Does every recursively enumerable set admit a finite-fold Diophantine representation?

Domenico Cantone[1], Alberto Casagrande[2], Francesco Fabris[2], and Eugenio Omodeo[2]

Dept. of Mathematics and Computer Science, University of Catania, Italy.

Dept. of Mathematics and Geosciences, University of Trieste, Italy.

June 20, 2019

Presentation Spirit and Outline

This is a review paper unifying many relevant works in the field.

We will investigate formulas like

$$\exists\, a,\ d,\ \ell,\ s, x,\ h \Bigg[\ (c-1)^2 + n = 0\ \vee (n \geqslant 1\ \&\ c + b = 0)\ \vee$$
$$\Big(n \geqslant 1\ \ \&\ \ b \geqslant 1\ \ \&\ \ \mathcal{J}(a,d)\ \ \&\ \ d > \ell\ \ \&\ \ a > b + n \qquad \&$$
$$\ell^2 = (a^2-1)\left[n + (a-1)\,s\right]^2 + 1\ \ \&\ \ Q(b+n-2,h) = x^2\ \ \&$$
$$2\,a\,b - b^2 - 1 \geqslant \left[(b+n+1)\,x\right] \max\left(c+1\right) \qquad \&$$
$$2\,a\,b - b^2 - 1\ \ |\,\ell - \ \left(a-b\right)\left[(a-1)\,s + n\right]\ -\ c\ \Big)\ \Bigg]$$

Presentation Spirit and Outline

Wait, don't run away . . . I was joking

Technical details will be avoided and we will

- gently introduce the problem
- motivate our interest
- suggest a route towards the answer

Presentation Spirit and Outline

Wait, don't run away . . . I was joking

Technical details will be avoided and we will

- gently introduce the problem
- motivate our interest
- suggest a route towards the answer

If your are interested on the details, have a look at the paper

Definition (Existentially Definable Relations)

$\mathcal{R} \subseteq \mathbb{N}^n$ is ***existentially definable in terms of*** $\mathcal{J}(\bullet, \ldots, \bullet)$ if

$$\mathcal{R}(a_1, \ldots, a_n) \iff (\exists x_1 \cdots \exists x_m)\, \varphi(a_1, \ldots, a_n, x_1, \ldots, x_m)$$

holds, over $\mathbb{N}$, for some formula φ that only involves:

———

Definition (Existentially Definable Relations)

$\mathcal{R} \subseteq \mathbb{N}^n$ is ***existentially definable in terms of*** $\mathcal{J}(\bullet, \ldots, \bullet)$ if

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

holds, over $\mathbb{N}$, for some formula φ that only involves:

- the shown variables
- positive integer constants

———

Definition (Existentially Definable Relations)

$\mathcal{R} \subseteq \mathbb{N}^n$ is ***existentially definable in terms of*** $\mathcal{J}(\bullet, \ldots, \bullet)$ if

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

holds, over $\mathbb{N}$, for some formula φ that only involves:

- the shown variables
- positive integer constants
- addition, multiplication
- the logical connectives $\&$, $\vee$, $\exists x$, $=$

———

Definition (Existentially Definable Relations)

$\mathcal{R} \subseteq \mathbb{N}^n$ is ***existentially definable in terms of*** $\mathcal{J}(\bullet, \ldots, \bullet)$ if

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

holds, over $\mathbb{N}$, for some formula φ that only involves:

- the shown variables
- positive integer constants
- addition, multiplication
- the logical connectives $\&$, $\vee$, $\exists x$, $=$
- a predicate for $\mathcal{J}$

———

Definition (Existentially Definable Relations)

$\mathcal{R} \subseteq \mathbb{N}^n$ is ***existentially definable in terms of*** $\mathcal{J}(\bullet, \ldots, \bullet)$ if

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

holds, over $\mathbb{N}$, for some formula φ that only involves:

- the shown variables
- positive integer constants
- addition, multiplication
- the logical connectives $\&$, $\vee$, $\exists x$, $=$
- a predicate for $\mathcal{J}$

When $\mathcal{J}$ is absent, $\mathcal{R}$ is also called ***Diophantine***.

Some examples

- $a = b + x + 1$
- $a = (x + 2) \cdot (y + 2) \lor a + x = 1$
- $b = x \cdot a + y + 1 \;\&\; b = y + 1 + z + 1$
- $a^a = 1 \;\&\; x^x = a + 1$

Some examples

- $a = b + x + 1$
  existentially defines $a > b$
- $a = (x+2)\cdot(y+2) \vee a + x = 1$
  existentially defines a **is not prime**
- $b = x \cdot a + y + 1 \;\&\; b = y + 1 + z + 1$
  existentially defines $b \nmid a$
- $a^a = 1 \;\&\; x^x = a + 1$
  existentially defines $a = 0$ *in terms of* ***exponentiation***

Some examples

- $a = b + x + 1$
  existentially defines $a > b$
- $a = (x+2)\cdot(y+2) \vee a + x = 1$
  existentially defines a **is not prime**
- $b = x \cdot a + y + 1 \;\&\; b = y + 1 + z + 1$
  existentially defines $b \nmid a$
- $a^a = 1 \;\&\; x^x = a + 1$
  existentially defines $a = 0$ *in terms of* ***exponentiation***

Many useful Diophantine constructs can be added as done for
$\bullet > \bullet$, $\bullet \nmid \bullet$, and $\bullet$ **is not prime**

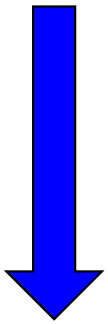
Theorem (DPR theorem [DPR61])

Every r.e. set is existentially definable in terms of exponentiation

Two important theorems

Theorem (DPR theorem [DPR61])

Every r.e. set is existentially definable in terms of exponentiation



"After the DPR-theorem was proved in 1961, in order to establish the existence of Diophantine representations for *every* effectively enumerable set it was sufficient to find a Diophantine representation for *one particular* set of triples

$$\{\langle a, b, c\rangle \mid a = b^c\}. \qquad (12)$$

"

[Mat10, p. 748]

Theorem (Matiyasevich's theorem (MRDP) [Mat74])

Every r.e. set is existentially definable

Definition (Single-fold existential definitions)

An existential definition

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

(as above) is ***single-fold*** if

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

(i.e., $\varphi(a_1, \ldots, a_n , x_1, \ldots, x_m)$ never has multiple solutions).

Definition (Single-fold existential definitions)

An existential definition

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

(as above) is ***single-fold*** if

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

(i.e., $\varphi(a_1, \ldots, a_n , x_1, \ldots, x_m)$ never has multiple solutions).

Finite-fold existential definitions

The definition of ***finite-fold***-ness is akin:

To each $\vec{a}$ there must correspond a *finite* number of solutions.

A Significant Improvement to DPR

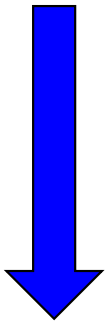
Theorem (An improvement to DPR [Mat74])

Every r.e. set admits an existential single-fold definition in terms of exponentiation.

A Significant Improvement to DPR

Theorem (An improvement to DPR [Mat74])

Every r.e. set admits an existential single-fold definition in terms of exponentiation.



"Today we are in a similar position with respect to single-fold (and finite-fold) Diophantine representations" (...) "it would be sufficient to find a single-fold (or, respectively, finite-fold) Diophantine representation for the same set of triples" i.e., $\{\langle a, b, c\rangle \mid a = b^c\}$. [Mat10, p. 748]

Aimed result

Every r.e. set admits an existential *single/finite-fold* definition.

A Motivating Application for Finite Foldness

Let $P(a, \vec{x})$ be Diophantine, let $\mathcal{M}$ be the set:

$$a \in \mathcal{M} \iff \exists \vec{x} \, \{P(a, \vec{x}) = 0\},$$

and let $\mathcal{M}_n$ be an initial fragment of $\mathcal{M}$, i.e.,

$$\mathcal{M}_n = \mathcal{M} \cap \{k \mid k \leqslant n\}$$

A Motivating Application for Finite Foldness

Let $P(a, \vec{x})$ be Diophantine, let $\mathcal{M}$ be the set:

$$a \in \mathcal{M} \iff \exists \vec{x} \, \{P(a, \vec{x}) = 0\},$$

and let $\mathcal{M}_n$ be an initial fragment of $\mathcal{M}$, i.e.,

$$\mathcal{M}_n = \mathcal{M} \cap \{k \mid k \leqslant n\}$$

How many bit do we need to transmit $\mathcal{M}_n$?

- trivially, n bits: 1 iff $k \in \mathcal{M}$

A Motivating Application for Finite Foldness

Let $P(a, \vec{x})$ be Diophantine, let $\mathcal{M}$ be the set:

$$a \in \mathcal{M} \iff \exists \vec{x} \, \{P(a, \vec{x}) = 0\},$$

and let $\mathcal{M}_n$ be an initial fragment of $\mathcal{M}$, i.e.,

$$\mathcal{M}_n = \mathcal{M} \cap \{k \mid k \leqslant n\}$$

How many bit do we need to transmit $\mathcal{M}_n$?

- trivially, n bits: 1 iff $k \in \mathcal{M}$
- if $\mathcal{M}$ is recursive, $\log n$ bits

A Motivating Application for Finite Foldness

Let $P(a, \vec{x})$ be Diophantine, let $\mathcal{M}$ be the set:

$$a \in \mathcal{M} \iff \exists \vec{x} \, \{P(a, \vec{x}) = 0\},$$

and let $\mathcal{M}_n$ be an initial fragment of $\mathcal{M}$, i.e.,

$$\mathcal{M}_n = \mathcal{M} \cap \{k \mid k \leqslant n\}$$

How many bit do we need to transmit $\mathcal{M}_n$?

- trivially, n bits: 1 iff $k \in \mathcal{M}$
- if $\mathcal{M}$ is recursive, $\log n$ bits
- if $\mathcal{M}$ is r.e., $2 \log n$ bits to transmit both n and k. $0 \in \mathcal{M} \| \ldots \| n \in \mathcal{M}$ is evaluated until we get k positive answers

A Motivating Application for Finite Foldness

Chaitin [Cha87] built two special Diophantine formulas and a $\mathcal{M}$

$$a \in \mathcal{M} \iff \exists^{\infty} \vec{x} \; \{E_L(a, \vec{x}) \; = \; E_R(a, \vec{x})\}, \tag{9}$$

such that

A Motivating Application for Finite Foldness

Chaitin [Cha87] built two special Diophantine formulas and a $\mathcal{M}$

$$a \in \mathcal{M} \iff \exists^{\infty} \vec{x} \, \{E_L(a, \vec{x}) \; = \; E_R(a, \vec{x})\}, \tag{9}$$

such that

> ... *"whatever so-called prefix-free compression algorithm is used, n bits (up to an additive constant) are required for representing the initial fragment (9) of $\mathcal{M}$"*
>
> [Mat10, p. 747]

Introducing Details and...

If there exists finite-fold Diophantine $\mathcal{D} \subseteq \mathbb{N} \times \mathbb{N}$ statifying

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.

then exponentiation is finite-fold Diophantine [Mat10]

Introducing Details and. . . Quit ASAP

If there exists finite-fold Diophantine $\mathcal{D} \subseteq \mathbb{N} \times \mathbb{N}$ statifying

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.

then exponentiation is finite-fold Diophantine [Mat10]

☞ 4 candidates for $\mathcal{D}$ proposed at CILC one year ago

Thank you for the attention!


Gregory Chaitin.
Algorithmic Information Theory.
Cambridge Univ. Press, Cambridge, 1987.


Martin Davis, Hilary Putnam, and Julia Robinson.
The decision problem for exponential Diophantine equations.
Annals of Mathematics, Second Series, 74(3):425–436, 1961.


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).


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

A "sibling" of the halting problem

One can find a concrete polynomial

$$H \in \mathbb{Z}[a, x_0, x_1, \ldots, x_\kappa, y, w]$$

such that

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

A "sibling" of the halting problem

One can find a concrete polynomial

$$H \in \mathbb{Z}[a, x_0, x_1, \ldots, x_\kappa, y, w]$$

such that

1. to each $a \in \mathbb{N}$, there corresponds at most one tuple $\langle v_0, v_1, \ldots, v_\kappa, u\rangle \in \mathbb{N}^{\kappa+2}$ s.t. $H(a, v_0, v_1, \ldots, v_\kappa, u, 2^u) > 0$;
2. to any monadic totally computable function $\mathcal{C}$, there correspond tuples $\langle a, v_0, v_1, \ldots, v_\kappa, u\rangle \in \mathbb{N}^{\kappa+3}$ s.t.

$$\begin{aligned} H(a, v_0, v_1, \ldots, v_\kappa, u, 2^u) &> 0 \quad \text{and} \\ \max\{v_0, v_1, \ldots, v_\kappa, u\} &> \mathcal{C}(a)\,. \end{aligned}$$

A "sibling" of the halting problem

One can find a concrete polynomial

$$H \in \mathbb{Z}[a, x_0, x_1, \ldots, x_\kappa, y, w]$$

such that

1. to each $a \in \mathbb{N}$, there corresponds at most one tuple $\langle v_0, v_1, \ldots, v_\kappa, u\rangle \in \mathbb{N}^{\kappa+2}$ s.t. $H(a, v_0, v_1, \ldots, v_\kappa, u, 2^u) > 0$;
2. to any monadic totally computable function $\mathcal{C}$, there correspond tuples $\langle a, v_0, v_1, \ldots, v_\kappa, u\rangle \in \mathbb{N}^{\kappa+3}$ s.t.

$$\begin{aligned} H(a, v_0, v_1, \ldots, v_\kappa, u, 2^u) &> 0 \qquad \text{and} \\ \max\{v_0, v_1, \ldots, v_\kappa, u\} &> \mathcal{C}(a)\,. \end{aligned}$$

Clue: Refer to an explicit enumeration $f_0, f_1, f_2, \ldots$ of all monadic partially computable functions and to a univocal representation D *à la* Matiyasevich of the relation $f_{a_1}(a_1) = a_2$, as shown above. Put:

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

Consider the increasing sequence

$$\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}} = \langle 0,\ 1,\ 4,\ 15,\ 56 \ldots \rangle$$

of all solutions to the equation

$$3\,y^2 + 1 \quad = \quad \square\ .$$

Put:

$$\mathcal{D}(p, q) \quad \Longleftrightarrow_{\mathsf{Def}} \quad \exists\, \ell\ \exists\, x \left[\, q = \boldsymbol{y}_{2^{2\,\ell+1}} \ \ \&\ \ q \ = \ (2\,x + 1)\,p \,\right].$$

Consider the increasing sequence

$$\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}} = \langle 0,\ 1,\ 4,\ 15,\ 56 \ldots \rangle$$

of all solutions to the equation

$$3\,y^2 + 1 \quad = \quad \square\ .$$

Put:

$$\mathcal{D}(p,q) \quad \Longleftrightarrow_{\mathsf{Def}} \quad \exists\,\ell\ \exists\,x \left[\, q = \boldsymbol{y}_{2^{2\,\ell+1}} \ \ \&\ \ q \ = \ (2\,x+1)\,p \,\right].$$

Then it turns out that $\mathcal{D}$ satisfies the above-stated condition and Julia Robinson's *exponential-growth* properties

$\mathcal{D}(p,q)$ implies $q < p^p$,
for each $k \geqslant 0$ there are p and q s.t. $\mathcal{D}(p,q)$ & $p^k < q$.

Consider the increasing sequence

$$\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}} = \langle 0,\ 1,\ 4,\ 15,\ 56 \ldots \rangle$$

of all solutions to the equation

$$3\,y^2 + 1 \quad = \quad \square \ .$$

Put:

$$\mathcal{D}(p,q) \quad \Longleftrightarrow_{\mathsf{Def}} \quad \exists\, \ell\ \exists\, x \left[\, q = \boldsymbol{y}_{2^{2\,\ell+1}} \ \ \&\ \ q \ = \ (2\,x+1)\,p \,\right].$$

Then it turns out that $\mathcal{D}$ satisfies the above-stated condition and Julia Robinson's *exponential-growth* properties

$$\mathcal{D}(p,q) \quad \text{implies} \quad q < p^p \ ,$$
$$\text{for each } k \geqslant 0 \text{ there are } p \text{ and } q \text{ s.t. } \mathcal{D}(p,q) \ \ \&\ \ p^k < q \ .$$

Also, $\mathcal{D}$ admits a finite-fold Diophantine repr. ***if*** the equation

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

admits at most finitely many solutions in $\mathbb{N}$.

A Prospected $\mathcal{D}$ (Omodeo–Cantone, 2017)

Consider the increasing sequence

$$\langle \boldsymbol{y}_i \rangle_{i \in \mathbb{N}} = \langle 0,\ 1,\ 4,\ 15,\ 56 \ldots \rangle$$

of all solutions to the equation

$$3\,y^2 + 1 \quad = \quad \square \ .$$

Put:

$$\mathcal{D}(p,q) \quad \Longleftrightarrow_{\mathsf{Def}} \quad \exists\, \ell\, \exists\, x \left[q = \boldsymbol{y}_{2^{2\,\ell+1}} \ \ \&\ \ q \ = \ (2\,x+1)\,p \right].$$

Then it turns out that $\mathcal{D}$ satisfies the above-stated condition and Julia Robinson's *exponential-growth* properties

$$\mathcal{D}(p,q) \quad \text{implies} \quad q < p^p \ ,$$
$$\text{for each } k \geqslant 0 \text{ there are } p \text{ and } q \text{ s.t. } \mathcal{D}(p,q) \ \ \&\ \ p^k < q \ .$$

Also, $\mathcal{D}$ admits a finite-fold Diophantine repr. ***if*** the equation

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

admits at most finitely many solutions in $\mathbb{N}$.