MATEMATYKA
DYSKRETNA
www.ii.uj.edu.pl/preMD/

Apoloniusz TYSZKA

A function which does not have any finite-fold Diophantine representation and probably equals $\Big\{(1,1)\Big\} \cup \left\{\left(n, 2^{2^{n-1}}\right) : n \in \{2,3,4,\ldots\}\right\}$

Preprint Nr MD 064
(otrzymany dnia 24 01 2013)

Kraków
2013

A function which does not have any finite-fold Diophantine representation and probably equals $\{(1,1)\} \cup \left\{\left(n, 2^{2^{n-1}}\right):\ n \in \{2,3,4,\ldots\}\right\}$

Apoloniusz Tyszka

Abstract

Let $g = \{(1,1)\} \cup \left\{\left(n, 2^{2^{n-1}}\right):\ n \in \{2,3,4,\ldots\}\right\}$. For a positive integer n, let $f(n)$ denote the smallest non-negative integer b such that for each system $S \subseteq \{x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k : i,j,k \in \{1,\ldots,n\}\}$ with a finite number of solutions in non-negative integers $x_1,\ldots,x_n$, all these solutions belong to $[0,b]^n$. We prove that the function f does not have any finite-fold Diophantine representation and $g(n) \leq f(n)$ for each n. We conjecture that $g = f$ and prove some corollaries of it.

Key words: Davis-Putnam-Robinson-Matiyasevich theorem, Diophantine equation with a finite number of solutions, finite-fold Diophantine representation.

2010 Mathematics Subject Classification: 03B30, 11U05.

The Davis-Putnam-Robinson-Matiyasevich theorem states that every recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a Diophantine representation, that is

$$(a_1,\ldots,a_n) \in \mathcal{M} \Longleftrightarrow \exists x_1,\ldots,x_m \in \mathbb{N}\ \ W(a_1,\ldots,a_n,x_1,\ldots,x_m) = 0 \qquad \text{(R)}$$

for some polynomial W with integer coefficients, see [4] and [3]. The polynomial W can be computed, if we know a Turing machine M such that, for all $(a_1,\ldots,a_n) \in \mathbb{N}^n$, M halts on $(a_1,\ldots,a_n)$ if and only if $(a_1,\ldots,a_n) \in \mathcal{M}$, see [4] and [3].

The representation (R) is said to be finite-fold if for any $a_1, \ldots, a_n \in \mathbb{N}$ the equation $W(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$ has at most finitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$.

Conjecture 1. *([2, pp. 341–342], [5, p. 42], [6, p. 79]) Each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a finite-fold Diophantine representation.*

Let $\mathcal{R}ng$ denote the class of all rings $\boldsymbol{K}$ that extend $\mathbb{Z}$. Th. Skolem proved that any Diophantine equation can be algorithmically transformed into an equivalent system of Diophantine equations of degree at most 2, see [7, pp. 2–3] and [4, pp. 3–4]. Let

$$E_n = \{x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}$$

The following result strengthens Skolem's theorem.

Lemma 1. *Let $D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$. Assume that $d_i = \deg(D, x_i) \geq 1$ for each $i \in \{1, \ldots, p\}$. We can compute a positive integer $n > p$ and a system $T \subseteq E_n$ which satisfies the following two conditions:*

`Condition 1.` *If $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}\}$, then*

$$\forall \tilde{x}_1, \ldots, \tilde{x}_p \in \boldsymbol{K} \Big(D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \Longleftrightarrow$$

$$\exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \boldsymbol{K}\ (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \textit{ solves } T\Big)$$

`Condition 2.` *If $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}\}$, then for each $\tilde{x}_1, \ldots, \tilde{x}_p \in \boldsymbol{K}$ with $D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0$, there exists a unique tuple $(\tilde{x}_{p+1}, \ldots, \tilde{x}_n) \in \boldsymbol{K}^{n-p}$ such that the tuple $(\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n)$ solves T.*

Conditions 1 and 2 imply that for each $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}\}$, the equation $D(x_1, \ldots, x_p) = 0$ and the system T have the same number of solutions in $\boldsymbol{K}$.

Proof. For $\boldsymbol{K} \in \mathcal{R}ng$, Lemma 1 is proved in [10]. We provide the proof for any $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}\}$. Let

$$D(x_1, \dots, x_p) = \sum a(i_1, \dots, i_p) \cdot x_1^{i_1} \cdot \ldots \cdot x_p^{i_p}$$

where $a(i_1, \dots, i_p)$ denote non-zero integers, and let M denote the maximum of the absolute values of the coefficients of $D(x_1, \dots, x_p)$. Let $\mathcal{T}$ denote the set of all polynomials $W(x_1, \dots, x_p) \in \mathbb{Z}[x_1, \dots, x_p]$ such that their coefficients belong to the interval $[0, M]$ and $\deg(W, x_i) \leq d_i$ for each $i \in \{1, \dots, p\}$. Let n denote the cardinality of $\mathcal{T}$. It is easy to check that

$$n = (M+1)^{(d_1+1) \cdot \ldots \cdot (d_p+1)} \geq 2^{2^p} > p$$

We define:

$$A(x_1, \dots, x_p) = \sum_{a(i_1, \dots, i_p) > 0} a(i_1, \dots, i_p) \cdot x_1^{i_1} \cdot \ldots \cdot x_p^{i_p}$$

$$B(x_1, \dots, x_p) = \sum_{a(i_1, \dots, i_p) < 0} -a(i_1, \dots, i_p) \cdot x_1^{i_1} \cdot \ldots \cdot x_p^{i_p}$$

The equation $D(x_1, \dots, x_p) = 0$ is equivalent to $0 + A(x_1, \dots, x_p) = B(x_1, \dots, x_p)$, where $0,\ A(x_1, \dots, x_p),\ B(x_1, \dots, x_p) \in \mathcal{T}$. We choose any bijection $\tau : \{1, \dots, n\} \longrightarrow \mathcal{T}$ such that $\tau(1) = x_1, \ \dots, \ \tau(p) = x_p$, and $\tau(p+1) = 0$. Let $\mathcal{H}$ denote the set of all equations from E_n which are identities in $\mathbb{Z}[x_1, \dots, x_p]$, if $x_i = \tau(i)$ for each $i \in \{1, \dots, n\}$. Since $\tau(p+1) = 0$, the equation $x_{p+1} + x_{p+1} = x_{p+1}$ belongs to $\mathcal{H}$. We define T as $\mathcal{H} \cup \{x_{p+1} + x_s = x_t\}$, where $s = \tau^{-1}(A(x_1, \dots, x_p))$ and $t = \tau^{-1}(B(x_1, \dots, x_p))$. For each $\tilde{x}_1, \dots, \tilde{x}_p \in \boldsymbol{K}$ with $D(\tilde{x}_1, \dots, \tilde{x}_p) = 0$, the sought-for elements $\tilde{x}_{p+1}, \dots, \tilde{x}_n \in \boldsymbol{K}$ exist, are unique, and satisfy

$$\forall i \in \{p+1, \dots, n\} \ \ \tilde{x}_i = \tau(i)[x_1 \mapsto \tilde{x}_1, \dots, x_p \mapsto \tilde{x}_p]$$

$\square$

For a positive integer n, let $f(n)$ denote the smallest non-negative integer b such that for each system $S \subseteq E_n$ with a finite number of solutions in non-negative integers $x_1, \ldots, x_n$, all these solutions belong to $[0, b]^n$. We find that $f(1) = 1$ and $f(2) = 4$, because the value of $f(1)$ is attained by the system $\{x_1 = 1\}$ and the value of $f(2)$ is attained by the system $\{x_1 + x_1 = x_2,\ x_1 \cdot x_1 = x_2\}$.

Lemma 2. *For each integer $n \geq 2$, $f(n+1) \geq f(n)^2 > f(n)$.*

Proof. If a system $S \subseteq E_n$ has only finitely many solutions in non-negative integers $x_1, \ldots, x_n$, then for each $i \in \{1, \ldots, n\}$ the system $S \cup \{x_i \cdot x_i = x_{n+1}\} \subseteq E_{n+1}$ has only finitely many solutions in non-negative integers $x_1, \ldots, x_{n+1}$. □

Theorem. *The function f does not have any finite-fold Diophantine representation.*

Proof. Assume, on the contrary, that there is a finite-fold Diophantine representation of f. By Lemma 1, there is an integer $s \geq 3$ such that for any non-negative integers x_1, x_2,

$$(x_1, x_2) \in f \Longleftrightarrow \exists x_3, \ldots, x_s \in \mathbb{N}\ \ \Phi(x_1, x_2, x_3, \ldots, x_s), \tag{E}$$

where the formula $\Phi(x_1, x_2, x_3, \ldots, x_s)$ is a conjunction of formulae of the forms $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ ($i, j, k \in \{1, \ldots, s\}$) and

(FF) for each non-negative integers x_1, x_2 at most finitely many tuples $(x_3, \ldots, x_s) \in \mathbb{N}^{s-2}$ satisfy $\Phi(x_1, x_2, x_3, \ldots, x_s)$.

Let S denote the following system

$$\left\{\begin{array}{rcl}
\multicolumn{3}{l}{\text{all equations occurring in } \Phi(x_1, x_2, x_3, \ldots, x_s)} \\
t_1 & = & 1 \\
t_1 + t_1 & = & t_2 \\
t_1 + t_2 & = & t_3 \\
 & \ldots & \\
t_1 + t_s & = & t_{s+1} \\
t_{s+1} + t_{s+1} & = & x_1
\end{array}\right.$$

with $2s+1$ variables. By the equivalence `(E)`, the system S is satisfiable over non-negative integers. The condition `(FF)` implies that S has only finitely many solutions in non-negative integers. If a tuple $(x_1, x_2, x_3, \ldots, x_s, t_1, \ldots, t_{s+1})$ of non-negative integers solves S, then $x_1 = 2s+2$. By the equivalence `(E)` and Lemma 2,

$$x_2 = f(x_1) = f(2s+2) > f(2s+1)$$

The inequality $x_2 > f(2s+1)$ contradicts the definition of $f(2s+1)$, as the system S contains $2s+1$ variables. □

Let $g = \{(1,1)\} \cup \left\{\left(n, 2^{2^{n-1}}\right) :\ n \in \{2,3,4,\ldots\}\right\}$. The system

$$\begin{cases} x_1 + x_1 &= x_2 \\ x_1 \cdot x_1 &= x_2 \\ x_2 \cdot x_2 &= x_3 \\ x_3 \cdot x_3 &= x_4 \\ & \ldots \\ x_{n-1} \cdot x_{n-1} &= x_n \end{cases}$$

has exactly two integer solutions, namely $(0, \ldots, 0)$ and $\left(2, 4, 16, 256, \ldots, 2^{2^{n-2}}, 2^{2^{n-1}}\right)$. Therefore, $g(n) \leq f(n)$ for each n. The following Conjecture 2 contradicts Conjecture 1, as it will follow from Corollary 2 or Corollary 3.

Conjecture 2. $g = f$.

Question. *Does there exist an algorithm which to each Diophantine equation assigns an integer which is greater than the heights of integer (non-negative integer, positive integer, rational) solutions, if these solutions form a finite set?*

Conjecture 2 provides an affirmative answer to the Question and implies the following three corollaries.

Corollary 1. *(cf. [1], [8], [9], [11]) There is an algorithm which to each Diophantine equation assigns an integer which is greater than the heights of integer (non-negative integer, positive integer, rational) solutions, if these solutions form a finite set.*

Corollary 2. *The function* $\mathbb{N} \ni n \to 2^n \in \mathbb{N}$ *does not have any finite-fold Diophantine representation.*

Proof. Assume, on the contrary, that there is a finite-fold Diophantine representation of the function $\mathbb{N} \ni n \to 2^n \in \mathbb{N}$. Then, Conjecture 1 is true ([5, p. 42]). This conclusion implies a negative answer to the Question restricted to non-negative integer solutions ([5, p. 42]). By this and Corollary 1, Conjecture 2 is false, a contradiction. □

Corollary 3. *If a set* $\mathcal{M} \subseteq \mathbb{N}$ *is recursively enumerable but not recursive, then a finite-fold Diophantine representation of* $\mathcal{M}$ *does not exist.*

Proof. Let $\mathcal{M} \subseteq \mathbb{N}$ be recursively enumerable but not recursive. Assume, on the contrary, that $\mathcal{M}$ has a finite-fold Diophantine representation. It means that there exists a polynomial $W(x, x_1, \ldots, x_m)$ with integer coefficients such that

$$\forall a \in \mathbb{N} \left(a \in \mathcal{M} \Longleftrightarrow \exists x_1, \ldots, x_m \in \mathbb{N} \;\; W(a, x_1, \ldots, x_m) = 0\right)$$

and for any $a \in \mathbb{N}$ the equation $W(a, x_1, \ldots, x_m) = 0$ has at most finitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$. By Corollary 1, there is a computable function $h : \mathbb{N} \to \mathbb{N}$ such that

$$\forall a, x_1, \ldots, x_m \in \mathbb{N} \left(W(a, x_1, \ldots, x_m) = 0 \Longrightarrow \max(x_1, \ldots, x_m) \leq h(a)\right)$$

Hence, we can decide whether a non-negative integer a belongs to $\mathcal{M}$ by checking whether the equation $W(a, x_1, \ldots, x_m) = 0$ has an integer solution in the box $[0, h(a)]^m$, a contradiction. □

References

[1] M. Cipu, *Small solutions to systems of polynomial equations with integer coefficients,* An. St. Univ. Ovidius Constanta 19 (2011), no. 2, 89–100, `http://www.emis.de/journals/ASUO/mathematics/pdf23/Cipu.pdf`, `http://www.anstuocmath.ro/mathematics/pdf23/Cipu.pdf`.

[2] M. Davis, Yu. Matiyasevich, J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution,* in: Mathematical developments arising from Hilbert problems (ed. F. E. Browder), Proc. Sympos. Pure Math., vol. 28, Part 2, Amer. Math. Soc., 1976, 323–378; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., 1996, 269–324.

[3] L. B. Kuijer, *Creating a diophantine description of a r.e. set and on the complexity of such a description,* MSc thesis, Faculty of Mathematics and Natural Sciences, University of Groningen, 2010, `http://irs.ub.rug.nl/dbi/4b87adf513823`.

[4] Yu. Matiyasevich, *Hilbert's tenth problem,* MIT Press, Cambridge, MA, 1993.

[5] Yu. Matiyasevich, *Hilbert's tenth problem: what was done and what is to be done.* Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 1–47, Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000.

[6] Yu. Matiyasevich, *Towards finite-fold Diophantine representations,* Zap. Nauchn. Sem. S.-Petersburg. Otdel. Mat. Inst. Steklov. (POMI) 377 (2010), 78–90, `ftp://ftp.pdmi.ras.ru/pub/publicat/znsl/v377/p078.pdf`.

[7] Th. Skolem, *Diophantische Gleichungen*, Julius Springer, Berlin, 1938.

[8] A. Tyszka, *A hypothetical upper bound for the solutions of a Diophantine equation with a finite number of solutions,* `http://arxiv.org/abs/0901.2093`.

[9] A. Tyszka, *How to solve a Diophantine equation with a finite number of integer solutions (in Polish)*, Matematyka-Społeczeństwo-Nauczanie, no. 50, January 2013, 16–20, `http://www.cyf-kr.edu.pl/~rttyszka/msn.pdf`.

[10] A. Tyszka, K. Molenda, M. Sporysz, *An algorithm which transforms any Diophantine equation into an equivalent system of equations of the forms* $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$, Int. Math. Forum 8 (2013), no. 1, 31–37, `http://m-hikari.com/imf/imf-2013/1-4-2013/tyszkaIMF1-4-2013-1.pdf`.

[11] A. Tyszka, M. Sporysz, A. Peszek, *A conjecture on integer arithmetic which implies that there is an algorithm which to each Diophantine equation assigns an integer which is greater than the heights of integer (non-negative integer, rational) solutions, if these solutions form a finite set,* Int. Math. Forum 8 (2013), no. 1, 39–46, `http://m-hikari.com/imf/imf-2013/1-4-2013/tyszkaIMF1-4-2013-2.pdf`.

Apoloniusz Tyszka
University of Agriculture
Faculty of Production and Power Engineering
Balicka 116B, 30-149 Kraków, Poland
E-mail: `rttyszka@cyf-kr.edu.pl`