A Brief History of Singlefold Diophantine Definitions

Domenico Cantone[1,*,†], Luca Cuzziol[*,†] and Eugenio G. Omodeo[2,*,†]

[1]University of Catania, DMI, viale Andrea Doria, 6, I-95125 Catania, Italy
[2]University of Trieste, DMG, via Alfonso Valerio 12/1, I-34127 Trieste, Italy

To the memory of Martin
(March 8, 1928 – January 1, 2023)

Abstract

Consider an $(m+1)$-ary relation $\mathcal{R}$ over the set $\mathbb{N}$ of natural numbers. Does there exist an arithmetical formula $\varphi(a_0, \ldots, a_m, x_1, \ldots, x_\kappa)$, not involving universal quantifiers, negation, or implication, such that the representation and univocity conditions, viz.,

$$\mathcal{R}(\vec{a}) \iff \exists x_1 \cdots \exists x_\kappa \, \varphi(\vec{a}, x_1, \ldots, x_\kappa) \quad \text{and}$$
$$\exists x_1 \cdots \exists x_\kappa \, \forall y_1 \cdots \forall y_\kappa \left[\varphi(\vec{a}, y_1, \ldots, y_\kappa) \implies \&_{i=1}^{\kappa} (y_i = x_i) \right],$$

are met by each tuple $\vec{\boldsymbol{a}} = \langle \boldsymbol{a}_0, \ldots, \boldsymbol{a}_m \rangle \in \mathbb{N}^{m+1}$?

A priori, the answer may depend on the richness of the language of arithmetic: Even if solely addition and multiplication operators (along with the equality relator and with positive integer constants) are adopted as primitive symbols of the arithmetical signature, the graph $\mathcal{R}$ of any primitive recursive function is representable; but can representability be reconciled with univocity without calling into play one extra operator designating either the dyadic operation $\langle b\,,\ n \rangle \mapsto b^n$ or just the monadic function $n \mapsto \boldsymbol{b}^n$ associated with a fixed integer $\boldsymbol{b} > 1$? As a preparatory step toward a hoped-for positive answer to this question, one may consider replacing the exponentiation operator by a dyadic relator designating an exponential-growth relation (a notion made explicit by Julia Bowman Robinson in 1952).

We will discuss the said univocity, aka 'single-fold-ness', issue—first raised by Yuri V. Matiyasevich in 1974—, framing it in historical context.

MS Classification 2020: 03D25, 11D25

Keywords

Hilbert's 10th problem, exponential-growth relation, single/finite-fold Diophantine representation, Pell's equation

1. Introduction

The notions of being listable, exponential Diophantine, and polynomial Diophantine were proved, in the decade 1960/1970, to capture the same family of relations on the set $\mathbb{N}$ of natural

CILC 2023: 38th Italian conference on Computational Logic, June 21–23, 2023, Udine
*Corresponding author.
†These authors contributed equally.
domenico.cantone@unict.it (D. Cantone); lucacuzz95@gmail.com (L. Cuzziol); eomodeo@units.it (E. G. Omodeo)
https://www.dmi.unict.it/cantone/ (D. Cantone)
0000-0002-1306-1166 (D. Cantone); 0000-0002-2759-6102 (L. Cuzziol); 0000-0003-3917-1942 (E. G. Omodeo)

numbers (see [1, 2]). Listability had been characterized mathematically decades earlier in various equivalent manners (we will recall one in Sec. 4); the other two notions can be characterized through arithmetical formulae concerning $\mathbb{N}$. To be specific, consider an arithmetic that offers constants denoting $0, 1, 2$ and maybe other positive integers, variables ranging over $\mathbb{N}$, operators designating addition, multiplication, and exponentiation, and the equality relator; then:

Definition 1. *A relation $\mathcal{D} \subseteq \mathbb{N}^{m+1}$ on natural numbers is called* [POLYNOMIAL] DIOPHANTINE *if there are arithmetical terms D' and D'' involving variables, $a_0, \ldots, a_m, x_1, \ldots, x_\kappa$, constants, and the addition and multiplication operators, such that the biimplication*[1]

$$\langle \boldsymbol{a}_0, \ldots \boldsymbol{a}_m \rangle \in \mathcal{D} \iff \exists\, x_1 \cdots \exists\, x_\kappa \; D'(\boldsymbol{a}_0, \ldots, \boldsymbol{a}_m, x_1, \ldots, x_\kappa) = D''(\boldsymbol{a}_0, \ldots, \boldsymbol{a}_m, x_1, \ldots, x_\kappa)$$

holds for all $\boldsymbol{a}_0, \ldots \boldsymbol{a}_m$ in $\mathbb{N}$. If also exponentiation—with variables in the exponent—is allowed to occur in D' and D'', then $\mathcal{D}$ is said to be EXPONENTIAL DIOPHANTINE.

A function f from $\mathbb{N}^m$ to $\mathbb{N}$ is termed likewise if its GRAPH, *namely the relation $\{\langle a_1, \ldots, a_m,\, a_0\rangle \,:\, f(a_1, \ldots, a_m) = a_0\}$ is Diophantine or, resp., exponential Diophantine.*

A valid biimplication of the form just shown is called a *Diophantine representation* (resp., an *exponential Diophantine representation*) of $\mathcal{D}$. Any listable relation admits an exponential Diophantine representation, as was first proved in [1]: this celebrated result, known as the Davis-Putnam-Robinson (or just *DPR*) theorem, underwent two improvements with respect to its original statement which we will now recall. In [3], Martin D. Davis managed to bring exponential specifications to the more generic format[2]

$$\vec{\boldsymbol{a}} \in \mathcal{D} \iff \exists\, u\, \exists\, v\, \exists\, \vec{x}\, [\, D(\vec{\boldsymbol{a}}, \vec{x}, u) = 0 \;\&\; \mathscr{J}(u\,,\, v)\,]\,,$$

where D is a polynomial (multivariate, with coefficients in $\mathbb{Z}$), hence devoid of exponentiation, while exponentiation is superseded by any fixed EXPONENTIAL-GROWTH RELATION (a notion that Julia Robinson proposed in [4] and slightly improved in [5]), i.e., a relation $\mathscr{J}$ such that

$$\begin{array}{rcl} \forall\, u\, \forall\, v \big[\, \mathscr{J}(u\,,\, v) & \implies & v \leqslant u^u \;\&\; u > 1 \,\big] \quad \text{and} \\ \forall\, \ell\, \exists\, u\, \exists\, v \big[\, \mathscr{J}(u\,,\, v) & \;\&\; & u^\ell < v \,\big]\,. \end{array} \tag{†}$$

In [6], Yuri V. Matiyasevich managed to bring exponential representations to the format[3]

$$\vec{\boldsymbol{a}} \in \mathcal{D} \iff \exists\, u\, \exists\, v\, \exists\, \vec{x}\, [\, D(\vec{\boldsymbol{a}}, \vec{x}, u) = 0 \;\&\; 2^u = v\,]\,,$$

where D is a polynomial, while ensuring single-fold-ness, henceforth dubbed UNIVOCITY, that is: *there is at most one solution to the constraint $D(\vec{\boldsymbol{a}}, \vec{x}, u) = 0 \;\&\; 2^u = v$, for any $\vec{\boldsymbol{a}}$.*

Now and then our focus will zoom in on FINITE-FOLD specifications, which are the ones admitting at most a finite number of solutions for each tuple $\vec{\boldsymbol{a}}$ of actual parameters.

Examples of exponential-growth relations are:

$$\mathscr{E}_1 = \big\{\, \langle u\,,\, 2^u\rangle \,:\, u \in \mathbb{N} \setminus \{0, 1\} \,\big\} \quad \text{and} \quad \mathscr{E}_2 = \big\{\, \langle u\,,\, F_{2\,u}\rangle \,:\, u \in \mathbb{N} \setminus \{0, 1\} \,\big\}\,,$$

[1] Bold symbols often differentiate, henceforth, actual from formal parameters; to wit, values from variables.
[2] Here and below, $\vec{\boldsymbol{a}}$ and $\vec{x}$ shorten $\boldsymbol{a}_0, \ldots, \boldsymbol{a}_m$ and $x_1, \ldots, x_\kappa$, respectively.
[3] Or even to the more elegant format $\vec{\boldsymbol{a}} \in \mathcal{D} \iff \exists\, u\, \exists\, \vec{x}\, [\, D(\vec{\boldsymbol{a}}, \vec{x}) = 4^u + u\,]$, see also [7, pp. 137–138].

where F is the Fibonacci progression defined by the recurrence $F_0 = 0\,,\ F_1 = 1\,,$ and $F_{i+2} = F_i + F_{i+1}$ for $i \in \mathbb{N}$. The relation $\mathscr{E}_1$ suggests the feasibility of an amalgamation—nowhere described in the literature, as far as the authors know—between the cited results of [3] and [6]; as for $\mathscr{E}_2$, it was precisely by exhibiting a polynomial Diophantine representation of it that Matiyasevich revealed the existence of an alike representation of exponentiation itself [2]. Aiming at unearthing the sought amalgamation, we will closely examine (see Sec. 6) Davis' and Matiyasevich's said reductions.

Polynomial Diophantine univocity—or, at worse, finitefold-ness—is the true challenge; this is why we also seek a relation that can play, in this respect, a role analogous to $\mathscr{E}_2$: a relation $\mathscr{M}$ which in addition to satisfying exponential growth, as well as any other requirements that might emerge from the amalgamated theorem (a potential such requirement is tagged (‡) in Sec. 7) admits a finite-fold, hopefully univocal, polynomial specification. After a suggestion provided by [8] (and then reiterated in [9, 10]), in Sec. 8 we candidate for such a role six relations associated with six special quaternary quartic equations, at least one of which we should prove to have only finitely many solutions—which, quite regrettably, we have been unable to do so far.

The paper is organized as follows. Sec. 2 illustrates, through a gallery of short examples, which kind of relations on $\mathbb{N}$ can be represented univocally by means of Diophantine polynomials without resorting to overly sophisticated tools. It is contended that when univocity does not come for free, it can be built into such a representation by insertion of clauses that insist on the minimality of the values to be assigned to the "unknowns" $x_1, \ldots, x_\kappa$; minimality can be enforced by means of bounded universal quantifiers, but can these quantifiers be recast just in terms of addition, multiplication, and existential quantification? Sec. 3 shows that a number-theoretic construct somehow related to bounded universal quantification does, in fact, admit a univocal *exponential* Diophantine representation: the construct we are referring to is the function $p(a, b, c) = \prod_{k=1}^{c}(a + b \cdot k)$, and clues about its kinship to bounded universal quantification are deferred to a later section. Sec. 4 digresses into presenting a special format, known as the *Davis normal form*, which can be used to represent the graph of any primitive recursive function. This is, in essence, a technique for specifying any listable relation in a manner that seemingly deviates from a Diophantine representation, as it involves one bounded universal quantifier. Sec. 4 also recaps a variant of the Davis normal form, enforcing univocity, derived by Yu. Matiyasevich from his momentous finding that every listable relation is Diophantine. All prerequisites are ripe enabling us to produce, in Sec. 5, a univocal exponential representation of any Diophantine—hence of any listable—relation $\mathcal{D}$, through reduction of the bounded universal quantifier to the said construct $p(a, b, c)$. At this point one of Matiyasevich's variants, embodying univocity, of the DPR theorem has been reached; in Sec. 6 we recall a more refined one, in which exponentiation is relegated, within a representation of $\mathcal{D}$, into a single literal of the form $2^u = v$. Two questions are then raised in Sec. 7: Could a suitable condition $\mathscr{M}(u, v)$ supersede this literal in the general representation scheme? And also: Can we manage to place a finite-fold Diophantine relation $\mathscr{M}(u, v)$ in this role? The truly original part of this paper is Sec. 8, where we review the entire catalog of our candidate $\mathscr{M}$'s.

2. Sampler of Univocal (or Nearly so) Diophantine Specifications

Let us start with motivating examples of univocal (polynomial first, then exponential) Diophantine specifications of various relations over $\mathbb{N}$. Before doing so, we observe that Diophantine relations can safely be nested one inside another; moreover, we can unconditionally admit the conjunction connective '$\&$' in the specification language, in view of the equivalence

$$\begin{aligned}&\big[\exists\,\vec{x}\;\; P'(\vec{a},\vec{x}) = P''(\vec{a},\vec{x})\big]\;\;\&\;\;\big[\exists\,\vec{y}\;\; Q'(\vec{b},\vec{y}) = Q''(\vec{b},\vec{y})\big]\quad\Longleftrightarrow\\ &\quad\exists\,\vec{x}\,\exists\,\vec{y}\,\big[P'(\vec{a},\vec{x})^2 + P''(\vec{a},\vec{x})^2 + Q'(\vec{b},\vec{y})^2 + Q''(\vec{b},\vec{y})^2 = 2\cdot\big(P'(\vec{a},\vec{x})\cdot P''(\vec{a},\vec{x}) + Q'(\vec{b},\vec{y})\cdot Q''(\vec{b},\vec{y})\big)\big].\end{aligned}$$

While these broadenings of the specification language do not affect univocity, the disjunction connective can be brought into play but should be handled with care: simple-minded use of the rewriting rule $P' = P''\;\vee\;Q' = Q''\;\rightsquigarrow\;P'\cdot Q' + P''\cdot Q'' = P'\cdot Q'' + P''\cdot Q'$ might, in fact, endanger univocity. E.g., restating $a = 0\;\vee\;\exists\,x\;b = x+1$ as $\exists\,x\;a\cdot b = a\cdot(x+1)$ would not work, because x could take any value in $\mathbb{N}$ when $a = 0$; this violation of univocity can easily be cured, though: we can overload the first disjunct with the requirement $x = 0$ before eliminating the propositional connectives, thus getting $\exists\,x\;\;(a+x)\cdot b = (a+x)\cdot(x+1)$.

Using '$\coloneqq$' to mean "stands for", we now provide the specifications of some basic relations among which divisibility, '$\mid$', coprimality, '$\perp$', and the graphs of integer quotient '$\div$' and remainder operation '$\%$':

$$\begin{array}{rcl@{\qquad}rcl}
a\in\varnothing & \coloneqq & a = a+1\,; & a\in\{b_0,\ldots,b_\ell\} & \coloneqq & \bigvee_{i\leqslant\ell} a = b_i\,;\\
a\leqslant b & \coloneqq & \exists\,x\;a+x = b\,; & a < b & \coloneqq & a+1\leqslant b\,;\\
a\neq b & \coloneqq & 2\cdot a\cdot b < a^2+b^2\,; & q = \square & \coloneqq & \exists\,x\;x^2 = q\,;\\
d\neq\square & \coloneqq & \exists\,x\,(x^2 < d\;\;\&\;\;d\leqslant x^2+2\cdot x)\,; & & & \\
b_1\max b_2 = a & \coloneqq & a\in\{b_1,b_2\}\;\;\&\;\;b_1\leqslant a\;\;\&\;\;b_2\leqslant a\,; & & & \\
b\div a = q & \coloneqq & \exists\,r\,\big(a\cdot q+r = b\;\;\&\;\;r < a\big)\,; & b\,\%\,a = r & \coloneqq & \exists\,q\,\big(a\cdot q+r = b\;\;\&\;\;r < a\big)\,;\\
a\perp b & \coloneqq & \exists\,x_1\,\exists\,x_2\,\exists\,y_1\,\exists\,y_2\,\big(x_1\cdot a+y_1\cdot b = x_2\cdot a+y_2\cdot b+1\big)\,; & & & \\
a\nmid b & \coloneqq & \exists\,q\,\exists\,r\,\big(a\cdot q+r+1 = b\;\;\&\;\;r+1 < a\big)\,; & & & \\
a\mid b & \coloneqq & \exists\,q\;a\cdot q = b\,; & s\equiv r\mod p & \coloneqq & p\mid\pm(s-r)\,.
\end{array}$$

Among these, the specifications lacking univocity are the ones of '$\mid$' (insofar as $a\cdot q = b$ holds for any q when $a = b = 0$), of 'mod' (unless one imposes $p\neq 0$), and of '$\perp$'. To fix them, put:

$$a\perp b\;\;\coloneqq\;\;\exists\,x\,\exists\,y\,\big(a^2x^2+1 = b^2y^2+2\cdot a\cdot x\;\;\&\;\;x < b\big)\,;\qquad a\mid b\;\;\coloneqq\;\;(a+b)\cdot(b\,\%\,a) = 0\,.$$

The former states that the equation $a\,x\pm b\,y = 1$ has a solution (necessarily unique) such that $x < b$; the definiens of the latter is plainly rewritable in primitive symbols, retaining univocity.

Generally speaking, univocity can be enforced in an existential definition that lacks it by insisting on the minimality of the values assigned to the existential variables, but this brings into play bounded universal quantifiers;[4] and it is far from obvious (see Sec. 5 below) how these can be disempowered into arithmetical constructs. As

[4] Bounded quantifiers can be introduced as usual; in particular: $\forall\,v\leqslant w\;\;\varphi\;\;\coloneqq\;\;\forall\,v\,(v\leqslant w\implies\varphi)$ and $\exists\,v\leqslant w\,\varphi\;\;\coloneqq\;\;\exists\,v\,(x\leqslant y\;\;\&\;\;\varphi)$.

an illustration of this point, consider the following Diophantine specification (alternative to the one proposed above) of the property of <u>not</u> being a perfect square:

$$d \neq \square \quad \coloneqq \quad \exists\, x\, \exists\, y\, \exists\, z\, \big[\, x^2 = d \cdot (y+1)^2 + 1 \;\;\&\;\; d = z + 1 \,\big] .$$

The theory of Pell equations (see, e.g., [11, Sec. 3.4]) ensures the correctness of this characterization; however, the number of solving triples is infinite for each non-square number and it is daredevil to introduce univocity by reformulating the definiens as

$$\exists\, x\, \exists\, y\, \exists\, z\, \big[\quad x^2 = d \cdot (y+1)^2 + 1 \;\;\&\;\; d = z + 1 \;\;\&\;\; \quad \forall\, x' < x\, \forall\, y' < y\, \big(x'^2 \neq d \cdot (y'+1)^2 + 1\big) \quad \big] .$$

3. Sampler of Univocal Exponential Diophantine Specifications

Suppose now that an exponentiation operator is adopted as a primitive arithmetical construct, along with a symbol designating the integer value 2. Then addition and multiplication can be viewed as derived constructs and no other constant m is essential (since $m = 1 + \cdots + 1$), as the following univocal exponential Diophantine specifications make evident:

$$\begin{array}{rrcl}
 & a = 0 & \coloneqq & \exists\, t\, \exists\, u\, \big(u^a = t = 2^a \;\;\&\;\; 2^t = u\big) ; \\
 & a = 1 & \coloneqq & \exists\, t\, \exists\, u\, \exists\, v\, \big(2^a = t = 2^u \;\;\&\;\; 2^v = t \;\;\&\;\; u^v = a\big) ; \\
 & a \cdot b = c & \coloneqq & \exists\, x\, \exists\, y\, \big(2^a = x \;\;\&\;\; 2^c = y \;\;\&\;\; x^b = y\big) ; \\
 & a + b = c & \coloneqq & \exists\, u\, \exists\, v\, \exists\, w\, \big(2^a = u \;\;\&\;\; 2^b = v \;\;\&\;\; 2^c = w \;\;\&\;\; u \cdot v = w\big), \\
\text{i.e.,} & a + b = c & \coloneqq & \exists\, u\, \exists\, v\, \exists\, w\, \exists\, x\, \exists\, y\, \big(2^a = u \;\;\&\;\; 2^b = v \;\;\&\;\; 2^c = w \;\;\&\;\; 2^u = x \;\;\&\;\; 2^w = y \;\;\&\;\; x^v = y\big) .
\end{array}$$

It is an easy task to figure out from the above table the following fact, that states more explicitly—and enhances with univocity—what is observed in [1, p. 427]:

Lemma 1. *Any exponential Diophantine specification* $\exists\, x_1 \cdots \exists\, x_\kappa\; \varphi(a_0, \ldots, a_m, x_1, \ldots, x_\kappa)$, *whose matrix* φ *is devoid of quantifiers and only involves the logical connectives* $=$, $\&$, $\vee$, *can be recast as*

$$\exists\, x_1 \cdots \exists\, x_\kappa\, \exists\, y_0 \cdots \exists\, y_\ell\, \big[\, y_0 = 2 \;\;\&\;\; \&_{\,i \leqslant s}\, b_i^{n_i} = c_i \,\big] ,$$

where $b_0, \ldots, b_s, n_0, \ldots, n_s, c_0, \ldots, c_s$ *are variables drawn from the set* $\{a_0, \ldots, a_m, x_1, \ldots, x_\kappa, y_0, \ldots, y_\ell\}$, *and where* b_i, n_i, c_i *are distinct signs for each* i.

If the source specification is univocal, so is the "flattened" one resulting from this recasting. ⊣

Very early on [4, pp.446–447], J. Robinson noted that binomial coefficient and factorial function are existentially definable in terms of exponentiation. The following univocal specifications are reminiscent of hers, but we rely, as for the factorial, on the modernized variant provided in [11, pp. 145–146]. The well-known binomial theorem justifies the first specification recalled here:

$$\tbinom{\ell}{i} = a \;\coloneqq\; \exists\, u\, \big[a = \big((u+1)^\ell \div u^i\big) \,\%\, u \;\;\&\;\; u = 2^\ell + 1\big] ; \quad j! = a \;\coloneqq\; a = \left[\left((2\,j)^j\right)^j \div \binom{(2\,j)^j}{j}\right] .$$

Constructs more general than $c!$ are the *falling factorial* $\prod_{k<c}(a-k)$ with $a \geqslant c$, and the related *raising factorial* $\prod_{k=1}^{c}(a+k)$. Concerning an even more general construct, we have:

Lemma 2 (Originating from [12, Lemma 2.2]—Enhanced, here, with univocity)**.** *Given a, b, c, d, the relationship*

$$\prod_{k=1}^{c}(a + b \cdot k) \quad = \quad d$$

*holds if and only if there exist—**and are uniquely determined**—m, p, q, r, s, t such that*

$$\Big(b \cdot c = 0 \ \&\ d = a^c \ \&\ m = p = q = r = s = t = 0\Big) \ \vee \ \Big[b \cdot c = t + 1 \ \&\ m = b \cdot (a + b \cdot c)^c + 1 \ \&\ b \cdot q = a + m \cdot p \ \&\ \Big[b^c \cdot c! \binom{q+c}{c}\Big] \,\%\, m = d \ \&\ \big[(q + r + 1 = m \ \&\ s = 0) \ \vee \ (q = m + r \ \&\ p + s + 1 = b)\big]\Big].$$

Proof. The first disjunct, regarding the case $b = 0 \ \vee \ c = 0$, does not deserve explanation; the second refines the existential specification of $\prod_{k=1}^{c}(a + b\,k)$,

$$\exists\, m\, \exists\, q\, \exists\, p \left(m = b\,(a + b\,c)^c + 1 \ \&\ b\,q = a + m\,p \ \&\ \left[b^c\,c! \binom{q+c}{c}\right] \,\%\, m = d\right),$$

proved in [11, pp. 147–149] for the case $b > 0 \ \&\ c > 0$. That specification leaves p and q under-determined; we are now ensuring univocity by indicating that if one tried to assign a smaller value to q, then either the value of q itself or the corresponding value of p would turn out to be negative. ⊣

In Sec. 4, we will exploit three computable functions admitting univocal exponential specifications; they are an injection from $\mathbb{N}^2$ onto $\mathbb{N}$ and its associated projections (see [13, Sec. 3.8]):

$$\begin{array}{rcl} \varpi(a\,,\,b) = c & \coloneqq & 2^a\,(2\,b+1) \ = \ c+1\,; \\ \lambda(c) = a & \coloneqq & 2^a \mid c+1 \ \ \& \ \ 2^{a+1} \nmid c+1\,; \\ \rho(c) = b & \coloneqq & \exists\, x \ \ 2^x\,(2\,b+1) \ = \ c+1\,. \end{array}$$

These definitions yield, for all $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{N}$, that:

$$\begin{array}{rcl} \varpi(\boldsymbol{a}\,,\,\boldsymbol{b}) = \boldsymbol{c} & \iff & \lambda(\boldsymbol{c}) = \boldsymbol{a} \ \&\ \rho(\boldsymbol{c}) = \boldsymbol{b}\,, \\ \boldsymbol{a} < \boldsymbol{a'} \ \&\ \boldsymbol{b} < \boldsymbol{b'} & \implies & \varpi(\boldsymbol{a}\,,\,\boldsymbol{b}) < \varpi(\boldsymbol{a'}\,,\,\boldsymbol{b}) \ \&\ \varpi(\boldsymbol{a}\,,\,\boldsymbol{b}) < \varpi(\boldsymbol{a}\,,\,\boldsymbol{b'})\,. \end{array}$$

4. Listable Sets and the Davis Normal Form

Intuitively speaking, a set $\mathscr{R} \subseteq \mathbb{N}^{m+1}$ is *listable* if there is an effective procedure for making a list (with repetition allowed) of the elements of $\mathscr{R}$. Computability theory provides the notion of RECURSIVELY ENUMERABLE (R.E.) set as a formal counterpart—satisfactory, by the Church–Turing thesis—of this intuitive notion. Here is one among various equivalent ways of characterizing it:

Characterization 1. *An $(m+1)$-ary relation $\mathscr{R}$ on $\mathbb{N}$ is called* R.E. *if either $\mathscr{R} = \emptyset$ or there are* primitive recursive *functions $r_0, \ldots, r_m$ from $\mathbb{N}$ to $\mathbb{N}$ such that*

$$\mathscr{R} \quad = \quad \{\langle r_0(i), \ldots, r_m(i)\rangle \ : \ i \in \mathbb{N}\}\ .$$

As this definition suggests, we mainly refer to monadic functions henceforth; hence we can rely on an *ad hoc* characterization of primitive recursiveness, that we borrow from [13, Sec. 4.9]:

Characterization 2. *Put* $\mathtt{n}(x) = 0$ *and* $\mathtt{s}(x) = x + 1$ *for each* $x \in \mathbb{N}$. *Primitive recursive functions are all and only those functions from* $\mathbb{N}$ *to* $\mathbb{N}$ *that either belong to the initial endowment* $\mathtt{n}(\cdot)$, $\mathtt{s}(\cdot)$, *and* $\lambda(\cdot)$, $\rho(\cdot)$ *(see above, end of Sec. 3), or are obtainable from that endowment through repeated use of the following three operations:*

1. composing $f(\cdot)$ *and* $g(\cdot)$ *into the function* $f \circ g$ *that sends every* x *to* $f\big(g(x)\big)$;
2. pairing $f(\cdot)$ *and* $g(\cdot)$ *into the function* $f \otimes g$ *that sends every* x *to* $\varpi\big(f(x), g(x)\big)$ *(see p. 6);*
3. *obtaining by* recursion *from* $f(\cdot)$ *and* $g(\cdot)$ *the function*

$$h(x) \;\coloneqq\; \begin{cases} 0 & \text{if} \quad x = 0\,, \\ f\left(\frac{x-1}{2}\right) & \text{if} \quad x \in \{\,1,\,3,\,5,\,7,\ldots\,\}\,, \\ g\left(h\left(\frac{x}{2}\right)\right) & \text{if} \quad x \in \{\,2,\,4,\,6,\,8,\ldots\,\}\,. \end{cases}$$

We then have:

Theorem 1. *The graph*

$$\mathcal{F}(a\,,\,b) \quad\Longleftrightarrow\quad F(a) = b$$

of any primitive recursive function F *from* $\mathbb{N}$ *into* $\mathbb{N}$ *can be specified by means of an arithmetical formula* φ *within which all universal quantifiers are bounded and negation does not occur* (nor does implication; usage of the conjunction and disjunction connectives $\,\&\,$, $\vee$ is subject to no restraints, also existential quantification can be used with no restraints, because we are assuming as a primitive sign $\exists$ as well as $\forall$).

Proof. The graphs of the initial functions $\mathtt{n}(\cdot)$, $\mathtt{s}(\cdot)$, $\lambda(\cdot)$, and $\rho(\cdot)$ can be specified, respectively, by $a+b = a$, $a+1 = b$, $\exists\, p \exists\, x\big(\,\mathit{Pow}(b,p)\;\&\;p\cdot(2\,x+1) = a+1\,\big)$, and $\exists\, x \exists\, p\big(\,\mathit{Pow}(x,p)\;\&\;p\cdot(2\,b+1) = a+1\,\big)$, where $\mathit{Pow}(a,b)$ is a formula describing the graph of 2^a—this function gets the value 1 when $a = 0$ and gets the value $2\cdot 2^t$ when $a = t+1$. By exploiting the Chinese remainder theorem in the manner explained in [5, pp. 79–80],[5] we get the specification

$$\begin{aligned} \mathit{Pow}(a,b) \;\coloneqq\; \exists\, u \exists\, d\Big[\;& 1 = u \;\%\; \big(1+d\big) \;\;\&\;\; b = u \;\%\; \big(1+(a+1)\cdot d\big) \;\;\&\; \\ & \forall t \leqslant a\Big(\; u \;\%\; \big(1+(t+2)\cdot d\big) \;= \\ & \qquad\qquad 2\cdot\big[u \;\%\; \big(1+(t+1)\cdot d\big)\big]\;\Big)\Big]\,. \end{aligned}$$

As for the mechanisms enabling the immediate construction of primitive recursive functions out of $f(\cdot)$ and $g(\cdot)$ that are supposed to satisfy the induction hypothesis, we so specify the

$$\text{graph of } f\circ g\colon\quad \exists\, y\big(\,g(a) = y \;\;\&\;\; f(y) = b\,\big)\,,$$

$$\text{graph of } f\otimes g\colon\quad \begin{cases} \exists\, x \exists\, y \exists\, p\Big[\;\; f(a) = x \;\;\&\;\; g(a) = y \;\;\&\; \\ \qquad\qquad \mathit{Pow}(x,p) \;\;\&\;\; p\cdot(y+y+1) = b+1\Big]\,, \end{cases}$$

[5] A corollary, originating from Gödel (1931), of the Chinese remainder theorem says: Consider integers $a_0, \ldots, a_n$ such that $0 \leqslant a_i < q$ holds for each i, and put $q_i \;=\; 1 + n\,!\cdot q\cdot(i+1)$. Then $a_0 = a \;\%\; q_0, \ldots, a_n = a \;\%\; q_n$ hold together for a sole $a < \prod_{j\leqslant n} q_j$.

and then conclude by so specifying the outcome of recursion:

$$\exists\, u\, \exists\, d\, \exists\, m \Big[\quad 0 = u \,\%\, \big(1+d\big) \;\;\&\;\; b = u \,\%\, \big(1+(a+1)\cdot d\big) \;\;\&\;\; m = a \div 2 \;\;\&$$

$$\forall t \leqslant m \Big(\; f(t) = u \,\%\, \big(1+(2\cdot t+2)\cdot d\big) \;\;\& \\ g\big(u \,\%\, \big(1+(t+2)\cdot d\big) = u \,\%\, \big(1+(2\cdot t+3)\cdot d\big) \;\Big)\Big] .$$

Needless to say, here the Chinese remainder theorem is at work again. ⊣

In light of the elicitation Char. 1 of listability, Thm. 1 can easily be generalized into:

Theorem 2. *Every listable (property or) relation on $\mathbb{N}$ can be specified by means of an arithmetical formula wherein all universal quantifiers are bounded and neither negation nor implication occurs.*

In [5, pp. 93–96], a syntactic manipulation algorithm is described that transforms any arithmetical formula φ endowed with the features stated in Thm. 1 (and in Thm. 2), and whose free variabes are $a_0, a_1, \ldots, a_m$, into a Diophantine polynomial $R(h, y, a_0, \ldots, a_m, x_1, \ldots, x_\kappa)$ such that:

$$\varphi(a_0, \ldots, a_m) \quad \Longleftrightarrow \quad \exists\, h\, \forall\, y \leqslant h\, \exists\, x_1 \leqslant h \cdots \exists\, x_\kappa \leqslant h \,\big[\, R(h, y, a_0, \ldots, a_m, x_1, \ldots, x_\kappa) = 0 \,\big].$$

This special format is called Davis normal form, because it was first brought to light (originally lacking bounds on the inner existential quantifiers) in [14, Part III]. We will now report on a perfectioning of this format, that Yuri Matiyasevich put forward after establishing that the *a priori* distinct notions of r.e. set and Diophantine set amount to one another (cf. [2]).

Ancillary to that, let us introduce the Cantor functions c_ℓ, with $\ell \in \mathbb{N} \setminus \{0\}$:

$$\begin{aligned} \mathsf{c}_1(u_1) &\coloneqq u_1 \,, \\ \mathsf{c}_{q+2}(u_1, \ldots, u_{q+2}) &\coloneqq \mathsf{c}_{q+1}\left(u_1, \ldots, u_q, \frac{(u_{q+1}+u_{q+2})^2 + 3\cdot u_{q+1} + u_{q+2}}{2}\right) . \end{aligned}$$

It thus turns out that each c_ℓ is a monotone injection of $\mathbb{N}^\ell$ onto $\mathbb{N}$. Yu. Matiyasevich stated:

Lemma 3 ([15, pp. 303–304])**.** *To each Diophantine polynomial $D(a_0, \ldots, a_m, x_1, \ldots, x_\kappa)$, there correspond Diophantine polynomials $P(h, y, a_0, \ldots, a_m, x_0, x_1, \ldots, x_\kappa) \geqslant 0$ and $E(a_0, \ldots, a_m, h) \geqslant 0$ such that the following biimplications hold (where $\vec{a}$ and $\vec{x}$ shorten $a_0, \ldots, a_m$ and $x_0, x_1, \ldots, x_\kappa$, respectively):*[6]

$$\begin{aligned} \exists\, x_1 \cdots \exists\, x_\kappa\; D(\vec{a}, x_1, \ldots, x_\kappa) = 0 \quad &\Longleftrightarrow \quad \exists\, h\, \forall\, y \leqslant h \quad \exists\, \vec{x} \;\; P(h, y, \vec{a}, \vec{x}) = 0 \\ &\Longleftrightarrow \quad \exists!\, h \;\; \forall\, y \leqslant h \;\; \exists\, \vec{x} \;\; P(h, y, \vec{a}, \vec{x}) = 0 \\ &\Longleftrightarrow \quad \exists\, h \;\; \forall\, y \leqslant h \;\; \exists!\, \vec{x} \;\; P(h, y, \vec{a}, \vec{x}) = 0 \\ \Longleftrightarrow \quad \exists\, h\, \forall\, y \leqslant h \;\; \exists\, x_0 \leqslant E(\vec{a}, h)\, \exists\, x_1 \leqslant E(\vec{a}, h) \cdots \exists\, x_\kappa \leqslant E(\vec{a}, h) \quad &P(h, y, \vec{a}, \vec{x}) = 0 \,. \end{aligned}$$

Proof. We will define $P(h, y, \vec{a}, x_0, x_1, \ldots, x_\kappa)$ so that $P = 0$ enforces univocally (also with respect to the new existential variables, h and x_0) the condition

$$\mathsf{c}_\kappa(x_1, \ldots, x_\kappa) = y \quad \& \quad \big[\big(y < h \;\&\; D(\vec{a}, x_1, \ldots, x_\kappa) \neq 0\big) \quad \vee \quad \big(y = h \;\&\; D(\vec{a}, x_1, \ldots, x_\kappa) = 0\big)\big].$$

[6] The sign '$\exists!$' (read: "there exists a sole") can be introduced as usual: $\exists!\, v\, \varphi \;\coloneqq\; \exists\, u\, \forall\, v\, (\, \varphi \Longleftrightarrow v = u\,)$.

For this purpose, we put[7]

$$P \;\coloneqq\; 2^{2^\kappa}\cdot\big(y-\mathsf{c}_\kappa(x_1,\ldots,x_\kappa)\big)^2+ \\ \big[(h-y)\cdot D^2(\vec{a},x_1,\ldots,x_\kappa)-x_0-1\big]^2\;\cdot\;\big[(h-y)^2+D^2(\vec{a},x_1,\ldots,x_\kappa)+x_0\big].$$

It is then clear that the variables h, $x_1,\ldots,x_\kappa$, and x_0 on the right-hand side of the claimed biimplications designate, respectively: the first u such that the κ-tuple $\langle\hat{x}_1,\ldots,\hat{x}_\kappa\rangle$ for which $\mathsf{c}_\kappa(\hat{x}_1,\ldots,\hat{x}_\kappa)=u$ holds solves the equation $D(\vec{a},x_1,\ldots,x_\kappa)=0$ (in the unknowns $x_1,\ldots,x_\kappa$); for each $y\leqslant h$, the κ-tuple $\langle x_{y,1},\ldots,x_{y,\kappa}\rangle$ such that $\mathsf{c}_\kappa(x_{y,1},\ldots,x_{y,\kappa})=y$; the accordance between positivity of $h-y$ and non-nullity of $D(\vec{a},x_{y,1},\ldots,x_{y,\kappa})$. When the left-hand side of each claimed biimplication is satisfied by specific a_i's, we can hence determine—and they are unique—a value for h and, corresponding to each y, values $x_{y,j}$'s that do to the case of the right-hand side; conversely, if h satisfies the right-hand side for given a_i's, then the corresponding $x_{h,1},\ldots,x_{h,\kappa}$ are such that $D(\vec{a},x_{h,1},\ldots,x_{h,\kappa})=0$. To end, we must address the issue of setting a suitable bound $E(\vec{a},h)$ on the variables x_j. Since no $x_{y,j}$ with $j>0$ can exceed h, we will enforce $E(\vec{a},h)\geqslant h$; to also take into proper account the values $x_{y,0}$, we put $E(\vec{a},h)\coloneqq h\cdot\big(1+\widetilde{E}(\vec{a},h)\big)$, where $\widetilde{E}(\vec{a},h)$ results from the polynomial $D^2(\vec{a},h,\ldots,h)$ through replacement of each one of its coefficients, k, by the absolute value $|k|$. ⊣

5. Reducing Bounded Universal Quantifiers to Exponentiation

The proof that the family of exponential Diophantine relations is closed under bounded universal quantification can be developed in many different ways (see [16, Chap.6]). Here we resume part of the development (Lemmas 4 e 5) from the recent monograph [11]—see also [17, pp. 252–256], in turn stemming from [1, pp. 433–435]—; the other part (Lemma 3 above and Lemma 6 below) is instead adapted from [6], in order to ensure univocity.

Lemma 4. (Cf. [11, p.154]). *To each Diophantine polynomial $P(h\,,\,y\,,\,a_1\,,\ldots,\,a_m\,,\,x_1\,,\ldots,\,x_\kappa)$ there correspond Diophantine polynomials $Q(h\,,\,u\,,\,a_1\,,\ldots,\,a_m)$ such that the following hold:*

- $Q(h\,,\,u\,,\,a_1\,,\ldots,\,a_m)\;>\;h\max u$;
- $Q(h\,,\,u\,,\,a_1\,,\ldots,\,a_m)\;\geqslant\;|P(h\,,\,y\,,\,a_1\,,\ldots,\,a_m\,,\,x_1\,,\ldots,\,x_\kappa)|$ *when* $y\leqslant h$ *and* $x_1\,,\ldots,\,x_\kappa\leqslant u$.

Proof. (Just a clue). The trick is similar to the one used at the end of the proof of Lemma 3. ⊣

Lemma 5 (From [11, pp. 150–153]). *If P and Q are as in Lemma 4 then, given $h,u,a_1,\ldots,a_m$,*

$$\forall\, y\leqslant h\;\exists\, x_1\leqslant u\cdots\exists\, x_\kappa\leqslant u\quad P(h\,,\,y\,,\,a_1\,,\ldots,\,a_m\,,\,x_1\,,\ldots,\,x_\kappa)\;\;=\;\;0$$

will hold if and only if there exist $t\,,\,z\,,\,w_1\,,\ldots,\,w_\kappa$ such that

(1) $t=Q(h\,,\,u\,,\,a_1\,,\ldots,\,a_m)\,!$;
(2) $1+(z+1)\,t=\prod_{y\leqslant h}\big(1+(y+1)\,t\big)$;
(3) $P(h\,,\,z\,,\,a_1\,,\ldots,\,a_m\,,\,w_1\,,\ldots,\,w_\kappa)\equiv 0\mod 1+(z+1)\,t$;

[7] The factor 2^{2^κ} abundantly suffices to elide the denominator of the polynomial c_κ.

(4) $1+(z+1)\,t \;\Big|\; \prod_{j\leqslant u}(w_i-j)$, *for* $i=1,\ldots,\kappa$. ⊣

Lemma 6. *Out of any given Diophantine polynomial* $D(a_1,\ldots,a_m,x_1,\ldots,x_\kappa)$, *one can construct three polynomials,* $P(h,y,a_1,\ldots,a_m,x_0,x_1,\ldots,x_\kappa)$, $E(a_1,\ldots,a_m,h)$, *and* $Q(h,u,a_1,\ldots,a_m)$, *each producing values in* $\mathbb{N}$ *when its variables range over* $\mathbb{N}$, *such that* $\exists\, x_1\cdots\exists\, x_\kappa\; D(a_1,\ldots,a_m,x_1,\ldots,x_\kappa)=0$ *holds if and only if there exist* ***uniquely determined*** $h\,,u\,,t\,,z\,,w_0\,,\ldots,w_\kappa\,,g_0\,,\ldots,g_\kappa\,,f_0\,,\ldots,f_\kappa$, *and* e *satisfying the following exponential Diophantine conditions:*

(1) $u=E(a_1,\ldots,a_m,h)\;\;\&\;\; t=Q(h\,,u\,,a_1\,,\ldots,a_m)\,!$;
(2) $e=1+(z+1)\,t\;\;\&\;\; e=\prod_{y=1}^{h+1}\big(1+y\,t\big)$;
(3) $e\mid P(h\,,z\,,a_1\,,\ldots,a_m\,,w_0\,,w_1\,,\ldots,w_\kappa)$;
(4) $g_i+u=w_i\;\;\&\;\; e\;\Big|\;\prod_{j\leqslant u}\big(g_i+j\big)$, *for* $i=0,1,\ldots,\kappa$;
(5) $\bigvee_{i\leqslant\kappa}\Big[\big(\,\&_{\,j<i}\;g_j=f_j+e\big)\;\;\&\;\; g_i+f_i+1=e\;\;\&\;\;\&_{\,j=i+1}^{\,\kappa}\;f_j=0\Big]$.

Proof. From D—assuming without loss of generality that $m>0$—we obtain P and E as in Lemma 3, then we get Q from P as in Lemma 4 (there is but one extra variable, x_0). Now we can apply Lemma 5, with $u=E(a_1,\ldots,a_m,h)$, and this accounts for the conditions (1)–(4). By means of the g_i, we are requiring that $w_i\geqslant u$; this is a legitimate request, in the light of the proof of Lemma 5, whose congruence $P(u\,,\,z\,,\,a_1\,,\ldots,\,a_m\,,\,w_0\,,w_1\,,\ldots,\,w_\kappa)\;\equiv\;0 \mod e$ is rewritten as a divisibility constraint between natural numbers here, by taking the fact $P(h\,,\,z\,,\,a_1\,,\ldots,\,a_m\,,\,w_0\,,w_1\,,\ldots,\,w_\kappa)\geqslant 0$ into account; moreover, within that proof we had represented each $w_i-x_{y,i}$ in the form w_i-j with $0\leqslant j\leqslant u$, here we are representing it in the form g_i+j with $0\leqslant j\leqslant u$.

As Lemma 3 suggests, in order to make the specification (1)–(4) univocal, it is enough to bring into play new unknowns $f_0,\ldots,f_\kappa$ subject to the constraint (5). That is, we are choosing as representative of the infinitely many $(\kappa+1)$-tuples $\langle w_0,\ldots,w_\kappa\rangle$ suitable to encode the list of tuples $\langle x_{0,i},\ldots,x_{h,i}\rangle$ $(i=0,\ldots,\kappa)$ as described within the proof of Lemma 5, the one whose components cannot be lowered by the amount e without at least one among them becoming smaller than u. ⊣

Knowing that each listable has a representation $\exists\,\vec{x}\;D(\vec{a}\,,\;\vec{x})=0$, we can view Lemma 6 as enriching the DPR theorem [1] with single-fold-ness; in short:

Theorem 3 (Matiyasevich, 1974)**.** *Each listable set has a* ***univocal*** *exponential Diophantine representation.*

6. Exponentiation as a Notable Quotient

Denote by $\langle \boldsymbol{y}_i(a)\rangle_{i\in\mathbb{N}}$ the endless, strictly ascending, sequence consisting of all non-negative integer solutions to the Pell equation[8]

$$(a^2-1)\,y^2+1\;=\;\square\quad\text{with}\quad a\in\mathbb{N}\setminus\{0,1\}\;;$$

[8]Once more, '$Q=\square$' means that Q must be a perfect square.

also put $\boldsymbol{x}_i(a) \coloneqq \sqrt{(a^2-1)\,\boldsymbol{y}_i^2(a)+1}$. Then:

Lemma 7. *The following law determines* ***uniquely*** *the values of* u, v *:*

$$\big((b \geqslant 1 \vee n = 0)\ \&\ a > b^n\big) \implies \left[\begin{array}{l} b^n = c \iff \exists\, u\, \exists\, v \left(u^2 - (a^2\, b^2 - 1)\, v^2 = 1\ \& \right. \\ \qquad \boldsymbol{x}_n(a) \leqslant u < a\, \boldsymbol{x}_n(a)\ \&\ c = u \div \boldsymbol{x}_n(a)\Big) \end{array}\right].$$

Moreover, if $b \geqslant 1\ \&\ w \geqslant 3\,(c+1)(n+1)$ *, then* $b^n = c \iff c = \boldsymbol{y}_{n+1}(b\,w+1) \div \boldsymbol{y}_{n+1}(w)$ *.*

Proof. Concerning the first claim, the proof can be traced back to [4, Lemmas 9 and 10] (see also [3, Lemma 3]). Concerning the second claim, see [15, p. 308]. ⊣

Through the first claim of Lemma 7, Martin Davis got a very neat and general restatement of the DPR theorem, where a single literal involving an exponential-growth relation $\mathscr{J}(u\,,\ v)$ supersedes exponentiation. Together with $\mathscr{J}(\centerdot,\ \centerdot)$, Davis' technique exploits a Diophantine relation $\mathscr{D}(\centerdot,\ \centerdot,\ \centerdot)$ on $\mathbb{N}$, such that[9]

- $\forall\, b\, \forall\, n\, \forall\, v\, \forall\, t\, \big[\, v > t\ \&\ \mathscr{D}(b,n,t) \implies v > b^n\,\big]$ and
- $\forall\, b\, \forall\, n\, \exists\, t\ \ \mathscr{D}(b,n,t)$,

along with the Diophantine relation

$$\begin{array}{rcl} \mathscr{E}(b,n,c,a,\ell) & \coloneqq & \exists\, u\, \exists\, v\, \exists\, w\, \big[\ \ \big(b = u = v = c = 0\ \&\ n = w+1\big)\ \vee \\ & & \big(u^2 - (a^2\, b^2 - 1)\, v^2 = 1\ \ \&\ w = 0\ \& \\ & & \ \ \ell \leqslant u < a\,\ell\ \&\ c = u \div \ell\big)\ \ \ \big]\,. \end{array}$$

It can be shown that

$$\begin{array}{rcl} \&_{\,i\leqslant s}\, b_i^{n_i} = c_i & \iff & (\exists\, a\,,\ t_0, \ldots, t_s,\ \ell_0, \ldots, \ell_s)\ \&_{\,i\leqslant s}\Big[\mathscr{D}(b_i,n_i,t_i)\ \&\ a > t_i\ \& \\ & & \qquad\qquad \mathscr{E}(b_i,n_i,c_i,a,\ell_i)\ \&\ \ell_i = \boldsymbol{x}_{n_i}(a)\Big]\,, \end{array}$$

whence $\boldsymbol{x}_{n_i}(a)$ can be eliminated thanks to the following:

Lemma 8 (Cf. [18, Lemma A.2])**.** *Suppose that* $a > 1$*,* $a > n$*, and* $\boldsymbol{x}_a(a) > \ell$ *. Then,*

$$\ell = \boldsymbol{x}_n(a) \iff \exists\, r\quad \ell^2 - (a^2-1)\,\big(n + (a-1)\,r\big)^2 = 1\,.$$

Ultimately, one gets the following proposition, whose proof we omit:

Lemma 9. *If* $\mathscr{J}(\centerdot,\ \centerdot)$ *is an exponential-growth relation and each* b_i, n_i, c_i *is either a variable or a non-negative integer constant, then we have*

$$\begin{array}{rcl} \&_{\,i\leqslant s}\, b_i^{n_i} = c_i & \iff & (\exists\, a, d,\ t_0, \ldots, t_s,\ \ell_0, \ldots, \ell_s,\ r_0, \ldots, r_s)\Big[\ \mathscr{J}(a\,,\ d)\ \& \\ & & \qquad \&_{\,i\leqslant s}\Big[\ \mathscr{D}(b_i,n_i,t_i)\ \&\ a > t_i\ \&\ a > n_i\ \& \\ & & \qquad\quad \mathscr{E}(b_i,n_i,c_i,a,\ell_i)\ \&\ \ell_i < d\ \& \\ & & \qquad\quad \ell_i^2 = (a^2-1)\,\big[n_i + (a-1)\,r_i\big]^2 + 1\ \Big]\ \Big]\,. \end{array}$$

[9] For definiteness, one could take $\mathscr{D}(b,n,t) \coloneqq \mathscr{Q}(b+n+2,t)$, where $\mathscr{Q}(w,u)$ is as in [7, p. 155], namely:
$\mathscr{Q}(w,u) \coloneqq (\exists\, x\,,\ y)\Big[\ u \geqslant w\,x\ \&\ x > 1\ \&\ x^2 - (w^2-1)\,(w-1)^2\,y^2 = 1\ \Big]$.

Therefore, in view of Lemma 1:

Theorem 4 (Davis, 1963). *Each listable subset of a Cartesian power $\mathbb{N}^{m+1}$ admits a specification of the form $\exists\, u\, \exists\, v\, \exists\, \vec{x}\, \big[D(\vec{a},\vec{x},u,v)=0\ \&\ \mathscr{J}(u\,,\,v)\big]$, where D is a Diophantine polynomial and $\mathscr{J}$ is any exponential-growth relation.*

In one respect, this achieves more than Thm. 3; in fact, here we have a generic exponential-growth relation in place of exponentiation. But, regrettably, univocity is not ensured.

Matiyasevich made a leap towards a reconciliation between Thm. 3 and Thm. 4 in [15, pp. 308–309]. In his theorem, reported below, the specific relation $2^u=v$ occurs instead of a generic $\mathscr{J}(u\,,\,v)$; and in its proof (which we omit) the second claim of Lemma 7 plays a decisive role:

Theorem 5 (Exponentiation, from dyadic to monadic). *A **univocal** exponential Diophantine specification of any relation $\&_{i=1}^{s}\, b_i^{n_i}=c_i$ (where b_i, n_i, c_i are as said above) is:*

$$\exists\, u\, \exists\, v\ \ \exists\, e_1\, \exists\, f_1\, \exists\, g_1\, \exists\, h_1 \cdots \exists\, e_s\, \exists\, f_s\, \exists\, g_s\, \exists\, h_s\, \Big[\ \ \mathcal{L}_1\ \&\ \mathcal{L}_2\ \&\ \&_{i=1}^{s}\, [(\,b_i=0\ \&\ \mathcal{L}_{3,i}\,)\ \vee\ (\,b_i>0\ \&\ \mathcal{L}_{4,i}\ \&\ \mathcal{L}_{5,i}\ \&\ \mathcal{L}_{6,i}\ \&\ \mathcal{L}_{7,i}\,)]\Big]\,,$$

where

$$\begin{aligned}
\mathcal{L}_1 &\coloneqq u=20\,\textstyle\sum_{i=1}^{s}(c_i+1)(2\,b_i+1)(n_i^2+1)\,,\\
\mathcal{L}_2 &\coloneqq 2^u=v\,,\\
\mathcal{L}_{3,i} &\coloneqq [(\,n_i=0\ \&\ c_i=1\,)\ \vee\ (\,n_i>0\ \&\ c_i=0\,)]\ \&\ e_i=f_i=g_i=h_i=0\,,\\
\mathcal{L}_{4,i} &\coloneqq c_i=f_i\div h_i\,,\\
\mathcal{L}_{5,i} &\coloneqq e_i^2-\big((b_i\,u+1)^2-1\big)\,f_i^2=1\ \&\ g_i^2-\big(u^2-1\big)\,h_i^2=1\,,\\
\mathcal{L}_{6,i} &\coloneqq f_i\equiv n_i+1 \bmod (b_i\,u)\ \&\ h_i\equiv n_i+1 \bmod (u-1)\,,\\
\mathcal{L}_{7,i} &\coloneqq f_i<v\ \&\ h_i<v\,.
\end{aligned}$$

Consequently, every listable subset of a Cartesian power $\mathbb{N}^{m+1}$ admits a univocal representation $\exists\, u\, \exists\, v\, \exists\, \vec{x}\, \big[D(a_0\,,\ldots,\,a_m\,,\,\vec{x},u,v)=0\ \&\ 2^u=v\big]$, where D is a Diophantine polynomial.

7. Two elusive issues

We are after a generalized variant of Thm. 5 which has, in place of its

$$\mathcal{L}_1\ \&\ 2^u=v\ \&\ \&_{i=1}^{s}\,[(\,b_i=0\ \&\ \mathcal{L}_{3,i}\,)\ \vee\ (\,b_i>0\ \&\ \mathcal{L}_{4,i}\ \&\ \mathcal{L}_{5,i}\ \&\ \mathcal{L}_{6,i}\ \&\ \mathcal{L}_{7,i}\,)]\,,$$

a suitable formula $D(\,\vec{a}\,,\,\vec{x}\,,\,u\,,\,v\,)=0\ \&\ \mathscr{M}(u\,,\,v)$, where D is a Diophantine polynomial in the parameters $\vec{a}$ and

- $\mathscr{M}$ is a dyadic relation subject to *particular requirements*—probably stronger than exponential-growth. Moreover,
- a concrete such $\mathscr{M}$ should be exhibited that admits a *finite-fold*—hopefully univocal—Diophantine polynomial specification.

The achievement of these two goals would answer positively an issue raised in [6] and [8]: "OPEN PROBLEM: *Is there a finitefold (or better a singlefold) Diophantine definition of $a=b^c$?*"

As regards which requirement should be imposed on $\mathscr{M}$, [9, p. 749] suggests the following (without explaining, though, why this would be adequate to ensure that the relation $2^u=v$—and therefore any listable set—has a finite Diophantine specification if $\mathscr{M}(u\,,\,v)$ has one):

Integers $\alpha > 1\,,\ \beta \geqslant 0\,,\ \gamma \geqslant 0\,,\ \delta > 0$ exist such that to each $w \in \mathbb{N} \setminus \{0\}$ there correspond u, v such that: $\mathscr{M}(u\,,\ v)\,,\ u < \gamma\, w^{\beta}$, and $v > \delta\, \alpha^{w}$ hold. (‡)

As for a concrete choice of $\mathscr{M}$, the most promising candidate at the time when [8] was published was an exponential-growth relation, $\mathscr{M}_7$, associated in a certain manner with the quaternary quartic equation $9 \cdot (u^2 + 7\,v^2)^2 - 7 \cdot (r^2 + 7\,s^2)^2 \ = \ 2$ that had been spotlighted in [19]. The proposed $\mathscr{M}_7$ would admit a finite-fold Diophantine polynomial specification if the said equation only had a finite number of integer solutions. Below, we will spotlight a few other quaternary quartics that may candidate as rule-them-all equations.

8. Candidate rule-them-all equations: how helpful can they be?

In [19], Martin Davis argued that Hilbert's 10^{th} problem would turn out to be algorithmically unsolvable if his quaternary quartic just recalled could be shown to admit only one solution in $\mathbb{N}$ (an expectation, btw, that came to an end in the early 1970s). In [18, 7, 20], by following Davis' same construction pattern, we increased the number of Diophantine equations that candidate as "rule-them-all equations" to six. Each such equation is associated with one of the eight so-called Heegner numbers $d \neq 1$; today we know that, if any of the equations

Number d	Associated quaternary quartic equation
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	$7 \cdot \left(r^2 + 7\,s^2\right)^2 - 3^2 \cdot \left(u^2 + 7\,v^2\right)^2 \ = \ -2$
11	$11 \cdot \left(r^2 + r\,s\, + 3\,s^2\right)^2 - \left(v^2 + v\,u + 3\,u^2\right)^2 \ = \ 2$
19	$19 \cdot 3^2 \cdot \left(r^2 + r\,s\, + 5\,s^2\right)^2 - 13^2 \cdot \left(v^2 + v\,u + 5\,u^2\right)^2 \ = \ 2$
43	$43 \cdot \left(r^2 + r\,s\, + 11\,s^2\right)^2 - \left(v^2 + v\,u + 11\,u^2\right)^2 \ = \ 2$

associated with the respective Pell equations $d\,y^2 + 1 = \square$ turned out to admit only a finite number of solutions in $\mathbb{Z}$, then every listable set—first and foremost the set of all triples $\langle b, n, c\rangle \in \mathbb{N}^3$ such that $b^n = c$—would admit a finite-fold polynomial Diophantine representation.

If the equation associated with d has a finite overall number of solutions, then the following dyadic relation $\mathscr{M}_d$ over $\mathbb{N}$ admits a polynomial Diophantine representation:

$$d \in \{2, 7\}: \qquad \mathscr{M}_d(p, q) \ \coloneqq \ \exists\, \ell > 4 \left[\, q = \widetilde{\boldsymbol{y}}_{2^\ell}(d) \ \ \& \ \ p \mid q \ \ \& \ \ p \geqslant 2^{\ell+1} \,\right],$$
$$d \in \{3, 11, 19, 43\}: \qquad \mathscr{M}_d(p, q) \ \coloneqq \ \exists\, \ell > 5 \left[\, q = \widetilde{\boldsymbol{y}}_{2^{2\,\ell+1}}(d) \ \ \& \ \ p \mid q \ \ \& \ \ p \geqslant 2^{2\,\ell+2} \,\right],$$

where $\langle \widetilde{\boldsymbol{y}}_i(d)\rangle_{i\in\mathbb{N}}$ is the endless, strictly ascending, sequence consisting of all solutions in $\mathbb{N}$ to the said equation $d\,y^2 + 1 = \square$. Independently of representability, each $\mathscr{M}_d$ turns out to satisfy Julia Robinson's exponential growth criteria and Matiyasevich's condition (‡) seen above.

It is very hard to guess whether the number of solutions to any of the six quartics shown above is finite or infinite. For quite a while the authors hoped that Matiyasevich's surmise that each r.e. set admits a single-fold polynomial Diophantine representation could be established by just proving that the sole solution to the quartic $2 \cdot \left(r^2 + 2\,s^2\right)^2 - \left(u^2 + 2\,v^2\right)^2 \ = \ 1$ in $\mathbb{N}$ is $\langle \bar{r}, \bar{s}, \bar{u}, \bar{v}\rangle \ = \ \langle 1, 0, 1, 0\rangle$; but a couple of days after [20] was published on arXiv, Evan

O'Dorney (University of Notre Dame) and Bogdan Grechuk (University of Leicester) sent us kind communications that they had found two, respectively three, non-trivial solutions to this equation. Their first solution is

$$\begin{aligned} r_1 &= 877858705853420680629262000814366081842686551436 7, \\ s_1 &= 179713932488256519754813410509015303713014994344 0, \\ u_1 &= 522161829581767869234369948366270495963105233171 3, \\ v_1 &= 673995831734307398531099945196547956085852187162 4; \end{aligned}$$

the components of the third solution are numbers of roughly 180 decimal digits each.

It must be mentioned that Apoloniusz Tyszka radically disbelieves Matiyasevich's finite-fold representability conjecture[10] which has been, throughout, (and firmly remains) our polar star.

Conclusion

One of the questions Yu. Matiyasevich raised, at the outset of his seminal paper [6] on the Diophantine single-/finite-fold representability issue, was:

> Suppose a proof is available that each
>
> $$D_a(x_1, \ldots, x_\kappa) \;=\; 0\,, \qquad\qquad a \in \mathbb{N}\,,$$
>
> in some indexed family of equations has at most one solution in $\mathbb{N}$. Can we extract from it an effective bound $\mathscr{C}_a$ ensuring, when $x_1 = \boldsymbol{v}_1 \quad, \ldots, \quad x_\kappa = \boldsymbol{v}_\kappa$ is such solution, that $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\kappa \leqslant \mathscr{C}_a$?

As we have recalled and explained among the conclusions of [7], his answer was negative in general, assuming the signature underlying the D_a's comprises exponentiation. Matiyasevich calls "noneffectivizable estimates" [15, 10] this and more general limiting results that follow from the univocal representability, in terms of exponentiation, of any r.e. set. Analogous limiting results about polynomial Diophantine equations would follow if it turned out that any r.e. set admits a finite-fold representation in merely polynomial terms; can such a representation be carried out? This entire paper has revolved around this question, to whose hoped-for positive answer the material outlined in Sec. 8 (cf. [20] for a reasoned account) might prove useful.

Matiyasevich also discussed in [22] (see [7, pp. 151–152] for a quick account) intriguing consequences that establishing the finite-fold Diophantine representability of any r.e. set would entail about the Diophantine characterization of the probability of selecting by chance a program that terminates on every input.

This paper is a companion of [7]. Two differences are: (1) In accordance with the historical path [1, 6] great emphasis is placed on the kinship between exponentiation and bounded universal quantification. (2) Novel candidate rule-them-all equations have entered into play.

[10] See, among many, https://arxiv.org/abs/0901.2093. As pointed out in [21, p. 711], even [8, p. 360] suggests a possibility that "would eliminate the possibility of singlefold definitions for all Diophantine sets".

Acknowledgments

The authors gratefully acknowledge partial support from project "STORAGE–Università degli Studi di Catania, Piano della Ricerca 2020/2022, Linea di intervento 2", from INdAM–GNCS 2019 and 2020 research funds, and from ICSC–Centro Nazionale di Ricerca in High-Performance Computing, Big Data and Quantum Computing.

The authors are indebted with Pietro Corvaja (University of Udine) and Pietro Campochiaro (Scuola Superiore di Catania) for helpful discussions, and to the anonymous referees for many useful suggestions.

References

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

[2] Yu. V. Matiyasevich, Diofantovost' perechislimykh mnozhestv, Doklady Akademii Nauk SSSR 191 (1970) 279–282. (Russian. Available in English translation as [23]; translation reprinted in [24, pp. 269–273]).

[3] M. Davis, Extensions and corollaries of recent work on Hilbert's tenth problem, Illinois Journal of Mathematics 7 (1963) 246–250. URL: https://doi.org/10.1215/ijm/1255644635.

[4] J. Robinson, Existential definability in arithmetic, Transactions of the American Mathematical Society 72 (1952) 437–449. Reprinted in [25, p. 47ff.].

[5] J. Robinson, Diophantine decision problems, in: W. J. LeVeque (Ed.), Studies in Number Theory, volume 6 of *Studies in Mathematics*, Mathematical Association of America, 1969, pp. 76–116.

[6] 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 (1974) 77–93. (Russian. Translated into English as [15]).

[7] D. Cantone, A. Casagrande, F. Fabris, E. G. Omodeo, The quest for Diophantine finite-fold-ness, Le Matematiche 76 (2021) 133–160. https://lematematiche.dmi.unict.it/index.php/lematematiche/article/view/2044.

[8] M. Davis, Yu. Matijasevič, 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*, American Mathematical Society, Providence, RI, 1976, pp. 323–378. Reprinted in [25, p. 269ff.].

[9] Yu. Matiyasevich, Towards finite-fold Diophantine representations, Journal of Mathematical Sciences 171 (2010) 745–752. URL: https://doi.org/10.1007/s10958-010-0179-4. doi:10.1007/s10958-010-0179-4.

[10] Yu. Matiyasevich, Martin Davis and Hilbert's tenth problem, in: [26], 2016, pp. 35–54.

[11] M. R. Murty, B. Fodden, Hilbert's tenth problem. An Introduction to Logic, Number Theory, and Computability, volume 88 of *Student mathematical library*, American Mathematical Society, Providence, RI, 2019.

[12] M. Davis, 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, 1959. (Part III reprinted in [26, pp. 411-430]).

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

[14] M. Davis, On the theory of recursive unsolvability, Ph.D. thesis, Princeton University, 1950.

[15] Yu. V. Matiyasevich, Existence of noneffectivizable estimates in the theory of exponential diophantine equations, Journal of Soviet Mathematics 8 (1977) 299–311. (Translated from [6]).
[16] Yu. V. Matiyasevich, Desyataya Problema Gilberta, Fizmatlit, Moscow, 1993. English translation: *Hilbert's Tenth problem.* The MIT Press, Cambridge (MA) and London, 1993. French translation: *Le dixième Problème de Hilbert: son indécidabilité*, Masson, Paris Milan Barcelone, 1995. URL: http://logic.pdmi.ras.ru/∼yumat/H10Pbook/.
[17] M. Davis, Hilbert's tenth problem is unsolvable, Amer. Math. Monthly 80 (1973) 233–269. Reprinted corrections in the Dover edition of *Computability and Unsolvability* [27, pp. 199–235].
[18] D. Cantone, E. G. Omodeo, "One equation to rule them all", revisited, Rendiconti dell'Istituto di Matematica dell'Università di Trieste (RIMUT) 53 (2021) 525–556. https://rendiconti.dmi.units.it/volumi/53/028.pdf.
[19] M. Davis, One equation to rule them all, Transactions of the New York Academy of Sciences. Series II 30 (1968) 766–773.
[20] D. Cantone, L. Cuzziol, E. G. Omodeo, Six equations in search of a finite-fold-ness proof, 2023. arXiv:2303.02208.
[21] A. Tyszka, A hypothetical way to compute an upper bound for the heights of solutions of a Diophantine equation with a finite number of solutions, in: M. Ganzha, L. A. Maciaszek, M. Paprzycki (Eds.), 2015 Federated Conference on Computer Science and Information Systems, FedCSIS 2015, Lódz, Poland, September 13-16, 2015, volume 5 of *Annals of Computer Science and Information Systems*, IEEE, 2015, pp. 709–716. URL: https://doi.org/10.15439/2015F41. doi:10.15439/2015F41.
[22] Yu. Matiyasevich. Diophantine flavor of Kolmogorov complexity. Transactions of the Institute for Informatics and Automation problems of NAS RA. Collected reports of participants of JAF-23 (June 2–5, 2004). pages 111–122. Yerevan, 2006.
[23] Ju. V. Matijasevič, Enumerable sets are Diophantine, Soviet Mathematics. Doklady 11 (1970) 354–358. (Translated from [2]).
[24] G. E. Sacks (Ed.), Mathematical Logic in the 20th Century, Singapore University Press, Singapore; World Scientific Publishing Co., Inc., River Edge, NJ, 2003.
[25] 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.
[26] E. G. Omodeo, A. Policriti (Eds.), Martin Davis on Computability, Computational Logic, and Mathematical Foundations, volume 10 of *Outstanding Contributions to Logic*, Springer, 2016.
[27] M. Davis, Computability and Unsolvability, McGraw-Hill, New York, 1958. Reprinted with an additional appendix, Dover 1983.