2	3		
		4	5	6		
7	8	9	10	11	12	13
14	15	16	**33**	17	18	19
20	21	22	23	24	25	26
		27	28	29		
		30	31	32		

FIGURE: The *Solo Noble* gameboard and a numbering of its holes

Below is an MLS description of the moves y_{i1}, y_{i2}, y_{i3} ($i = 1, \ldots, 31$) by which one can solve the classic puzzle portrayed above:

$$x_1 = \{ n_1, \ldots, n_{32} \} \;\&\; x_{32} = \{ n_? \}$$

$$\& \bigwedge_{m=1}^{32} \Big(x_{m+1} = x_m \setminus \{ y_{m1}, y_{m2} \} \cup \{ y_{m3} \} \;\&\; y_{m3} \notin x_m \;\&\; \{ y_{m1}, \{ y_{m2} \}, y_{m3} \} \in z \;\&\; n_{m+1} = n_m \cup \{ n_m \} \Big)$$

$$\& \; z = \big\{ \{ n_1, \{ n_2 \}, n_3 \}, \ldots, \{ n_{16}, \{ n_{33} \}, n_{17} \}, \ldots, \{ n_{30}, \{ n_{31} \}, n_{32} \}, \{ n_1, \{ n_4 \}, n_9 \}, \ldots, \{ n_{10}, \{ n_{33} \}, n_{23} \}, \ldots, \{ n_{24}, \{ n_{29} \}, n_{32} \} \big\}$$

$$\& \; n_1 = \{ \varnothing \}.$$

Here the x_m's represent the successive configurations of the gameboard, the n_m's represent consecutive natural numbers, and z encodes the set of triples of adjacent holes on the board, from which each move must be selected. The condition $x_{32} = \{ n_? \}$ expresses the goal of ending with exactly one hole occupied.