Can a single equation witness that every r.e. set admits a finite-fold Diophantine representation?*

Domenico Cantone[1] and Eugenio G. Omodeo[2]

[1] Dept. of Mathematics and Computer Science, University of Catania, Italy.
domenico.cantone@unict.it
[2] Dept. of Mathematics and Geosciences, University of Trieste, Italy.
eomodeo@units.it

Abstract. As of today, the question remains open as to whether the quaternary quartic equation

$$9 \cdot \left(u^2 + 7\,v^2\right)^2 - 7 \cdot \left(r^2 + 7\,s^2\right)^2 = 2\,, \tag{*}$$

which M. Davis put forward in 1968, has only finitely many solutions in integers. If the answer were affirmative then—as noted by M. Davis, Yu. V. Matiyasevich, and J. Robinson in 1976—every r.e. set would turn out to admit a single-fold polynomial Diophantine representation.
New candidate 'rule-them-all' equations, constructed by the same recipe which led to (*), are proposed in this paper.

Key words. Hilbert's 10^{th} problem, exponential-growth relation, finite-fold Diophantine representation, Pell's equation.

Introduction

As was anticipated in [3] and then conclusively shown in 1961 [4], every recursively enumerable relation $\mathcal{R}(a_1, \ldots, a_n) \subseteq \mathbb{N}^n$ can be specified in the form

$$\mathcal{R}(a_1, \ldots, a_n) \Longleftrightarrow \exists\, x_1 \cdots \exists\, x_m\ \varphi(\overbrace{\underbrace{a_1, \ldots, a_n}_{\text{parameters}}\,,\,\underbrace{x_1, \ldots, x_m}_{\text{unknowns}}}^{\text{variables}})\,, \tag{†}$$

for some formula φ that only involves:

- the shown variables,
- positive integer constants,
- addition, multiplication, *exponentiation* (namely the predicate $x^y = z$),
- the logical connectives $\&$, $\vee$, $\exists\, x$, $=$.

This result, known as the Davis-Putnam-Robinson (or 'DPR') theorem, was later improved by Yu. Matiyasevich in two respects: in [7] he showed how to ban

* The second author has been partially supported by INdAM-GNCS and by the project FRA-UniTS 2016.

use of exponentiation, altogether, from (†); in [8], while retaining exponentiation, he achieved *single-fold*-ness of the representation, in the sense explained below.[1]

A representation

$$\exists \vec{x}\ \varphi(\vec{a}, \vec{x})$$

of $\mathcal{R}$ in the above form (†) is said to be ***single-fold*** if

$$\forall \vec{a}\ \forall \vec{x}\ \forall \vec{y} \left[\varphi(\vec{a}, \vec{x}) \ \&\ \varphi(\vec{a}, \vec{y}) \Longrightarrow \vec{x} = \vec{y} \right]$$

(i.e., the constraint $\varphi(a_1, \dots, a_n, x_1, \dots, x_m)$ never has multiple solutions). The definition of ***finite-fold***-ness is akin: The overall number of solutions (in the x's) that correspond to each n-tuple $\langle a_1, \dots, a_n \rangle$ of actual parameters must be finite.

In [6], Matiyasevich argues on the significance of combining his two improvements to DPR, and on the difficulty (as yet unsolved) of this reconciliation. Full elimination of exponentiation from (†) is generally achieved in two phases: one first gets the polynomial Diophantine representation of a relation of *exponential growth* (see [11]), and then integrates this representation with additional constraints in order to represent the predicate $x^y = z$ polynomially. Unfortunately, though, the solutions to the equations introduced in the first phase have a periodic behavior, causing the equations that specify exponentiation to have infinitely many solutions.

One way out of this difficulty was indicated in [2], and has been recently recalled in [6, 9]: If one managed to prove that there are only a finite number of solutions to a certain quaternary quartic equation, which M. Davis put forward in his "*One equation to rule them all*" [1], then a relation of exponential growth could be represented by a single-fold Diophantine polynomial equation.

Skepticism concerning the finitude of the set of solutions to Davis's equation began to circulate among number theorists after D. Shanks and S. S. Wagstaff [14] discovered some fifty elements of this set. This is why we sought—and will present in this paper—new candidates to the role of 'rule-them-all' equation, by resorting to much the same recipe which enabled Davis to obtain his own.

1 Four candidate rule-them-all equations

As of today, there are four competitors for the role of '*rule-them-all' equation*' over $\mathbb{N}$ (one was originally proposed in [1], the other three were detected by us):

-2: $$2 \cdot \left(r^2 + 2\,s^2\right)^2 - \left(u^2 + 2\,v^2\right)^2 = 1\,;$$

-3: $$3 \cdot \left(r^2 + 3\,s^2\right)^2 - \left(u^2 + 3\,v^2\right)^2 = 2\,;$$

-7: $$9 \cdot \left(u^2 + 7\,v^2\right)^2 - 7 \cdot \left(r^2 + 7\,s^2\right)^2 = 2\,;$$

[1] A virtue of the representation proposed in [8] is that the predicate $x^y = z$ occurs in it only once; Matiyasevich was in fact able to ensure singlefold-ness while reducing (†) to the elegant format

$$\mathcal{R}(a_1, \dots, a_n) \Longleftrightarrow \exists x_0\, \exists x_1 \cdots \exists x_m\ P(a_1, \dots, a_n,\ x_1, \dots, x_m) \ =\ 4^{x_0} + x_0\,,$$

where P is a polynomial with coefficients in $\mathbb{Z}$.

-11: $11 \cdot \left(r^2 \pm r\,s + 3\,s^2\right)^2 - \left(v^2 \pm v\,u + 3\,u^2\right)^2 = 2$
(four sign combinations).

Each one of these equations stems from a square-free rational integer $d > 1$ such that the integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ form a unique-factorization domain. The numbers in question are known to be 1, 2, 3, 7, 11, 19, 43, 67, 163, and no others. Consider, for each such d except $d = 1$, also the equation $d\,y^2 + 1 = \square$ (meaning: '$d\,y^2 + 1$ is a perfect square'). As is well known, this is a Pell equation endowed with infinitely many solutions in $\mathbb{N}$. The equations we have listed are associated—in the manner discussed below—with the discriminants $-2, -3, -7, -11$ of the corresponding Pell equations; in principle we could have associated a rule-them-all equation also with each one of $-19, -43, -67, -163$.

Trivial solutions: A solution in $\mathbb{N}$, for each of the four rule-them-all equations shown above, is: $r = u = 1\,,\ s = v = 0\,.$

The trivial solutions, in $\mathbb{Z}$, of $11 \cdot \left(r^2 + r\,s + 3\,s^2\right)^2 - \left(v^2 + v\,u + 3\,u^2\right)^2 = 2$ are: $s = 0$, $r \in \{-1, 1\}$ and either $v = 0$, $u \in \{-1, 1\}$ or $u = 1$, $v = -1$.

Non-trivial solutions (in $\mathbb{N}$): As mentioned in the Introduction, at least 50 solutions were found for the rule-them-all equation with discriminant -7.

Two non-trivial solutions for the discriminant -3 were detected, and kindly communicated to us, by Boris Z. Moroz (Rheinische Friedrich-Wilhelms-Universität Bonn) and Carsten Roschinski:[2]

$$r = 16\,,\quad s = 25\,,\quad u = 4\,,\quad v = 35\,;$$
$$r = 124088\,,\ s = 7307\,,\ u = 134788\,,\ v = 54097\,.$$

Presently we know no non-trivial solutions for the discriminants -2 and -11.

Relative to each one of our discriminants $-2, -3, -7, -11$, we have a notion of ***representable number***; to wit, a positive integer which can be written in the respective quadratic form (with $u, v \in \mathbb{Z}$):

-2: $u^2 + 2\,v^2\,,$
-3: $u^2 + 3\,v^2\,,$
-7: $u^2 + 7\,v^2\,,$
-11: $v^2 + v\,u + 3\,u^2\,.$

Let us also point out, for the respective discriminants, the ***poison primes***:

-2: prime numbers p such that $p \equiv 5, 7 \pmod{8}$;
-3: prime numbers p such that $p \equiv 2 \pmod{3}$;
-7: prime numbers p such that $p \equiv 3, 5, 6 \pmod{7}$;
-11: prime numbers p such that $p \equiv 2, 6, 7, 8, 10 \pmod{11}$.

Thus, it can be proved that the representable positive integers are precisely the ones in whose factorization no poison prime appears with an odd exponent.[3]

[2] Independently, also Alessandro Logar (Univ. of Trieste) found the same solutions.
[3] In the case of -7, this claim must be restrained to the *odd* representable positive integers.

2 Quick discussion referring to the discriminant -11

Since we cannot afford discussing at length each of the four candidate rule-them-all equations, we will offer a bird's-eye view of how to construct, directly from the *unproven assertion* that the quaternary quartic equation

$$11 \cdot \left(r^2 + r\,s\, + 3\,s^2\right)^2 - \left(v^2 + v\,u + 3\,u^2\right)^2 = 2 \tag{‡}$$

has only finitely many integer solutions, a finite-fold polynomial Diophantine representation of a relation of exponential growth.

Take into account the increasing sequence $\langle y_i \rangle_{i\in\mathbb{N}} = \langle 0, 3, 60, 1197, \ldots \rangle$ of all solutions to the Pell equation $11\,y^2 + 1 = \Box$. Also consider the relations:

$$\begin{aligned} OD(a,\, b) \;&\Leftrightarrow_{\text{Def}}\; \exists\, x\left[\,(2\,x+1)\,a = b\,\right], \\ \mathcal{J}(\,u\,,\,w\,) \;&\Leftrightarrow_{\text{Def}}\; w \in \{y_{2^{2\,\ell+1}} : \ell \geqslant 2\} \;\&\; OD(\,u\,,\,w\,)\,. \end{aligned}$$

It can easily be shown that $\mathcal{J}$ is of ***exponential growth*** in Julia Robinson's sense, namely that:

- $\mathcal{J}(u, v)$ implies $v < u^u$;
- for each ℓ, there are u and v such that $\mathcal{J}(u, v)$ & $u^\ell < v$.

Does the predicate $w \in \{y_{2^{2\,\ell+1}} : \ell \geqslant 2\}$—and, consequently, $\mathcal{J}$—admit a polynomial Diophantine representation? It turns out that the following are necessary and sufficient conditions in order for $w \in \{y_{2^{2\,\ell+1}} : \ell \geqslant 2\}$ to hold:

(i) $w > 3$;
(ii) $11\,w^2 + 1 = \Box$;
(iii) $\exists\, v\, \exists\, u\, \left(w = v^2 \pm v\,u + 3\,u^2\right)$;
(iv) $[(\boldsymbol{r}^2 + \boldsymbol{r}\,\boldsymbol{s} + 3\,\boldsymbol{s}^2) \cdot (\boldsymbol{v}^2 + \boldsymbol{v}\boldsymbol{u} + 3\,\boldsymbol{u}^2)] \nmid w$, for any non-trivial *integer* solution to $11 \cdot \left(r^2 + r\,s + 3\,s^2\right)^2 - \left(v^2 + v\,u + 3\,u^2\right)^2 = 2$.

This results in a Diophantine specification **if** *the number of solutions to the novel quaternary quartic* (‡) *is finite*! An issue that must be left open here.

Notice that the only potential source of multiple solutions to the above representation of $\mathcal{J}$ is condition (iii), which, anyhow, is finite-fold.

The issue as to whether (‡) has only finitely many solutions over $\mathbb{N}$ can be recast as the analogous problem concerning the system

$$\begin{cases} 11\,\xi^2 - \eta^2 = 2 \\ \qquad\quad \xi\,\eta = \nu^2 + \nu\,t + 3\,t^2 \end{cases}$$

over $\mathbb{Z}$.

The existence of finite-fold Diophantine representations for all r.e. sets thus reduces to the finitude of the set of integer points lying on a specific surface.

Acknowledgements

Discussions with Pietro Corvaja were very fruitful for the matters of this paper.

References

[1] M. Davis. One equation to rule them all. *Transactions of the New York Academy of Sciences. Series II*, 30(6):766–773, 1968.

[2] M. Davis, Yu. Matijasevič, and J. 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 [12, p. 269ff.].

[3] M. Davis and H. Putnam. A computational proof procedure; Axioms for number theory; Research on Hilbert's Tenth Problem. Technical Report AFOSR TR59-124, U.S. Air Force, October 1959. (Part III reprinted in [10, pp. 411-430]).

[4] M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential Diophantine equations. *Annals of Mathematics, Second Series*, 74(3):425–436, 1961.

[5] J. V. Matijasevič. Enumerable sets are Diophantine. *Soviet Mathematics. Doklady*, 11(3):354–358, 1970. (Translated from [7]).

[6] Yu. Matiyasevich. Towards finite-fold Diophantine representations. *Journal of Mathematical Sciences*, 171(6):745–752, Dec 2010.

[7] Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Doklady Akademii Nauk SSSR*, 191(2):279–282, 1970. (Russian. Available in English translation as [5]; translation reprinted in [13, pp. 269–273]).

[8] Yu. V. Matiyasevich. Sushchestvovanie neèffektiviziruemykh otsenok v teorii èkponentsial'no diofantovykh uravneniĭ. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, 40:77–93, 1974. (Russian. Translated into English as Yu. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential Diophantine equations, *Journal of Soviet Mathematics*, 8(3):299–311, 1977).

[9] Yu. V. Matiyasevich. Martin Davis and Hilbert's tenth problem. In Omodeo and Policriti [10], pages 35–54.

[10] E. G. Omodeo and A. Policriti, editors. *Martin Davis on Computability, Computational Logic, and Mathematical Foundations*, volume 10 of *Outstanding Contributions to Logic*. Springer, 2016.

[11] J. Robinson. Existential definability in arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. Reprinted in [12, p. 47ff.].

[12] J. 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.

[13] G. E. Sacks, editor. *Mathematical Logic in the 20th Century*. Singapore University Press, Singapore; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.

[14] D. Shanks and S. S. Wagstaff, Jr. 48 more solutions of Martin Davis's quaternary quartic equation. *Mathematics of Computation*, 64(212):1717–1731, 1995.

A Addendum referring to the discriminant -11

Here we provide clues on how to associate a quaternary quartic, candidate rule-them-all, equation with the number -11.

Along with the above-considered sequence $\langle y_i \rangle_{i\in\mathbb{N}}$ of all solutions to the Pell equation $11\,y^2+1=\square$, take also into account the associated sequence $\langle x_i \rangle_{i\in\mathbb{N}} = \langle 1, 10, 199, 3970, \dots \rangle$ with $x_i = \sqrt{11\,y_i^2+1}$. Then we have:

- for every $h>0$, y_{2^h} is representable in the form $v^2+v\,u+3\,u^2$ iff $2 \nmid h$, since $y_{2^h} = 2^{h+1}\cdot 15 \cdot \prod_{0<i<h} x_{2^i}$;
- if $y_{2^\ell\,(2\,h+1)}$ is representable (in that form), so are $\overbrace{3\,x_h+11\,y_h \text{ and } x_h+3\,y_h}^{coprime\ numbers}$;
- if y_n is representable for some $n>0$ *not* a power of 2, then the system

$$\begin{cases} X^2-11\,Y^2=1\,, \\ 3\,X+11\,Y \;= v^2+v\,u+3\,u^2\,, \\ X+\;3\,Y \;= r^2+r\,s+3\,s^2 \end{cases}$$

has an integer solution for which $Y \neq 0$; consequently, the equation

$$11\cdot\left(r^2+r\,s+3\,s^2\right)^2-\left(v^2+v\,u+3\,u^2\right)^2=2 \qquad (\ddagger)$$

has a non-trivial integer solution $\langle \bar{r}, \bar{s}, \bar{v}, \bar{u}\rangle$, a solution being dubbed *trivial* when it satisfies both of $r^2+r\,s+3\,s^2=1$ and $v^2+v\,u+3\,u^2=3$. Such a solution $\langle \bar{r}, \bar{s}, \bar{v}, \bar{u}\rangle$ will also satisfy $\left[\left(r^2+r\,s+3\,s^2\right)\cdot\left(v^2+v\,u+3\,u^2\right)\right] \mid y_n$.

Let $\mathcal{H}$ stand for the assertion (whose truth, as of today, must be left open):

|| *The equation (‡) has no solutions in integers except the trivial ones.*

Moreover, let $\mathcal{H}'$ stand for the weaker—and also open—assertion:

|| *The equation (‡) admits at most finitely many solutions in integers.*

Then the above-listed facts yield that:

Theorem 1. $\mathcal{H}$ implies that y_n is representable for $n>1$ if and only if n is an odd power of 2.

Corollary 1. $\mathcal{H}$ implies that $\{\, y_{2^{2\,\ell+1}} \,:\, \ell=0,1,2,\dots\}$ is a Diophantine set.

Lemma 1. $\mathcal{H}'$ implies that $\{\, y_{2^{2\,\ell+1}} \,:\, \ell=0,1,2,\dots\}$ is a Diophantine set.