LE MATEMATICHE
Vol. LXXVI (2021) – Issue I, pp. 133–160
doi: 10.4418/2021.76.1.8

THE QUEST FOR DIOPHANTINE FINITE-FOLD-NESS

D. CANTONE - A. CASAGRANDE - F. FABRIS - E. G. OMODEO

Dedicated to Martin Davis and Yuri Matiyasevich for their respective 90th and 70th birthdays, and to the memory of Julia Robinson, for her centennial.

The Davis-Putnam-Robinson theorem showed that every partially computable m-ary function $f(a_1,\ldots,a_m) = c$ on the natural numbers can be specified by means of an exponential Diophantine formula involving, along with parameters $a_1,\ldots,a_m,c$, some number κ of existentially quantified variables. Yuri Matiyasevich improved this theorem in two ways: on the one hand, he proved that the same goal can be achieved with no recourse to exponentiation and, thereby, he provided a negative answer to Hilbert's 10th problem; on the other hand, he showed how to construct an exponential Diophantine equation specifying f which, once $a_1,\ldots,a_m$ have been fixed, is solved by at most one tuple $\langle v_0,\ldots,v_\kappa\rangle$ of values for the remaining variables. This latter property is called single-foldness. Whether there exists a single- (or, at worst, finite-) fold polynomial Diophantine representation of any partially computable function on the natural numbers is as yet an open problem. This work surveys relevant results on this subject and tries to draw a route towards a hoped-for positive answer to the finite-fold-ness issue.

Received on February 25, 2020

AMS 2010 Subject Classification: 03D25, 03D35

Keywords: Hilbert's 10^{th} problem, exponential-growth relation, finite-fold Diophantine representation, rule-them-all equation, Pell's equation.

Acknowledgments: We gratefully acknowledge partial support from project "STORAGE—Università degli Studi di Catania, Piano della Ricerca 2020/2022, Linea di intervento 2", from GNCS-INdAM 2020 research funds, from project FRA-UniTS 2020, and from "Università degli Studi di Trieste, Dipartimenti di Eccellenza, DMG".

1. Introduction

The celebrated Davis-Putnam-Robinson theorem of 1961 ensures that every computable function $\mathcal{F}$ from a subset of $\mathbb{N}^m$ into $\mathbb{N} = \{0,1,2,\dots\}$ can be specified as

$$\mathcal{F}(a_1,\dots,a_m) = c \iff (\exists x_1 \cdots \exists x_\kappa)\ \varphi(\overbrace{\underbrace{a_1,\dots,a_m,c}_{\text{parameters}}, \underbrace{x_1,\dots,x_\kappa}_{\text{unknowns}}}^{\text{p.w. distinct variables}}), \qquad (\dagger)$$

for some formula φ that only involves:

- individual variables,[1] including (as free variables) the shown ones;
- non-negative integer constants;
- addition, multiplication, and exponentiation operators;[2]
- the logical connectives $\&$, $\vee$, $\exists\, v$, $=$.

Two major improvements to this result were achieved by Yuri Matiyasevich. In [13] he showed that (†) can be set up without exponentiation; in [15], while retaining exponentiation in it, he boiled φ down to the format

$$\begin{aligned}&\varphi(\,a_1,\dots,a_m,c\,,x_1,\dots,x_\kappa) \quad := \\ &\qquad P'\,(a_1,\dots,a_m,c,\,x_2\,,\dots,x_\kappa) = 4^{x_1} + x_1 + P''(a_1,\dots,a_m,c,\,x_2\,,\dots,x_\kappa),\end{aligned}$$

where $\boldsymbol{\kappa} > 0$ and P' and P'' are polynomials with coefficients in $\mathbb{N}$, devoid of occurrences of x_1, such that *no two* tuples

$$\langle \boldsymbol{a}_1,\dots,\boldsymbol{a}_m,\boldsymbol{v}_0,\boldsymbol{v}_1,\dots,\boldsymbol{v}_\kappa\rangle\,, \qquad \langle \boldsymbol{a}_1,\dots,\boldsymbol{a}_m,\boldsymbol{u}_0,\boldsymbol{u}_1,\dots,\boldsymbol{u}_\kappa\rangle$$

on $\mathbb{N}$ exist satisfying $\varphi(\,\boldsymbol{a}_1,\dots,\boldsymbol{a}_m\,,\,\boldsymbol{v}_0,\dots,\boldsymbol{v}_\kappa)\ \ \&\ \ \varphi(\,\boldsymbol{a}_1,\dots,\boldsymbol{a}_m\,,\,\boldsymbol{u}_0,\dots,\boldsymbol{u}_\kappa)$. Thus, every tuple $\langle \boldsymbol{a}_1,\dots,\boldsymbol{a}_m\rangle$ on $\mathbb{N}$ either admits no continuation $\langle \boldsymbol{v}_0,\dots,\boldsymbol{v}_\kappa\rangle$ satisfying φ—and then $\langle \boldsymbol{a}_1,\dots,\boldsymbol{a}_m\rangle$ does not belong to the domain of $\mathcal{F}$—or exactly one, and then $\boldsymbol{v}_0$ is precisely the value $\mathcal{F}(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m)$.

By introducing a little terminology—rather common in recursion theory, cf. [6]—we will be better-off in what follows. A set $\mathcal{R} \subseteq \mathbb{N}^m$, with $\boldsymbol{m} > 0$, is called

recursively enumerable (or, shortly, ***r.e.***)**:** when it is the domain of a partially computable function $\mathcal{F}$ taking $\boldsymbol{m}$ arguments (see, e.g., [9, Sect. 2.4]);

[1] NB: Throughout this paper, individual variables are supposed to range over $\mathbb{N}$.

[2] We name *exponentiation* the dyadic operation $\langle r, p\rangle \mapsto r^p$ (occasionally, also $p \mapsto 2^p$).

***exponential Diophantine*:** when it can be specified as

$$\mathcal{R}(a_1,\dots,a_m) \iff (\exists x_1 \cdots \exists x_\kappa)\ \varphi(\overbrace{\underbrace{a_1,\dots,a_m}_{\text{parameters}}, \underbrace{x_1,\dots,x_\kappa}_{\text{unknowns}}}^{\text{variables}}), \qquad (*)$$

for some formula φ involving the syntactic means listed at the beginning;

***Diophantine*:** when it can be specified in the form $(*)$, with φ involving the syntactic armory just recalled, *save* exponentiation.

Moreover, a representation of $\mathcal{R}$ in the form $(*)$ is said to be

single-fold or ***univocal*:** when each tuple $\langle \boldsymbol{a}_1,\dots,\boldsymbol{a}_m\rangle$ of natural numbers has at most one continuation $\langle \boldsymbol{v}_1,\dots,\boldsymbol{v}_\kappa\rangle$ such that $\varphi(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m,\boldsymbol{v}_1,\dots,\boldsymbol{v}_\kappa)$;

***finite-fold*:** when each tuple $\langle \boldsymbol{a}_1,\dots,\boldsymbol{a}_m\rangle$ of natural numbers has only finitely many continuations $\langle \boldsymbol{v}_1,\dots,\boldsymbol{v}_\kappa\rangle$ such that $\varphi(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m,\boldsymbol{v}_1,\dots,\boldsymbol{v}_\kappa)$ holds.

Let us sum up, in terms of these notions, the above-cited important results, along with two open issues raised many years ago, which still motivate us here:

DPR61 [8], known as DPR: Every r.e. set is exponential Diophantine (and conversely).

Mat70 [13], known as DPRM: Every r.e. set is Diophantine (and conversely).

Mat74 [15]: Every r.e. set admits a univocal exponential Diophantine representation.

DMR76 [7]: Does every r.e. set admit a univocal Diophantine representation?

Mat10 [17]: Does every r.e. set admit a finite-fold Diophantine representation?

A positive answer to DMR76 would combine together both of Matiyasevich's improvements to DPR, namely Mat70 and Mat74; in [17], Matiyasevich argues on the significance of this combination, and on the difficulty (as yet unsolved) of this reconciliation. In [18, p. 50], after discussing the issue again, he ends up by saying: "This relationship between undecidability and non-effectivizability is one of the main stimuli to improve the DPRM-theorem to single-fold (or at least to finite-fold) representations and thus establish the existence of non-effectivizable estimates for genuine Diophantine equations".

The derivation of DPRM from DPR required that exponentiation itself were proved to be Diophantine. A result by Julia Robinson, which we recapitulate in Sect. 3, played historically a key role in this arduous task: she had reduced the task to the quest for a Diophantine relation of *exponential growth* (a notion to be recalled soon here); and, indeed, Matiyasevich found a polynomial Diophantine representation of a specific exponential-growth relation.

After Matiyasevich [17], we have some hope that a positive answer to Mat10 can likewise be obtained by proving two facts:

- there exists a relation $\mathcal{D}(p,q)$, sharing with the relation $2^p = q$ (seen as the set $\{\langle p\,, 2^p\rangle \mid p \in \mathbb{N}\}$) a certain special property (see Fig. 1[3]), that admits a finite-fold Diophantine representation;

- consequently, via a reduction technique reminiscent of J. Robinson's one, exponentiation will have a finite-fold Diophantine representation. (Hence, via Mat74, every r.e. set will inherit the finite-fold Diophantine representability.)

Concerning the former goal, [1] and [2] propose four exponential-growth relations as candidate $\mathcal{D}$'s; moreover, [2] proves that one of them enjoys the "special property" shown in Fig. 1. It is hard to establish whether any of these candidates is Diophantine; clearly enough, though, if any of them is indeed Diophantine, then it has a finite-fold representation.

Concerning the latter goal, in order to convince ourselves (as well as our readers) that the sought "reduction technique reminiscent of J. Robinson's one" does exist, and to get closer to it, we undertake in this paper a comparison among various published versions of Robinson's technique, discussing how her idea evolved over the years from its original formulation of 1952 towards simpler implementations, one of which might fit our needs.

There exist integers $\alpha > 1\,,\ \beta \geqslant 0,\ \gamma \geqslant 0\,, \delta > 0$ such that to each $w \in \mathbb{N}$ other than 0 there correspond $p\,, q$ such that $\mathcal{D}(p,q)$, $p < \gamma w^{\beta}$, and $q > \delta\, \alpha^{w}$ hold.

Figure 1: A property (elicited in [17]) which, if enjoyed by a relation $\mathcal{D} \subseteq \mathbb{N} \times \mathbb{N}$ admitting a finite-fold Diophantine representation, would ensure existence of a finite-fold Diophantine representation of exponentiation.

In preparation for some conclusive answer to Mat10—be it positive or negative—, this paper brings together scattered notes on finite-fold Diophantine representability. The forthcoming material is organized as follows.

Sect. 2 reports the construction of a univocal exponential Diophantine representation of any given r.e. set $\mathcal{R}$. Out of a formally specified register machine that reaches termination on the tuples belonging to $\mathcal{R}$—and only on those—, the proposed construction technique generates a formula φ such that $(*)$ holds. By and large, singlefold-ness results from the determinism of the device emulated by the exponential constraints embodied into φ.

Then Sect. 3 discusses two ways of reducing exponentiation to any exponential-growth dyadic relation $\mathcal{J}(p,q)$; both techniques are due to Julia

[3] Notice that in the case of the relation $2^p = q$ we could take $\alpha = \beta = \delta = \gamma/2 = 2$ and then $p = w+2$, $q = 2^{w+2}$.

Robinson, who proposed them in 1952 and 1969 respectively. They ensure that if a (polynomial) Diophantine representation for $\mathcal{J}$ is found, then it can be converted into a Diophantine representation of exponentiation, and hence of any given r.e. set. Appendix A expounds the original correctness proof regarding the result of 1969.

Sect. 4 reports three ways, devised by Davis, Matiyasevich, and J. Robinson, of reducing exponentiation to the sequence $\langle \boldsymbol{y}_i(a)\rangle_{i\in\mathbb{N}}$ of solutions to the special-form Pell equation $(a^2-1)\,y^2+1=\square$ with $a>1$.[4] Appendices B and C dwell upon the techniques by which those three reductions were obtained.

To end, Sect. 5 presents four candidate "*rule-them-all equations*", and devotes some discussion to one of them. The prototype of those special equations was devised by Martin Davis over forty years ago [4], and still resists attempts to assess whether or not it has infinitely many integral solutions. Some hope that each r.e. set admits a finite-fold Diophantine representation lies, notwithstanding, in the expectation that a rule-them-all equation will be discovered to have a finite overall number of solutions in rational integers.

Remark 1.1. Note that allowing the existential variables to range over the set $\mathbb{Z}$ of signed integers (as would be closer to the habits of number theorists), or over $\mathbb{N}$ (as we have preferred to do), amount to the same when exponentiation does not occur in the above representation format $(*)$. In particular (see [19, p. 253]), it would suffice to replace each of our $\mathbb{N}$-valued x_i's by a sum $X_i^2+Y_i^2+Z_i^2+Z_i$ involving three new $\mathbb{Z}$-valued variables, to get a specification

$$(\exists X_1\cdots\exists X_\kappa)(\exists Y_1\cdots\exists Y_\kappa)(\exists Z_1\cdots\exists Z_\kappa)$$
$$\varphi(\,a_1,\ldots,a_m\,,X_1^2+Y_1^2+Z_1^2+Z_1,\ldots,X_\kappa^2+Y_\kappa^2+Z_\kappa^2+Z_\kappa\,),$$

interchangeable with $(\exists x_1\cdots\exists x_\kappa)\ \varphi(\,a_1,\ldots,a_m\,,x_1,\ldots,x_\kappa\,)$, of the same $\mathcal{R}\subseteq\mathbb{N}^m$.

2. Univocal exponential representation of any r.e. set

Where does singlefold-ness of the exponential representation of an r.e. set $\mathcal{R}\subseteq\mathbb{N}^m$ whatsoever stem from? In [15], where it was first achieved, such a representation took the form

$$\mathcal{R}(a_1,\ldots,a_m) \iff (\exists x_1\cdots\exists x_\kappa\exists y\exists w)\big[\ 2^y=w\ \&\ D(\,a_1,\ldots,a_m\,,x_1,\ldots,x_\kappa,y,w\,)=0\big],$$

where D is a polynomial in the variables $a_1,\ldots,a_m\,,x_1,\ldots,x_\kappa,y,w$ with integral coefficients; this was then rewritten, by exploiting an idea of Hilary Putnam, as

$$\mathcal{R}(a_1,\ldots,a_m) \iff (\exists x_1\cdots\exists x_\kappa\exists y\exists z\exists u)\qquad 4^u+u\ =\ \big[y+(y+z)^2\big]\,\big[1-D^2(\,a_1,\ldots,a_m\,,x_1,\ldots,x_\kappa,y,y+z\,)\big]\ .$$

[4] '$Q=\square$' means that the value of Q must be a perfect square.

This format is very elegant,[5] but the proof of the associated representability result less transparent than later single-fold-representability proofs where exponentiation was employed more liberally. Various proofs referred to *register machines*, a popular model of abstract computing device, to which James P. Jones and Yu. V. Matiyasevich resorted in three papers (see, e.g., [10]). We rely upon Martin Davis's account [6, Chapter 6] of the Jones-Matiysevich's approach in carrying out our considerations below.

A register machine $\boldsymbol{\pi}$ consists of a list $\Im_0, \ldots, \Im_\ell$ of *instructions*; any execution of $\boldsymbol{\pi}$ begins with instruction $\Im_0$ and, unless it goes on forever, it terminates with $\Im_\ell$. Finitely many program variables, $\mathsf{R}_0, \mathsf{R}_1, \ldots, \mathsf{R}_m, \ldots, \mathsf{R}_r$, called *registers*, occur in $\boldsymbol{\pi}$; of these, R_0 will hold the result $\boldsymbol{a}_0$ of the computation upon termination, <u>if</u> execution does reach $\Im_\ell$. At the outset, the registers $\mathsf{R}_1, \ldots, \mathsf{R}_m$ must hold the respective input values $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$, while the values of all remaining registers are supposed to be 0. Here, w.l.o.g., we shall require that $\boldsymbol{a}_0 = 0$.

There are instructions of five types:

$\mathsf{R}_j \;\leftarrow\; \mathsf{R}_j + 1$	increment
$\mathsf{R}_j \;\leftarrow\; \mathsf{R}_j - 1$	decrement
IF $\mathsf{R}_j = 0$ **GOTO** k	conditional branch
GOTO k	*un*conditional branch
STOP	halt

Suitable programming rules enforce that: (0) **STOP** only appears at the end of $\boldsymbol{\pi}$, namely as $\Im_\ell$; (1) the number k that follows **GOTO** in a branch instruction always belongs to the interval $0, \ldots, \boldsymbol{\ell}$; (2) it never happens that a decrement $\mathsf{R}_j \leftarrow \mathsf{R}_j - 1$ is reached when the current value of its register R_j is 0; (3) when—if ever—the instruction $\Im_\ell$ is reached, each one of $(\mathsf{R}_0,)$ $\mathsf{R}_1, \ldots, \mathsf{R}_r$ has value 0.

The behavior of $\boldsymbol{\pi}$ when its execution is triggered with input values $\boldsymbol{a}_i$ loaded in its input registers $\mathsf{R}_1, \ldots, \mathsf{R}_m$ should be readily grasped by any person familiar with procedural programming. In order to describe that functioning, we must specify by means of exponential Diophantine constraints how the values of the registers evolve over time and which instruction is about being effected at each of the discrete time instants beating the execution.

An unknown, s, representing the overall number of execution steps, will play a crucial role; in fact, we are interested in the r.e. set $\mathcal{R}$ consisting of

[5] Notice that the polynomial $y + (y+z)^2$ belongs to Kosovskiĭ's family of polynomials $x_1 + (x_1+x_2)^2 + (x_1+x_2+x_3)^3 + \cdots + (x_1 + \cdots + x_n)^n$ defining, for each $n \in \mathbb{N}$, an injective function of $\mathbb{N}^n$ into $\mathbb{N}$—see [11].

those tuples $\langle \boldsymbol{a}_1, \dots, \boldsymbol{a}_m \rangle$ which, when fed into $\boldsymbol{\pi}$, lead $\boldsymbol{\pi}$ to termination. Unless execution terminates, no natural number $\boldsymbol{s}$ should be an acceptable value for s under the constraints to be associated with $\boldsymbol{\pi}$; on the other hand, when a tuple leads to termination, an acceptable value $\boldsymbol{s}$ for s must exist and it must be unique, because the abstract computing device which we are modeling is deterministic. In the latter case, the course of values of each register R_j ($j = 0, \dots, \boldsymbol{r}$) can be modeled as the sequence $\langle \boldsymbol{\mathfrak{r}}_{j,0}, \dots, \boldsymbol{\mathfrak{r}}_{j,s} \rangle$ formed by its initial value $\boldsymbol{\mathfrak{r}}_{j,0}$ and by its subsequent values $\boldsymbol{\mathfrak{r}}_{j,t}$ with $t > 0$, where $\boldsymbol{\mathfrak{r}}_{j,t}$ is the value held by R_j right after the execution of the t-th step. Notice that if execution terminates in $\boldsymbol{s}$ computation steps, no register will ever hold a value exceeding the quantity $\boldsymbol{a}_1 + \cdots + \boldsymbol{a}_m + \boldsymbol{s}$; therefore we can represent the course of values of each R_j by a single unknown, $\mathfrak{r}_j$, designating the amount $\sum_{t=0}^{s} \boldsymbol{\mathfrak{r}}_{j,t}\, \boldsymbol{Q}^t$, where $\boldsymbol{Q} > \boldsymbol{a}_1 + \cdots + \boldsymbol{a}_m + \boldsymbol{s}$ is a base for the positional encoding of numbers large-enough in order that every $\boldsymbol{\mathfrak{r}}_{j,t}$ acts as a digit. Since $\boldsymbol{s}$ is *a priori* unknown, $\boldsymbol{Q}$ must in its turn show as an unknown, Q, in the constraints specifying $\boldsymbol{\pi}$. Out of practical concerns, it turns out convenient to subject Q, along with a buddy unknown $\flat$, to the conditions

$$2^{\flat} \ \leqslant\ (2a_1 + \cdots + 2a_m + 2s)\ \max\ (\boldsymbol{\ell} + 1)\ <\ 2^{\flat} \cdot 2\ =\ Q\,,$$

ensuring its uniqueness—and thus, thanks to the determinism of $\boldsymbol{\pi}$, also the uniqueness of $\mathfrak{r}_0, \dots, \mathfrak{r}_r$.

Additional unknowns $\mathfrak{l}_0, \dots, \mathfrak{l}_\ell$ are needed to describe which instruction is executed at each instant: $\mathfrak{l}_i$ designates the amount $\sum_{t=0}^{s} \boldsymbol{\mathfrak{l}}_{i,t}\, \boldsymbol{Q}^t$, where $\boldsymbol{\mathfrak{l}}_{i,t} = 1$ if the instruction to be executed at time t is $\mathfrak{I}_i$, and $\boldsymbol{\mathfrak{l}}_{i,t} = 0$ otherwise. One final unknown, I, is required to satisfy the equations

$$1 + (Q-1)\,I = Q^{s+1} = \sum_{i=0}^{\ell} \mathfrak{l}_i\,,$$

so that I designates $\sum_{t=0}^{s} \boldsymbol{Q}^t$. Thus, with respect to the bases Q and 2, I reads

$$\underbrace{1 \dots 11}_{s+1} \qquad \text{and} \qquad \underbrace{\underbrace{0 \dots 0}_{\flat}1 \dots \underbrace{0 \dots 0}_{\flat}1}_{s+1}$$

and the equation on the right reflects the fact that exactly one instruction is executed at each step. Putting

$$\Delta_{j,i} \quad =_{\text{Def}} \quad \begin{cases} \ \ 0 & \text{when } \mathfrak{I}_i \text{ does not affect } \mathsf{R}_j\,\text{, else} \\ \pm 1 & \text{according to whether } \mathfrak{I}_i \text{ is } \mathsf{R}_j \leftarrow \mathsf{R}_j \pm 1\,, \end{cases}$$

we must then require, for $j = 0, \dots, \boldsymbol{r}$ that

$$\mathfrak{r}_j \quad = \quad \left(\mathfrak{r}_j + \textstyle\sum_{i=0}^{\ell} \Delta_{j,i}\, \mathfrak{l}_i\right) Q + \begin{cases} a_j & \text{if} \quad 0 < j \leqslant \boldsymbol{m}\,, \\ 0 & \text{otherwise,} \end{cases}$$

to state how the course of values of each variable is ruled by the execution steps.[6]

To perfect the constraint-based description of the execution of $\boldsymbol{\pi}$, we shall resort to the *masking* relation $a \sqsubseteq b$ that occurs between $a = \sum_{h=0}^{k} a_h 2^h$ and $b = \sum_{h=0}^{k} b_h 2^h$, with $a_0, b_0, \ldots, a_k, b_k \in \{0,1\}$, if and only if $a_h \leqslant b_h$ holds for $h = 0,1,\ldots,k$. Since $\binom{0}{1} = 0$ and $1 = \binom{0}{0} = \binom{1}{0} = \binom{1}{1}$, the Lucas's congruence

$$\binom{\sum_{h=0}^{k} b_h 2^h}{\sum_{h=0}^{k} a_h 2^h} \equiv \prod_{h=0}^{k} \binom{b_h}{a_h} \pmod{2}$$

yields that $a \sqsubseteq b$ holds if and only if $\binom{b}{a}$ is odd. The masking relation hence is exponential Diophantine; in fact, thanks to the binomial theorem, $a \sqsubseteq b$ holds if and only if the remainder of the integer division of $\left\lfloor \left(2^{b+1}+1\right)^{b} / 2^{ba+a} \right\rfloor$ by 2^{b+1} is odd. The final constraints needed are, for $j = 0,1,\ldots,\boldsymbol{r}$ and $i = 0,1,\ldots,\boldsymbol{\ell}$:

- $\mathfrak{r}_j \sqsubseteq \lfloor Q/2-1 \rfloor I$ and $\mathfrak{l}_i \sqsubseteq I$, $1 \sqsubseteq \mathfrak{l}_0$, $\mathfrak{l}_\ell \sqsubseteq Q^s$;
- $Q\,\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1}$ when $\Im_i$ is an incre-/decre-ment instruction;
- $Q\,\mathfrak{l}_i \sqsubseteq \mathfrak{l}_k$ when $\Im_i$ is an unconditional branch instruction **GOTO** k;
- $Q\,\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1} + \mathfrak{l}_k$ and $Q\,\mathfrak{l}_i \sqsubseteq \mathfrak{l}_{i+1} + QI - 2\,\mathfrak{r}_j$ when $\Im_i$ is a conditional branch instruction **IF** $\mathsf{R}_j = 0$ **GOTO** k.

Example 2.1 (Adapted from [7]). Goldbach's conjecture, stating that *every even integer greater than 2 is the sum of two prime numbers*, can be formulated in a first-order arithmetic of natural numbers by the sentence

$$\forall a \exists p \exists q \forall u \forall v \Big(\big((p = u \cdot v \lor q = u \cdot v) \Longrightarrow (u = 1 \Longleftrightarrow v \neq 1) \big) \;\&\; a+a+4 = p+q \Big).$$

Thanks to DPR, the conjecture can also be formulated with no quantifier alternations, by means of a sentence of the form

$$\neg(\exists x_0 \cdots \exists x_\kappa)\, \gamma(0, x_0, x_1, \ldots, x_\kappa),$$

where γ is a quantifier-free exponential Diophantine formula enforcing that

$$\mathcal{G}(a) = c \quad \Longleftrightarrow \quad (\exists x_1 \cdots \exists x_\kappa)\, \gamma(\overbrace{\underbrace{c\,,\,a}_{\text{param's}}\,,\,\underbrace{x_1,\ldots,x_\kappa}_{\text{unknowns}}}^{\text{variables}}),$$

[6] Rather than presupposing that the value $\boldsymbol{a}_0$ of the output register be 0 at the end, here we could have modified the condition associated with R_0 into $\mathfrak{r}_0 = \left(\mathfrak{r}_0 + \sum_{i=0}^{\ell} \Delta_{0,i}\,\mathfrak{l}_i\right) Q - Q^{s+1} a_0$, thus capturing the *graph* $\langle \boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \rangle$—an r.e. set on its own right—of the function computed by $\boldsymbol{\pi}$ instead of its domain.

holds, where

$$\mathcal{G}(a) \quad =_{\text{Def}} \quad \begin{cases} 1 & \text{if there are prime numbers } p, q \\ & \text{such that } a+a+4 = p+q\,, \\ 0 & \text{otherwise.} \end{cases}$$

Such a γ can be built by conjoining together all constraints that specify the behavior of a register machine $\boldsymbol{\gamma}$ computing $\mathcal{G}$, in the manner discussed above.[7]

3. Two admirable ways of specifying exponentiation in terms of a relation of exponential growth

In her seminal paper [22] published in 1952, Julia Robinson discusses—among many things—how to specify the graph of exponentiation, namely the triadic relation $b^n = c$, in the format

$$b^n = c \quad \Longleftrightarrow \quad (\exists x_1 \cdots \exists x_\kappa)\ \varphi(\overbrace{\underbrace{b,n,c}_{\text{param's}}\ ,\underbrace{x_1,\ldots,x_\kappa}_{\text{unknowns}}}^{\text{variables}}) \qquad (\ddagger)$$

closely analogous to (†), with permission to employ in the construction of φ, instead of exponentiation, a dyadic relation $\mathcal{J}$ which is *of exponential growth* in the following sense:

i) $\mathcal{J}(p,q)$ implies $q < p^p$;

ii) for each $\ell \geqslant 0$, there are p and q such that $\mathcal{J}(p,q)$ and $p^\ell < q$.

The essence of such a specification is best explained in terms of a polynomial which, chronologically (see [20, p. 531]), made its first appearance long after 1952:

Lemma 3.1. *There is a polynomial Q in two variables with coefficients in* $\mathbb{N}$ *such that* (using $\tau = \square$ as a short for $\exists q\,(\,\tau = q^2\,)$)*:*

- $Q(w,h) = \square \implies h > w^w$*;*
- *to every w, there correspond h's such that $Q(w,h) = \square$.*

Proof, just a clue. It suffices to take $Q(w,h) := (w+2)^3\,(w+4)\,(h+1)^2+1$. ⊣

[7] Bear in mind, here, the remark made in the preceding footnote.

Theorem 3.2. *Let Q be as in Lemma 3.1. The following bi-implication then holds if $\mathcal{J}$ meets the exponential-growth requirements i) and ii).*

$$\begin{aligned} b^n = c \iff (\exists w, h, a, d, \ell, u, v, s, q)\Big[\ & (c-1)^2 + b + n = 0 \vee \\ & (c+b = 0 \,\&\, n \geqslant 1) \vee \\ \Big(& b \geqslant 1 \;\&\; c \geqslant 1 \;\&\; d \geqslant \ell \;\&\; \mathcal{J}(a,d) \quad \& \\ & \ell^2 = \left(a^2-1\right)\left[n+(a-1)\,s\right]^2 + 1 \quad \& \\ & w > b \max n \;\&\; Q(w,h) = q^2 \;\&\; a \geqslant h \max\,(c+1) \;\& \\ & u^2 = (a^2 b^2 - 1)\, v^2 + 1 \;\&\; c = \lfloor u/\ell \rfloor \Big) \Big]. \end{aligned}$$

This rule, if there exists a Diophantine relation $\mathcal{J}$ satisfying i) & ii), provides a Diophantine representation of exponentiation.

Proof. Proving the stated bi-implication is not a simple matter: we refer the interested reader to [2, Appendix A] for details on this.

Concerning the second part of the claim, we must show that certain relations are Diophantine; namely: $x \geqslant y \iff \exists v\,(x = v + y)$, $x > y \iff x \geqslant y + 1$, $x = y \max z \Leftrightarrow (x = y \geqslant z \vee x = z \geqslant y)$, $x = \lfloor y/z \rfloor \Leftrightarrow \exists q\,\big(qz \leqslant y < (q+1)z\big)$. ⊣

In [23, p. 109 and p. 112], J. Robinson simplifies the above construction and proof, getting:

Theorem 3.3. *Suppose that $\mathcal{J}$ is an exponential-growth relation such that $\mathcal{J}(p,q)$ implies $p > 1$, and let Q be as in the proof of Lemma 3.1. Then the bi-implication*

$$\begin{aligned} b^n = c \iff (\exists a, d, \ell, s, x, h)\Big[\ & (c-1)^2 + n = 0 \quad \vee \\ & (n \geqslant 1 \,\&\, c + b = 0) \quad \vee \\ \Big(& n \geqslant 1 \;\&\; b \geqslant 1 \;\&\; \mathcal{J}(a,d) \;\&\; d > \ell \;\&\; a > b + n \quad \& \\ & \ell^2 = (a^2-1)\left[n+(a-1)\,s\right]^2 + 1 \;\&\; Q(b+n-2,h) = x^2 \;\& \\ & 2ab - b^2 - 1 \geqslant \left[(b+n+1)\,x\right] \max\left(c+1\right) \quad \& \\ & 2ab - b^2 - 1 \mid \ell - \left(a-b\right)\left[(a-1)\,s+n\right] - c \Big) \Big] \end{aligned}$$

holds, which gives us a Diophantine repr. of exponentiation if $\mathcal{J}$ is Diophantine.

Proof. A proof of the stated bi-implication is provided in Appendix A; clearly divisibility is Diophantine, since $x \mid y \iff \exists\, v\,(y = v\,x)$. $\dashv$

4. Three ways of specifying exponentiation in terms of the sequence of solutions to a special-form Pell equation

Pell equations of the special form $x^2 - (a^2-1)\,y^2 = 1$, with $a > 1$, have peeped in in the preceding section. Through one such equation we enforced a relationship between ℓ and $r := \big(n + (a-1)\,s\big)$ in Theorems 3.2 and 3.3. Constraints involving the tricky polynomial $Q(w,h)$ have also shown up; as one sees, $Q(w,h) = q^2$ can be put in the said Pell format, becoming $q^2 - \big[(w+3)^2 - 1\big]\,\big[(w+2)\,(h+1)\big]^2 = 1$.

Generally speaking, the Pell equation $x^2 - d\,y^2 = 1$ in the unknowns x, y has *in*finitely many solutions in $\mathbb{N}$, provided that the parameter d (also in $\mathbb{N}$) is *not* a perfect square. In the special case when $d = a^2 - 1$ with $a > 1$, the increasing sequence $\big\langle \langle \boldsymbol{x}_i(a)\,,\, \boldsymbol{y}_i(a)\rangle \big\rangle_{i\in\mathbb{N}}$ of its solutions satisfies the recurrences

$$\begin{array}{rclcrclcrcl} \boldsymbol{y}_0(a) & = & 0\,, & \quad & \boldsymbol{y}_1(a) & = & 1 = \boldsymbol{x}_0(a)\,, & \quad & a & = & \boldsymbol{x}_1(a)\,, \\ & & & & \boldsymbol{y}_{i+2}(a) & = & 2a\boldsymbol{y}_{i+1}(a) - \boldsymbol{y}_i(a)\,, & & & & \\ & & & & \boldsymbol{x}_{i+2}(a) & = & 2a\boldsymbol{x}_{i+1}(a) - \boldsymbol{x}_i(a)\,. & & & & \end{array}$$

We summarize in Fig. 2 the combinatorial interplay among items in this sequence yielded by their generating rules (see, e.g., [22, pp. 439–440] and [20, pp. 527–528]).

Many of the facts in Fig. 2 are needed, of course, in order to detail the proofs of Theorems 3.2 and 3.3. They also enter Davis's proof [5] of the following:

Theorem 4.1. *The bi-implication*

$$b^n = c \iff (\exists\, a, \ell, r)\Bigg[\begin{array}{ll} (c-1)^2 + b + n + a + \ell + r = 0 & \vee \\ (n \geqslant 1 \;\&\; c + b + a + \ell + r = 0) & \vee \\ \Big(b \geqslant 1 \;\&\; \ell = \boldsymbol{x}_n(a) \;\&\; r = \boldsymbol{y}_n(a) & \& \\ \quad a = \boldsymbol{x}_{b+n}(b+n+1) \;\&\; b+n \mid \boldsymbol{y}_{b+n}(b+n+1) & \& \\ \quad 2ab - b^2 - 1 \geqslant c & \& \\ \quad c \equiv \ell - (a-b)\,r \;(\bmod\; 2ab - b^2 - 1\,)\Big) \end{array}\Bigg]$$

1. $(2a)^i \geqslant \boldsymbol{y}_{i+1}(a) > \boldsymbol{y}_{i+1}(a)/a > \boldsymbol{y}_i(a) \geqslant i$ and $\boldsymbol{y}_{i+1}(a) \geqslant (2a-1)^i$;
2. $\boldsymbol{x}_{i+1}(a) > \boldsymbol{x}_{i+1}(a)/a \geqslant \boldsymbol{x}_i(a) \geqslant a^i > i$ and
   $a^{2i+2} \geqslant (2a)^{i+1} > \boldsymbol{x}_{i+1}(a), \quad \boldsymbol{x}_{i+2}(a) > a^{i+2}$;
3. $\boldsymbol{x}_i(a) - (a-b)\,\boldsymbol{y}_i(a) \equiv b^i \pmod{2ab - b^2 - 1}$;
4. $\boldsymbol{y}_i(a) \equiv i \pmod{a-1}$;
5. $(b \geqslant 1 \,\&\, a > b^n) \Longrightarrow [b^n = c \Longleftrightarrow c\,\boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_n(ab) < (c+1)\,\boldsymbol{x}_n(a)]$;
6. $(b \geqslant 1 \,\&\, a > b^n) \Longrightarrow \big[\ \boldsymbol{x}_n(a) \leqslant \boldsymbol{x}_m(ab) < a\boldsymbol{x}_n(a) \quad \Longleftrightarrow \quad m = n\ \big]$;
7. $\boldsymbol{y}_n(a) \mid \boldsymbol{y}_\ell(a)$ if and only if $n \mid \ell$; if $\boldsymbol{y}_n^2(a) \mid \boldsymbol{y}_\ell(a)$, then $\boldsymbol{y}_n(a) \mid \ell$.

Figure 2: The wealth of interplay among solutions to the Pell equation $x^2 - (a^2-1)\,y^2 = 1$.

holds, where a, ℓ, and r are uniquely determined. This gives us a Diophantine representation of exponentiation, whichever way we manage to get a Diophantine representation of the triadic relation $\boldsymbol{y}_i(a) = y$ (whose arguments are: i, a, y).

Proof. A proof of the stated bi-implication results from Appendix B; clearly congruency is Diophantine, since $x \equiv y \pmod{z} \Leftrightarrow \exists v\,\big(v^2 z^2 - (x-y)^2 = 0\big)$. ⊣

What we are seeing here is, in essence, a *singlefold* representation of exponentiation *in terms* of the triadic relation $\boldsymbol{y}_i(a) = y$.[8] In fact, for any triple b, n, c of natural numbers: if $b^n \neq c$, the shown system in the unknowns a, ℓ, r etc. has no solution; if $b^n = c$, then it has exactly one solution. Matters change if we specify the relation $\boldsymbol{y}_i(a) = y$ by polynomial Diophantine means (which is doable—see, e.g., [5] and [20]); for, then, additional unknowns enter into play, which lead to infinitely many solutions when any solution exists.

As stressed in [18, pp. 43–44], all today known methods of constructing a polynomial Diophantine representation (‡) are in fact based on the study

[8] To see this more clearly, one should set aside various eliminable constructs. E.g. ‘|’, along with $\boldsymbol{x}_{b+n}(b+n+1)$, can be eliminated by rewriting the fourth line of the above specification as a constraint involving a new unknown w, as: $(b+n)\,w = \boldsymbol{y}_{b+n}(b+n+1)$ & $\big[(b+n+1)^2 - 1\big]\,\big[(b+n)\,w\big]^2 + 1 = a^2$. Likewise, $\ell = \boldsymbol{x}_n(a)$ becomes $(a^2-1)\,r^2 + 1 = \ell^2$, and three unknowns will result from elimination of $\geqslant, >$, and $\equiv$.

of the behavior of recurrent sequences like the famous Fibonacci progression $\langle 0,1,1,2,3,5,8,\ldots\rangle$, or a sequence $\langle \boldsymbol{y}_0(a), \boldsymbol{y}_1(a), \boldsymbol{y}_2(a), \ldots\rangle$, "taken some modulo; clearly, this behavior is periodic and as a consequence each known Diophantine representation of exponentiation is infinite-fold".[9]

The situation does not improve, as for the finite-fold-ness issue, even if we resort to the elegant specification of exponentiation proposed in [16] by Matiyasevich, who considers the sequence $\langle \boldsymbol{m}_0(a), \boldsymbol{m}_1(a), \boldsymbol{m}_2(a), \ldots\rangle$ with $a \in \mathbb{N} \setminus \{0,1\}$ characterized by the second-order recurrence

$$\boldsymbol{m}_0(a) \;=\; 0, \qquad \boldsymbol{m}_1(a) \;=\; 1, \qquad \boldsymbol{m}_{i+2}(a) = a\boldsymbol{m}_{i+1}(a) - \boldsymbol{m}_i(a)\,.$$

The distinguished scholar achieves a *singlefold* representation of exponentiation *in terms* of the triadic relation $\boldsymbol{m}_i(a) = m$. His result, as stated here, also refers to the sequence $\langle \boldsymbol{y}_i(a)\rangle_{i\in\mathbb{N}}$;[10] it is explained, albeit briefly, in our Appendix C.

Theorem 4.2 ([16, pp. 31–32])**.** *The bi-implications*

$$\begin{array}{lllll}
b^n = c & \Longleftrightarrow & c = & \lfloor \boldsymbol{m}_{n+1}(16b(n+1)\boldsymbol{m}_{n+1}(2b+2)+4)\ / & \\
& & & \ \boldsymbol{m}_{n+1}(16\quad(n+1)\boldsymbol{m}_{n+1}(2b+2))\rfloor & \\
& \Longleftrightarrow & c = & \lfloor \boldsymbol{y}_{n+1}(8b(n+1)\boldsymbol{y}_{n+1}(b+1)+2)\ / & \\
& & & \ \boldsymbol{y}_{n+1}(8\quad(n+1)\boldsymbol{y}_{n+1}(b+1))\rfloor & \\
& \Longleftrightarrow & (\exists x,y,z,r,s)\big(& z = cy+r\ \&\ 1+r+s = y & \& \\
& & & z = \boldsymbol{y}_{n+1}(bx+2) & \& \\
& & & y = \boldsymbol{y}_{n+1}(x) & \& \\
& & & x = 8(n+1)\boldsymbol{y}_{n+1}(b+1) & \big)\,.
\end{array}$$

hold, where x, y, z, r, and s are uniquely determined. This gives us a Diophantine representation of exponentiation, whichever way we manage to get a Diophantine representation of either one of the triadic relations $\boldsymbol{m}_i(a) = m$, $\boldsymbol{y}_i(a) = y$.

One slightly less slick, but nevertheless very elegant, reduction of exponentiation to the sequence $\langle \boldsymbol{y}_i(a)\rangle_{i\in\mathbb{N}}$ also deserves being mentioned:

[9] k-TH ORDER LINEAR RECURRENCES (with $k > 0$) are defined to be sequences $a_0, a_1, a_2, \ldots$ in which $a_n = b_{k-1}\,a_{n-1} + \cdots + b_0\,a_{n-k}$ holds for every $n \geqslant k$, where: the b_i's are integer coefficients, $b_0 = \pm 1$, and the polynomial $\lambda^k - b_{k-1}\lambda^{k-1} - \cdots - b_1\lambda - b_0$ is irreducible over $\mathbb{Q}$. A Diophantine representation of exponentiation is most often associated with a second-order recurrence, but Maxim A. Vsemirnov showed that certain recurrent sequences of orders 3 and 4 can also do the job (cf. [26]).

[10] An early reduction of exponentiation to an integer quotient that involves, besides Diophantine functions, only the triadic relation $\boldsymbol{y}_i(a) = y$, appears in [15, p. 308].

Theorem 4.3 ([20, pp. 534–535])**.** *When $b \geqslant 1$ and $n \geqslant 1$, the bi-implication*

$$b^n = c \iff (\exists m, k, p, q)\left[\begin{array}{ll} k+n+1 = \boldsymbol{y}_{mb}(n+1) & \& \\ m = 4n(c+1)+b+2 & \& \\ (m^2-1)p^2+1 = q^2 & \& \\ m-1 \mid p-n-1 & \& \\ \big(p^2-4(k+n+1-pc)^2\big)\, bcn > 0 & \end{array}\right]$$

holds (whence, trivially, the variable m can be eliminated).

5. Promising (Diophantine?) exponential-growth relations

In 1968, Martin Davis focused upon the subset

$$\mathcal{J}_7(p,q) \quad \Leftrightarrow_{\text{Def}} \quad \exists \ell \left[q = \boldsymbol{y}_{2^\ell} \ \& \ p \geqslant 2^\ell \ \& \ p > 16\right]$$

of $\mathbb{N}^2$, where $\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}}$ is the increasing sequence $\langle 0,3,48,765,\ldots\rangle$ consisting of the infinitely many non-negative integer solutions to the Pell equation $7y^2 + 1 = \Box$. In [4], he showed that $\mathcal{J}_7$ is a relation of exponential growth and raised the question: Is $\mathcal{J}_7$ a Diophantine set? Davis showed that the answer is affirmative—and then every r.e. set turns out to be Diophantine—provided there exist only a finite number of integral solutions to the quaternary quartic equation

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

which (if finite-folded) would hence acquire the title of "*rule-them all equation*".

By much the same treatment conceived by Davis, two of the authors of this paper[11] found a few more candidate rule-them-all equations (see [2]). They are:

$$\begin{array}{rcl} 2 \cdot \left(r^2+2s^2\right)^2 - \left(u^2+2v^2\right)^2 & = & 1, \\ 3 \cdot \left(r^2+3s^2\right)^2 - \left(u^2+3v^2\right)^2 & = & 2, \\ 11 \cdot \left(r^2+rs+3s^2\right)^2 - \left(v^2+vu+3u^2\right)^2 & = & 2. \end{array}$$

In his treatment of $\mathcal{J}_7$, Davis took advantage of the fact that 7 is one of the nine square-free rational integers $d > 0$ such that the integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ form a unique-factorization integral domain.[12] Our

[11] Thanks to clues given by Martin Davis and by Pietro Corvaja.

[12] Recall that the *ring of integers* of an algebraic number field K is the ring of all elements of K which are roots of monic polynomials $x^n + c_{n-1}x^{n-1} + \cdots + c_0$ with rational integer coefficients c_i.

new equations correspond to the discriminants $-2, -3, -11$; four more discriminants, corresponding to the values $d \in \{19, 43, 67, 163\}$, might lead to further candidate rule-them-all equations, but they remain as of today untreated.[13]

For each $d \in \{2, 3, 11\}$, we figured out an exponential-growth dyadic relation $\mathcal{J}_d$ which would turn to be Diophantine if one succeeded in proving that the corresponding quaternary quartic equation has, in all, finitely many solutions. The relations at stake are:

$\mathcal{J}_2(p,q) \Leftrightarrow_{\mathrm{Def}} \exists \ell \left[q = \boldsymbol{y}_{2^\ell} \;\; \& \;\; p \geqslant 2^{\ell+1} \;\; \& \;\; p \mid q \right]$, where $\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}}$ is the endless, strictly ascending, sequence $\langle 0, 2, 12, 70, 408, \ldots \rangle$ consisting of all non-negative integer solutions to the Pell equation $2y^2 + 1 = \square$;

$\mathcal{J}_3(p,q) \Leftrightarrow_{\mathrm{Def}} \exists \ell \left[q = \boldsymbol{y}_{2^{2\ell+1}} \;\; \& \;\; 2^{2\ell+2} \mid p \;\; \& \;\; p \mid q \right]$, where $\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}}$ is the ascending sequence $\langle 0, 1, 4, 15, 56, 209, \ldots \rangle$ consisting of all distinct non-negative integer solutions to the Pell equation $3y^2 + 1 = \square$;

$\mathcal{J}_{11}(p,q) \Leftrightarrow_{\mathrm{Def}} \exists \ell \left[q = \boldsymbol{y}_{2^{2\ell+1}} \;\; \& \;\; p \geqslant 2^{2\ell+2} \;\; \& \;\; p \mid q \;\; \& \;\; \ell > 1 \right]$, where $\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}}$ is the ascending sequence $\langle 0, 3, 60, 1197, \ldots \rangle$ consisting of all distinct non-negative integer solutions to the Pell equation $11y^2 + 1 = \square$.

In the ongoing, we will offer a bird's-eye view of how to construct, directly from the *unproven assertion* that the equation

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

has only finitely many integral solutions, a finite-fold polynomial Diophantine representation of the relation $\mathcal{J}_2$. As regards the other three candidate rule-them-all equations: the ones corresponding to $\mathcal{J}_7$ and $\mathcal{J}_3$ are treated in detail, respectively, in [4] and in [2] ([2] even shows that the property stated in Fig. 1 is satisfied by $\mathcal{D} = \mathcal{J}_3$); the one corresponding to $\mathcal{J}_{11}$ is treated—albeit more briefly—in [1].[14]

[13] Note added in proof. In Dec 2020, Luca Cuzziol obtained this candidate rule-them-all equation corresponding to $d = 19$:

$$171 \cdot \left(r^2 + rs + 5s^2\right)^2 - 169 \cdot \left(v^2 + vu + 5u^2\right)^2 \;\; = \;\; 2\,.$$

In March 2021, he also associated a candidate rule-them-all equation to $d = 43$.

[14] Note added in proof. In Dec 2020, Luca Cuzziol found these non-trivial solutions to the equation $171 \cdot \left(r^2 + rs + 5s^2\right)^2 - 169 \cdot \left(v^2 + vu + 5u^2\right)^2 = 2$ associated with $d = 11$:

$$\begin{array}{lllll} r = 8, & s = 9, & v = 30, & u = 7, & \text{and} \\ r = 8, & s = 9, & v = 13, & u = 17. & \end{array}$$

Along with the above-indicated sequence $\langle \boldsymbol{y}_i \rangle_{i\in\mathbb{N}}$ of all solutions to the Pell equation $2y^2+1=\Box$ in $\mathbb{N}$, take also into account the associated sequence $\langle \boldsymbol{x}_i \rangle_{i\in\mathbb{N}} = \langle 1,3,17,99,577,\ldots\rangle$ with $\boldsymbol{x}_i = \sqrt{2y^2+1}$. Call a positive integer w *representable* if there are non-negative integers u,v such that $w=u^2+2v^2$. Thus we will have:

- A positive integer is representable if and only if in its factorization no prime number p such that either $p\equiv 5 \pmod 8$ or $p \equiv 7 \pmod 8$ holds appears with an odd exponent.
- Every number of the form $\boldsymbol{y}_{2^\ell}$ is representable. In fact, $\boldsymbol{y}_{2^0}=\boldsymbol{y}_1=2=0^2+2\cdot 1^2$. If $\ell>0$, then we have $\boldsymbol{y}_{2^\ell}=2^{\ell+1}\cdot 3\cdot\prod_{0<i<\ell}\boldsymbol{x}_{2^i}$, where $\boldsymbol{x}_{2^i}=\boldsymbol{x}^2_{2^{i-1}}+2\boldsymbol{y}^2_{2^{i-1}}$ holds for each factor $\boldsymbol{x}_{2^i}$; hence $\boldsymbol{y}_{2^\ell}$ is representable, inasmuch as the product of representable numbers.
- If $\boldsymbol{y}_{2\ell+1}$ (with $\ell \geqslant 0$) is representable, so are $\overbrace{\boldsymbol{x}_\ell+2\boldsymbol{y}_\ell \text{ and } \boldsymbol{x}_\ell+\boldsymbol{y}_\ell}^{\textit{coprime numbers}}$.
- If $\boldsymbol{y}_n$ is representable for some $n>0$ *not* a power of 2, then the system

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

  has an integral solution for which $Y\neq 0$; consequently, the equation (‡) has a non-trivial integral solution $\langle \bar r,\bar s,\bar u,\bar v\rangle$ such that $\left[2\,(\bar r^2+2\,\bar s^2)\,(\bar u^2+2\,\bar v^2)\right] \mid \boldsymbol{y}_n$, a solution being dubbed *trivial* when it satisfies $r=\pm 1\ \ \&\ \ s=0$.

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, in all, finitely many solutions in integers.*

Then the above-listed facts yield that:

Theorem 5.1. $\mathcal{H}$ implies that, for $n>0$, $\boldsymbol{y}_n$ is representable if and only if n is a power of 2.

Corollary 5.2. $\mathcal{H}$ implies that $\{\boldsymbol{y}_{2^\ell} \mid \ell=0,1,2,\ldots\}$ is a Diophantine set.

Lemma 5.3. $\mathcal{H}'$ implies that $\{\boldsymbol{y}_{2^\ell} \mid \ell = 0, 1, 2, \dots\}$ is a Diophantine set.

The following bi-implication is plainly recognized to hold:

$$\mathcal{J}_2(p,q) \iff (p = 2 \ \& \ q = 2) \vee \big(q \in \{\boldsymbol{y}_{2^\ell} \mid \ell > 0\} \ \& \exists x[(2x+1)\,p = q]\big).$$

Does the predicate $q \in \{\boldsymbol{y}_{2^\ell} \mid \ell > 0\}$—and, consequently, $\mathcal{J}_2$—admit a polynomial Diophantine representation? It turns out that the following are necessary and sufficient conditions in order for $q \in \{\boldsymbol{y}_{2^\ell} \mid \ell > 0\}$ to hold:

(i) $q > 2$;

(ii) $2q^2 + 1 = \square$ (i.e., $q = \boldsymbol{y}_n$ holds for some $n \geqslant 0$);

(iii) $(\exists u, v)(y = u^2 + 2v^2)$ (i.e., y is representable);

(iv) $2\,(u^2+2v^2)\,(r^2+2s^2) \nmid q$, for any non-trivial solution $\langle u, v, r, s\rangle$ to (‡).

Notice that (i)–(iii) are immediately expressible by existential Diophantine equations. Moreover, if $\mathcal{H}'$ is true, then also (iv) is expressible by an existential Diophantine equation. Indeed, let $\langle u_0, v_0, r_0, s_0\rangle, \dots, \langle u_m, v_m, r_m, s_m\rangle$ be all of the non-trivial solutions to (‡) in $\mathbb{N}$. Then (iv) is easily seen to be equivalent to

$$(\exists w_0, \dots, w_m, z_0, \dots, z_m, t_0, \dots, t_m) \bigwedge_{i=0}^{m} \Big[q = 2\,(u_i^2 + 2v_i^2)\,(r_i^2 + 2s_i^2)\,t_i + w_i + 1 \\ \& \ w_i + z_i + 2 = 2\,(u_i^2 + 2v_i^2)\,(r_i^2 + 2s_i^2)\Big].$$

This leads to a Diophantine specification of $\mathcal{J}_2$ **if** *the number of solutions to* (‡) *is finite* ! (An issue that we are unable to answer.)

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 our quaternary quartic equation (‡) has only finitely many solutions in $\mathbb{N}$ can be recast as the analogous problem concerning the system[15]

$$\begin{cases} \xi^2 - 2\eta^2 &= -1 \\ \xi\,\eta &= t^2 + 2w^2 \end{cases}$$

over $\mathbb{Z}$. The existence of finite-fold Diophantine representations for all r.e. sets thus reduces to the finitude of the set of integral points lying on a specific surface.

[15] In order to transform the solutions to this system into solutions to (‡), notice that ξ and η turn out to be coprime numbers; consequently, the representability of their product implies the representability of both of them.

Conclusions: Potential outcomes

A striking consequence of the univocal exponential representability of any r.e. set was noted in [15, p. 300 and p. 310]. One can find a concrete polynomial $B(a, x_0, x_1, \ldots, x_\kappa, y, w)$ with integral coefficients such that:

1) to each $\boldsymbol{a} \in \mathbb{N}$, there corresponds at most one $\boldsymbol{k}+2$ tuple $\langle \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u} \rangle$ such that $B(\boldsymbol{a}, \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u}, 2^{\boldsymbol{u}}) > 0$ holds;

2) to any monadic totally computable function $\mathcal{C}$, there correspond $(\boldsymbol{k}+3)$-length tuples $\langle \boldsymbol{a}, \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u} \rangle$ of natural numbers such that
$$B(\boldsymbol{a}, \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u}, 2^{\boldsymbol{u}}) > 0 \quad \text{and} \quad \max\{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u}\} > \mathcal{C}(\boldsymbol{a}).$$

To see this, refer to an explicit enumeration $\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2, \ldots$ of all monadic partially computable functions (see [9, p. 73 ff]), so that both of

$$\begin{array}{rcl} \mathcal{H} & = & \{ \langle a_1, a_2 \rangle \in \mathbb{N}^2 \mid \boldsymbol{f}_{a_1}(a_1) = a_2 \}, \\ \mathcal{K} & = & \{ a \in \mathbb{N} \mid \langle a, x \rangle \in \mathcal{H} \text{ holds for some } x \} \end{array}$$

are r.e. sets, the complement $\mathbb{N} \setminus \mathcal{K}$ of the latter is not an r.e. set, and the former can be represented in the univocal form shown at the beginning of Sect. 2, namely

$$\boldsymbol{f}_{a_1}(a_1) = a_2 \iff (\exists x_1 \cdots \exists x_\kappa \exists y \exists w)[\ 2^y = w \ \&\ D(a_1, a_2, x_1, \ldots, x_\kappa, y, w) = 0\ ],$$

where D is a polynomial with integral coefficients; then put

$$B(a, x_0, x_1, \ldots, x_\kappa, y, w) \quad =_{\text{Def}} \quad 1 - D^2(a, x_0, x_1, \ldots, x_\kappa, y, w),$$

so that $B(a, x_0, x_1, \ldots, x_\kappa, y, 2^y) > 0$ holds if and only if $\boldsymbol{f}_a(a) = x_0$, and hence B satisfies 1).

By way of contradiction, suppose that there is a monadic totally computable function $\mathcal{C}_*$ such that the inequalities $\boldsymbol{v}_0 \leqslant \mathcal{C}_*(\boldsymbol{a}), \ldots, \boldsymbol{v}_\kappa \leqslant \mathcal{C}_*(\boldsymbol{a})$, and $\boldsymbol{u} \leqslant \mathcal{C}_*(\boldsymbol{a})$ hold whenever a tuple $\langle \boldsymbol{a}, \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u} \rangle$ of natural numbers exists such that $B(\boldsymbol{a}, \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa, \boldsymbol{u}, 2^{\boldsymbol{u}}) > 0$ holds; that is, they hold when a pair $\langle \boldsymbol{a}, \boldsymbol{v}_0 \rangle \in \mathcal{H}$ exists (this happens, e.g., for the infinitely many $\boldsymbol{a}$'s satisfying $\mathcal{C}_* = \boldsymbol{f}_a$). In particular, the said inequalities must hold when $\boldsymbol{a} \in \mathcal{K}$. But then this would offer us a criterion for checking whether or not $\boldsymbol{a} \in \mathcal{K}$, by evaluating a bounded family of expressions of the form $B(\boldsymbol{a}, v_0, v_1, \ldots, v_\kappa, u, 2^u)$; however, this would conflict with the fact that $\mathbb{N} \setminus \mathcal{K}$ is not r.e. We conclude that B satisfies 2).

Summing up, we are in this situation: thanks to *reductio ad absurdum*, we have found that the course of values of the concrete arithmetic expression $B(a, v_0, v_1, \ldots, v_\kappa, u, 2^u)$ exceeds zero at most once for each value $\boldsymbol{a}$ of a; it is unconceivable, though, that one can put an effective upper bound on the values for $v_0, v_1, \ldots, v_\kappa, u, 2^u$ in $\mathbb{N}$ which may enforce $B(a, v_0, v_1, \ldots, v_\kappa, u, 2^u) > 0$.

A proof that every r.e. set admits a finite-fold Diophantine polynomial representation would yield analogous, equally striking consequences about 'non-effectivizable estimates' (cf. [18]).

Other possible consequences affect the Diophantine characterization of the probability of selecting by chance a program which terminates on every input (see [3, 21]). For any model C of computation according to which the programs are self-delimiting binary sequences, programs can be selected by chance by flipping an unbiased coin until a valid program comes out. So, the probability of selecting by chance a program which halts in the specific model C is

$$\Omega =_{\text{Def}} \sum_{p \text{ halts in } C} 2^{-|p|}$$

where $|p|$ is the length of the binary sequence representing the program p.

Gregory Chaitin proved that Ω is an irrational number smaller than 1 for any C and that no i-length prefix, Ω_i, of the binary sequence representing Ω can be compressed [3], i.e., the length of the shortest program p_{Ω_i} that outputs Ω_i is greater than i itself. As a consequence, the sequence of bits representing Ω, $\{\Omega[k]\}_{k\in\mathbb{N}}$, is not r.e.; for, if this were the case, then there would exist a program p_Ω of length $l = |p_\Omega| \in \mathbb{N}$ such that p_Ω would also generate Ω_{l+1}, a fact contradicting the incompressibility of Ω_{l+1}.

Since $\{\Omega[k]\}_{k\in\mathbb{N}}$ is not r.e., it is not Diophantine either, by DPRM [7, 14]. However, Chaitin proved the following theorem:

Theorem 5.4 ([3])**.** *There exists a family*

$$\chi(k, N, x_1, \ldots, x_\kappa) = 0 \qquad (\S)$$

(indexed by the pairs k, N) of Diophantine equations such that, for each k, there are infinitely many values of N for which equation (§) has a solution if $\Omega[k] = 1$, and only a finite number of values of N for which (§) admits solution if $\Omega[k] = 0$.

From Theorem 5.4 and from the single-fold exponential Diophantine representation of r.e. sets [15], it follows that there exists a family of exponential Diophantine equations

$$\chi^e(k, x_0, x_1, \ldots, x_\kappa) = 0$$

which, for each k, has an overall finite number of solutions if and only if $\Omega[k] = 0$.

So, either every r.e. set admits a finite-fold Diophantine representation, in which case the above result can be strengthened and $\{\Omega[k]\}_{k\in\mathbb{N}}$ can be characterized by discriminating finite- from infinite-foldness of polynomial Diophantine equations, or $\{\Omega[k]\}_{k\in\mathbb{N}}$ could be unspecifiable via finite-foldness of polynomial Diophantine equations, which would indicate a significantly different expressive power between exponential and polynomial Diophantine equations.

Acknowledgements

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

REFERENCES

[1] D. Cantone and E. G. Omodeo. Can a single equation witness that every r.e. set admits a finite-fold Diophantine representation? In P. Felli and M. Montali, editors, *Proceedings of the 33rd Italian Conference on Computational Logic, Bolzano, Italy, September 20-22, 2018.*, volume 2214 of *CEUR Workshop Proceedings*, pages 147–152. CEUR-WS.org, 2018.

[2] D. Cantone and E. G. Omodeo. “One equation to rule them all”, revisited. 2019? In preparation.

[3] G. J. Chaitin. *Algorithmic Information Theory*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1987.

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

[5] M. Davis. An explicit Diophantine definition of the exponential function. *Commun. Pur. Appl. Math.*, XXIV(2):137–145, 1971.

[6] M. Davis. *Lecture Notes in Logic*. Courant Institute of Mathematical Sciences, New York University, 1993.

[7] 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 [24, p. 269ff.].

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

[9] M. D. Davis, R. Sigal, and E. J. Weyuker. *Computability, complexity, and languages – Fundamentals of theoretical computer science*. Computer Science ad scientific computing. Academic Press, 1994.

[10] J. P. Jones and Yu. V. Matijasevič. Register machine proof of the theorem on exponential Diophantine representation of enumerable sets. *The Journal of Symbolic Logic*, 49(3):818–829, 1984.

[11] N. K. Kosovskiĭ. O Diofantovykh predstavleniyakh posledovatel’nosti resheniĭ uravneniya Pellya. *Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR (LOMI)*, 20:49–59, 1971. (Russian. Available in English translation as [12]).

[12] N. K. Kosovskiĭ. Diophantine representation of the sequence of solutions of the Pell equation. *J. of Soviet Mathematics*, 1(1):28–35, 1973. (Translated from [11]).

[13] Yu. V. Matiyasevich. Diofantovost' perechislimykh mnozhestv. *Doklady Akademii Nauk SSSR*, 191(2):279–282, 1970. (Russian. Available in English translation as [14]; translation reprinted in [25, pp. 269–273]).

[14] Ju. V. Matijasevič. Enumerable sets are Diophantine. *Soviet Mathematics. Doklady*, 11(3):354–358, 1970. (Translated from [13]).

[15] 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).

[16] Yu. V. Matiyasevich. *Hilbert's tenth problem*. The MIT Press, Cambridge (MA) and London, 1993.

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

[18] Yu. V. Matiyasevich. Martin Davis and Hilbert's tenth problem. volume 10 of *Outstanding Contributions to Logic*, pages 35–54. Springer, 2016.

[19] Ju. V. Matijasevič. Diophantine representation of the set of prime numbers. *Soviet Mathematics. Doklady*, 12(1):249–254, 1971.

[20] Yu. Matijasevič and J. Robinson. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, XXVII:521–553, 1975. Reprinted in [24, p. 235ff.].

[21] T. Ord and T. D. Kieu. On the existence of a new family of Diophantine equations for Ω. *Fund. Inform.*, 56(3):273–284, 2003.

[22] J. Robinson. Existential definability in arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. Reprinted in [24, p. 47ff.].

[23] J. Robinson. Diophantine decision problems. In W. J. LeVeque, editor, *Studies in Number Theory*, volume 6 of *Studies in Mathematics*, pages 76–116. Mathematical Association of America, 1969.

[24] 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.

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

[26] M. A. Vsemirnov. Diophantine representation of linear recurrences. I. *Journal of Mathematical Sciences*, 89(2):1113–1118, 1998. Originally published, in Russian, in Notes of Scientific Seminars of St. Petersburg Division of Steklov Institute of Mathematics (POMI), 227 (1995), pp. 52–60.

A. A quick account of the reduction, as proposed in [23], of exponentiation to any exponential-growth relation

Suppose that $\mathscr{Q} \subset \mathbb{N} \times \mathbb{N}$ and $\mathscr{S} \subset \mathbb{N} \times \mathbb{N}$ are such that

i) $\mathscr{Q}(w,u)$ implies $u \geqslant w^{w}$,

ii) $w > 1 \,\&\, u \geqslant w^{2w}$ implies $\mathscr{Q}(w,u)$;

iii) $\mathscr{S}(p,q)$ implies $p > 1 \,\&\, q \leqslant p^{p}$,

iv) for each $k \geqslant 0$, there are p and q such that $\mathscr{S}(p,q)$ and $p^{k} < q$.

Then, as we will prove:

$$\begin{array}{rl}
b^{n} = c \iff (\exists a\,,d\,,\ell\,,r\,,v\,,s\,,t) \Big[& (c-1)^{2} + n = 0 \quad \vee \\
& (n \geqslant 1 \,\&\, c + b = 0) \vee \\
\Big(& n \geqslant 1 \;\&\; b \geqslant 1 \;\&\; \mathscr{S}(a,d) \;\&\; d > \ell \qquad \& \\
& \ell^{2} = (a^{2}-1)\,r^{2} + 1 \;\;\&\;\; r = (a-1)\,s + n \;\& \\
& \mathscr{Q}(b+n+1\,,v) \;\;\&\;\; v = 2ab - b^{2} - 1 \qquad \& \\
& a > b+n \;\;\&\;\; v > c \qquad \& \\
& \ell \;=\; (a-b)\,r \;+\; vt \;+\; c \qquad \Big)\Big].
\end{array} \qquad (@)$$

Lemma A.1. *The above bi-implication* (@) *holds if i), ii), iii), and iv) hold.*

Proof. Assuming that $n \geqslant 1 \;\&\; b \geqslant 1$, we must show that $b^{n} = c$ holds if and only if: there are natural numbers a, d, ℓ, r, and $v = 2ab - b^{2} - 1$, such that the conditions $\mathscr{S}(a,d)$, $d > \ell$, $\ell^{2} - (a^{2}-1)\,r^{2} = 1$, $\mathscr{Q}(b+n+1, v)$ hold and, moreover, n is the remainder of the integer division of r by $a-1$ and c is the remainder of the division of $\ell - (a-b)\,r$ by v.

('$\Longleftarrow$'): By means of i), we get $v \geqslant (b+n+1)^{b+n+1} > b^{n}$; by means of iii), $a > 1$ and $\ell < a^{a}$. Thus, since $n \geqslant 1$ implies $r > 0$, we get $\ell = \boldsymbol{x}_{i}(a)$ and $r = \boldsymbol{y}_{i}(a)$ for some i such that $0 < i < a$; therefore—taking the congruence $\boldsymbol{y}_{i}(a) \equiv i \pmod{a-1}$ into account—$i \equiv n \pmod{a-1}$, and hence $i = n$ is the remainder of the division of r by $a-1$. Since $\ell - (a-b)\,r \equiv b^{n} \pmod{v}$—thanks to the congruence $\boldsymbol{x}_{j}(a) - (a-b)\,\boldsymbol{y}_{j}(a) \equiv b^{j} \pmod{2ab - b^{2} - 1}$ holding for all j—and, moreover, $\ell - (a-b)\,r \equiv c \pmod{v}$, $c < v$, $b^{n} < v$, we conclude that $c = b^{n}$ as desired.

(‘$\Longrightarrow$’): Notice that iii) and iv) imply that for every k there exists an infinite sequence

$$\langle p_0 \, , q_0 \rangle \, , \langle p_1 \, , q_1 \rangle \, , \langle p_2 \, , q_2 \rangle \, , \ldots$$

in $\mathbb{N} \times \mathbb{N}$ such that $\mathscr{S}(p_j, q_j)$, $q_j > p_j^k$, and $p_{j+1} > p_j$ hold for every j.[16] Hence we can choose an a so large that: for some d, $\mathscr{S}(a,d)$ and $d > a^{2n}$ holds; $a > n+b$; $\mathscr{Q}(b+n+1 \, , 2ab-b^2-1)$ (to enforce this, by ii), it suffices to pick an a such that $2ab-b^2-1 \geqslant (b+n+1)^{2(b+n+1)})$ and, in consequence of i), $2ab-b^2-1 > b^n$. To satisfy all desired conditions, it will then suffice to take $\ell = \boldsymbol{x}_n(a)$ and $r = \boldsymbol{y}_n(a)$, thanks to the congruence $\boldsymbol{x}_n(a) - (a-b)\,\boldsymbol{y}_n(a) \equiv b^n \pmod{2ab-b^2-1}$.

$\dashv$

In order for $\mathscr{Q}$ to behave as wanted, it suffices to put:[17]

$$\mathscr{Q}(w,u) \quad =_{\text{Def}} \quad (\exists x \, , y) \Big[\quad u \geqslant wx \quad \& \quad x > 1 \qquad \& \\ x^2 - (w^2-1)\,(w-1)^2 y^2 = 1 \quad \Big].$$

Lemma A.2. *As just defined, the Diophantine relation $\mathscr{Q}(w,u)$ satisfies i) & ii).*

Proof. Suppose first that $\mathscr{Q}(w,u)$ holds. From $x > 1$ it follows that $w \notin \{0,1\}$; hence $x = \boldsymbol{x}_n(w)$ & $(w-1)\,y = \boldsymbol{y}_n(w)$ holds for some $n > 0$. Since $\boldsymbol{y}_i(w) \equiv i \pmod{w-1}$ holds for all i, we get $n \equiv 0 \pmod{w-1}$; therefore $n \geqslant w-1$ and, hence, $u \geqslant w\boldsymbol{x}_{w-1}(w) \geqslant w^w$. This proves i).

Suppose next that $w > 1$. By taking $x = \boldsymbol{x}_{w-1}(w)$ and $y = \boldsymbol{y}_{w-1}(w)\,/\,(w-1)$, we easily check that $\mathscr{Q}(w,u)$ holds for every $u \geqslant w\boldsymbol{x}_{w-1}(w)$. Since $\boldsymbol{x}_i(w) < (2w)^i \leqslant w^{2i}$ holds for every $i > 0$, we get $w\boldsymbol{x}_{w-1}(w) < w\,w^{2w-2} < w^{2w}$; therefore, $\mathscr{Q}(w,u)$ holds for every $u \geqslant w^{2w}$. This proves ii). $\dashv$

From Lemma A.2 and Thm A.1, by taking the above implementation of $\mathscr{Q}$—where we replace y by $h+1$—into account, we get straightforwardly:

[16] To choose p_0, q_0 so that $\mathscr{S}(p_0, q_0)$ & $q_0 > p_0^k$, just rely on iv). Inductively, assuming $\mathscr{S}(p_j, q_j)$ & $q_j > p_j^k$, notice that $p_j \neq 0$ & $p_j^{p_j} \geqslant q_j$ holds by iii), hence $p_j > k$ follows; therefore, by choosing p_{j+1} and q_{j+1} so that $\mathscr{S}(p_{j+1}, q_{j+1})$ & $q_{j+1} > p_{j+1}^{p_j}$, we will enforce $q_{j+1} > p_{j+1}^k$; on the other hand, $p_{j+1} \neq 0$ & $p_{j+1}^{p_{j+1}} \geqslant q_{j+1}$, and therefore $p_{j+1} > p_j$.

[17] Notice that for $w \geqslant 2$ the inequality $x > 1$ amounts to the same as $y > 0$. Also notice that if we put $\widehat{Q}(w,y) := (w-1)^3\,(w+1)\,y^2 + 1$, then the equation appearing inside the *definiens* of $\mathscr{Q}$ can be shortened into $\widehat{Q}(w,y) = x^2$, and the polynomial $Q(w,h)$ as specified in the proof of Lemma 3.1 can be rewritten as $\widehat{Q}(w+3, h+1)$.

Corollary A.3. *If $\mathscr{S}$ is a Diophantine relation satisfying iii) & iv), the following rule provides a Diophantine representation of exponentiation:*

$$\begin{array}{lll}
b^n = c \iff (\exists\, a,\, d,\, \ell,\, s,\, x,\, h)\Big[& (c-1)^2+n=0 & \vee\\
& (n \geqslant 1 \,\&\, c+b=0) & \vee\\
& \Big(n \geqslant 1 \ \&\ b\geqslant 1 \ \&\ \mathscr{S}(a,d) \ \&\ d>\ell & \&\\
& \ell^2 = \big(a^2-1\big)\,\big[(a-1)\,s+n\big]^2+1 & \&\\
& x^2 = (b+n)^3\,(b+n+2)\,(h+1)^2+1 & \&\\
& 2ab-b^2-1 \geqslant (b+n+1)\,x & \&\\
& 2ab-b^2-1 > c \ \ \&\ \ a > b+n & \&\\
& 2ab-b^2-1 \mid \ell - \big(a-b\big)\,\big[(a-1)\,s+n\big] - c\Big) & \Big].
\end{array}$$

(Besides a,d,ℓ,s,x,h, one needs one additional existential variable in the right-hand side of this bi-implication in order to eliminate each inequality, plus one more to eliminate the divisibility relator '$|$'. Thanks to the inequality $a-b>0$, we can also get rid of ℓ, thus reducing the number of existential variables to 12.)

B. Davis's reduction of $b^n = c$ to the relation $r = \boldsymbol{y}_n(a)$

The following crucial link between exponentiation and the sequence $\langle \boldsymbol{y}_i(a)\rangle_{i\in\mathbb{N}}$ was pointed out in [5] and explained at length, again, in [6]:

$$\begin{array}{rr}
b \geqslant 1 \implies \Big[\ b^n = c \iff (\exists\, t,\, a,\, \ell,\, r,\, h)\Big(& r = \boldsymbol{y}_n(a) \ \ \&\\
& \ell^2 - (a^2-1)\,r^2 = 1 \ \ \&\\
& t > b \ \ \&\ \ t > n \ \ \&\\
& (t^2-1)\,(t-1)^2\,(h+1)^2+1 = a^2 \ \ \&\\
& c < 2ab-b^2-1 \ \ \&\\
& c \equiv \ell-(a-b)\,r \ (\bmod\ 2ab-b^2-1\,) \quad \Big)\Big].
\end{array}$$

Specifically, when $b \geqslant 1$ and $b^n = c$, the constraints here appearing in the scope of $\exists$ can be satisfied in infinitely many ways: for, corresponding to any $t > n \max b$, it suffices to put $a = \boldsymbol{x}_{t-1}(t)$ in order to be able to determine the values of ℓ, r, and h uniquely (see Lemma B.1 below).

In light of the above biimplication, if we now provided a Diophantine representation of the relation $r = \boldsymbol{y}_n(a)$, we would readily get that the relation $b^n = c$ is also Diophantine.

Let us recall here the proof of the above-stated relationship between exponentiation and the Pell equation. We begin with the proposition:

Lemma B.1. *If $b \geqslant 1$ and $b^n = c$, then to each number of the form $a = \boldsymbol{x}_{(s+1)\,(t-1)}(t)$ with $t > b \max n$ there correspond uniquely values ℓ, r, h such that the following conditions are met: $r = \boldsymbol{y}_n(a)$, $\ell = \boldsymbol{x}_n(a)$, $c < 2ab - b^2 - 1$, $c \equiv \ell - (a-b)\,r \ (\bmod\ 2ab - b^2 - 1)$, and $a^2 - (t^2-1)\,(t-1)^2\,(h+1)^2 = 1$.*

Proof. Observe that, since $t > b \geqslant 1$, the Pell equation $x^2 - (t^2-1)\,y^2 = 1$ has the usual infinite sequence $\langle\langle \boldsymbol{x}_i(t)\,, \boldsymbol{y}_i(t)\rangle\rangle_{i\in\mathbb{N}}$ of solutions; therefore, it makes sense to put $a := \boldsymbol{x}_{(s+1)\,(t-1)}(t)$. In its turn $a > 1$ holds, because $\boldsymbol{x}_{(s+1)\,(t-1)}(t) \geqslant \boldsymbol{x}_1(t) > 1$; hence it makes sense to put $r := \boldsymbol{y}_n(a)$ and $\ell := \boldsymbol{x}_n(a)$.

Plainly, $a \geqslant \boldsymbol{x}_{t-1}(t) \geqslant t^{t-1} > b^n$; hence it is easy to see that the inequality $b^n < 2ab - b^2 - 1$ is satisfied[18] when $n > 0$. The same inequality holds when $n = 0$, as it follows from $a \geqslant t^{t-1} \geqslant t > b \geqslant 1$.

The last two conditions in the claim simply state well-known congruences that are satisfied (as recalled in Fig. 2) by the solutions of any Pell equation of the special form being considered here. In particular,

$$c \equiv \ell - (a-b)\,r \ (\ \bmod\ 2ab - b^2 - 1\ )$$

states that

$$b^n \equiv \boldsymbol{x}_n(a) - (a-b)\,\boldsymbol{y}_n(a)\ (\ \bmod\ 2ab - b^2 - 1\ ). \qquad (\circ)$$

As for $a^2 - (t^2-1)\,(t-1)^2\,(h+1)^2 = 1$, it merely expresses that $\boldsymbol{y}_{(s+1)\,(t-1)}(t)$ is a non-null multiple of $t-1$—; recall, in fact, that $a = \boldsymbol{x}_{(s+1)\,(t-1)}(t)$ and $t - 1 > 0$, and that the congruence $\boldsymbol{y}_i(t) \equiv i\ (\bmod\ t-1)$ holds in general, for every i. ⊣

We next come to the converse of Lemma B.1:

Lemma B.2. *Suppose that $b \geqslant 1$ and that the conditions*

$$\begin{array}{l} c \leqslant 2ab - b^2 - 1, \\ c \equiv \ell - (a-b)\,r\ (\ \bmod\ 2ab - b^2 - 1\ ) \\ \ell^2 - (a^2-1)\,r^2 = 1 \\ a^2 - (t^2-1)\,(t-1)^2\,(h+1)^2 = 1 \\ t > b \max n, \end{array}$$

[18] Here, as we will again do in the proof of Lemma B.2, we are making use of the following fact (which gets easily proven even for a real number b): *If $n > 0$, $b \geqslant 1$, and $a > b^n$ (with $a, n \in \mathbb{N}$), then $2ab - b^2 - 1 > b^n$.*

are satisfied by a, ℓ, r, t, and h, where n is the value ensuring that $r = \boldsymbol{y}_n(a)$. Then $b^n = c$ holds.

Proof. Since $t > b \geqslant 1$, the Pell equation $x^2 - (t^2 - 1)y^2 = 1$ has the usual infinite sequence $\langle\langle \boldsymbol{x}_i(t), \boldsymbol{y}_i(t)\rangle\rangle_{i \in \mathbb{N}}$ of solutions; thus, since $a^2 - (t^2 - 1)y^2 = 1$ holds for some $y > 0$, we have $a = \boldsymbol{x}_j(t)$ for some j, where $j > 0$—since $a \geqslant t$—and $\ell = \boldsymbol{x}_n(a)$, $r = \boldsymbol{y}_n(a)$ holds for a suitable n. Consequently $2ab - b^2 - 1 \geqslant 2$; moreover, by the well-known congruence ($\circ$) recalled above, we have

$$c \equiv b^n \pmod{2ab - b^2 - 1},$$

whence the sought equality will follow if we manage to prove that the side b^n of this congruence is smaller than $2ab - b^2 - 1$ (for, $c \leqslant 2ab - b^2 - 1$ is an explicit assumption and $b^n \geqslant 1$). Since this is obvious when $n = 0$, we will assume $n > 0$.

To see that $b^n < 2ab - b^2 - 1$, we argue as follows. Clearly $\boldsymbol{y}_j(t) = (t - 1)(h + 1)$ holds, whence $(t - 1)(h + 1) \equiv j \pmod{t - 1}$, i.e. $t - 1 \mid j$, follows. Since $j \neq 0$, we get $j \geqslant t - 1$, and therefore $a = \boldsymbol{x}_j(t) \geqslant t^j \geqslant t^{t-1} > b^n$. The sought inequality follows, which completes the proof. ⊣ ⊣

Corollary B.3. *Put* $Q(w,h) \;:=\; (w+2)^3 (w+4)(h+1)^2 + 1$. *Then,*

$$\begin{aligned} b^n = c \iff (\exists a, \ell, r, j, h)\Big[\; & (c-1)^2 + b + n = 0 \;\vee\; (n \geqslant 1 \;\&\; c + b = 0) \quad \vee \\ & \Big(b \geqslant 1 \;\&\; r = \boldsymbol{y}_n(a) \quad \& \\ & \ell^2 = (a^2 - 1)r^2 + 1 \;\&\; Q(b + j - 2, h) = a^2 \;\& \\ & 2ab - b^2 - 1 \geqslant c \quad \& \quad b + j \geqslant n \quad \& \\ & c \equiv \ell - (a - b)r \pmod{2ab - b^2 - 1}\Big)\Big]. \end{aligned}$$

Proof. Suppose first that there are a, ℓ, r, j, h satisfying the conditions in the scope of '$\exists$', and that $b \geqslant 1$. By putting $t := b + j + 1$, we obviously get $t > b \max n$ and $a^2 - (t^2 - 1)(t - 1)^2(h + 1)^2 = 1$, so that $b^n = c$ holds by Lemma B.2.

Conversely, suppose that $b^n = c$ holds, where $b \geqslant 1$. Put $t := b + n + 1$, $j := n$, and $a := \boldsymbol{x}_{t-1}(t)$. Then, by Lemma B.1, unique values ℓ, r, h exist satisfying all conditions that appear in the third disjunct of the scope of '$\exists$' in the claim. ⊣ ⊣

C. Representing exponentiation as an integer quotient

In the ongoing, in order to prove that

$$b^n = c \quad \Longleftrightarrow \quad c = \quad \left\lfloor \frac{\mathbf{y}_{n+1}(\,8\,b\,(n+1)\,\mathbf{y}_{n+1}(b+1)+2\,)}{\mathbf{y}_{n+1}(\,8\quad(n+1)\,\mathbf{y}_{n+1}(b+1)\qquad)} \right\rfloor ,$$

we will proceed to show, for b and n natural numbers, that

$$b^n \quad = \quad \lim_{x\to\infty} \frac{\mathbf{y}_{n+1}(bx+2)}{\mathbf{y}_{n+1}(x)} \, ;$$

this, in the light of the corollary which follows, will give us

$$b^n \quad = \quad \lfloor \mathbf{y}_{n+1}(bx+2)\ /\ \mathbf{y}_{n+1}(x) \rfloor \qquad (*)$$

where x is a natural number sufficently large to reduce the distance between b^n and $\mathbf{y}_{n+1}(bx+2)\ /\ \mathbf{y}_{n+1}(x)$ to an amount less than 1. We will carefully assess how to take the value of x big enough. Our treatment adheres closely to [16, pp. 31–32].

We begin by recalling, from fact 1 of Fig. 2:

Lemma C.1. *For $a \geqslant 2$ and $i \in \mathbb{N}$, the following inequalities hold:*

$$(2a-1)^i \quad \leqslant \quad \mathbf{y}_{i+1}(a) \quad \leqslant \quad (2a)^i \ .$$

Here the increase on the left is strict when $i > 0$; on the other side, when $i > 1$.

Corollary C.2. *For $b, n, x \in \mathbb{N}$ with $x \geqslant 2$,*

$$\frac{\mathbf{y}_{n+1}(bx+2)}{\mathbf{y}_{n+1}(x)} \quad \geqslant \quad b^n \, .$$

Proof. Thanks to Lemma C.1, we have

$$\frac{\mathbf{y}_{n+1}(bx+2)}{\mathbf{y}_{n+1}(x)} \quad \geqslant \quad \frac{(2bx+3)^n}{(2x)^n} \quad \geqslant \quad \frac{(2bx)^n}{(2x)^n} \quad = \quad b^n \, .$$

⊣

Assessment of a value of x which fits our needs (cf. [16, p. 32]):

$$\frac{\mathbf{y}_{n+1}(bx+2)}{\mathbf{y}_{n+1}(x)} \begin{cases} = \quad 1 & \text{for} \quad b=0 \qquad \text{and} \quad x \geqslant 2\,; \\ < \quad \frac{4^n}{(2x-1)^n} \quad < \quad 1 & \text{for} \quad b=0<n \quad \text{and} \quad x>2\,; \\ \leqslant \quad b^n\left(1+\frac{16n}{2x}\right) & \text{for} \quad b>0<n \quad \text{and} \quad x>8n\,. \end{cases}$$

Thus (*) becomes true as soon as $x \geqslant 8\,(n+1)\,(b+1)^n$; we can, e.g., enforce it by putting $x := 8\,(n+1)\mathbf{y}_{n+1}(b+1)$, thus getting the formulation of $b^n = c$ shown at the beginning of this appendix.

D. CANTONE
Dept. of Mathematics and Computer Science
University of Catania, Italy
e-mail: `domenico.cantone@unict.it`

A. CASAGRANDE
Dept. of Mathematics and Geosciences
University of Trieste, Italy
e-mail: `acasagrande@units.it`

F. FABRIS
Dept. of Mathematics and Geosciences
University of Trieste, Italy
e-mail: `ffabris@units.it`

E. G. OMODEO
Dept. of Mathematics and Geosciences
University of Trieste, Italy
e-mail: `eomodeo@units.it`