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

HILBERT'S $10^{\underline{th}}$ PROBLEM (1900)

Given: a Diophantine eq.

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

Algorithmic decider

$\mathfrak{H}$

$\hookrightarrow$ **yes** / **no**

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

Given: a Diophantine eq.

$D(x_1, \ldots, x_m) = 0$ $\hookrightarrow$ Algorithmic decider $\mathfrak{H}$ $\hookrightarrow$ **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.

$D(x_1, \ldots, x_m) = 0 \hookrightarrow$ Algorithmic decider $\mathfrak{H}$ $\hookrightarrow$ **yes** / **no**

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 $\boxed{\text{integer}}$ (positive, negative, or null).

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 $\boxed{\text{refer } \textbf{H10} \text{ to } \mathbb{N}}$

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

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

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

Consider a polynomial Diophantine equation

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

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

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

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.

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'):

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

§Cf. [Mat93, p. 4]

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'):

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

[§] 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:

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:

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

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

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:

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

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

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.

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.
Foreword by Martin Davis. Springer, London, 2011.