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

Apoloniusz TYSZKA

Is there an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the number of integer solutions if the solution set is finite?

Preprint Nr MD 067
(otrzymany dnia 14.06.2013)

Kraków
2013

Is there an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the number of integer solutions if the solution set is finite?

Apoloniusz Tyszka

Abstract

Let $E_n = \{x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\}\}$. For a positive integer n, let $f(n)$ denote the greatest finite total number of solutions of a subsystem of E_n in integers $x_1, \ldots, x_n$. We prove: (1) the function f is strictly increasing, (2) if a non-decreasing function g from positive integers to positive integers satisfies $f(n) \leq g(n)$ for any n, then a finite-fold Diophantine representation of g does not exist, (3) if the question of the title has a positive answer, then there is a computable strictly increasing function g from positive integers to positive integers such that $f(n) \leq g(n)$ for any n and a finite-fold Diophantine representation of g does not exist.

Key words: Davis-Putnam-Robinson-Matiyasevich theorem, finite-fold Diophantine representation.

2010 Mathematics Subject Classification: 03D25, 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

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

for some polynomial W with integer coefficients, see [3] and [2]. 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 [3] and [2].

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 only finitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$.

Open Problem ([1, pp. 341–342], [4, p. 42], [5, p. 79]). *Does 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 [6, pp. 2–3] and [3, 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:*

(4) *If* $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}\}$*, then*

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

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

(5) *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 (4) *and* (5) *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 [7]. We provide the proof for any $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}\}$. Let

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

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

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

□

For a positive integer n, let $f(n)$ denote the greatest finite total number of solutions of a subsystem of E_n in integers $x_1,\dots,x_n$. Obviously, $f(1)=2$ as the equation $x_1\cdot x_1=x_1$ has exactly two integer solutions.

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

Proof. If r is a positive integer and a system $S\subseteq E_n$ has exactly r solutions in integers $x_1,\dots,x_n$, then the system $S\cup\{x_{n+1}\cdot x_{n+1}=x_{n+1}\}\subseteq E_{n+1}$ has exactly $2r$ solutions in integers $x_1,\dots,x_{n+1}$. □

Corollary. *The function f is strictly increasing.*

A function $\beta:\mathbb{N}\setminus\{0\}\to\mathbb{N}\setminus\{0\}$ is said to majorize a function $\alpha:\mathbb{N}\setminus\{0\}\to\mathbb{N}\setminus\{0\}$ provided $\alpha(n)\leq\beta(n)$ for any n.

Theorem 1. *If a non-decreasing function $g:\mathbb{N}\setminus\{0\}\to\mathbb{N}\setminus\{0\}$ majorizes f, then a finite-fold Diophantine representation of g does not exist.*

Proof. Assume, on the contrary, that there is a finite-fold Diophantine representation of g. It means that there is a polynomial $W(x_1,x_2,x_3,\dots,x_m)$ with integer coefficients such that

(6) for any non-negative integers x_1, x_2,

$$(x_1, x_2) \in g \Longleftrightarrow \exists x_3, \dots, x_m \in \mathbb{N} \;\; W(x_1, x_2, x_3, \dots, x_m) = 0$$

and for each non-negative integers x_1, x_2 at most finitely many tuples $(x_3, \dots, x_m) \in \mathbb{N}^{m-2}$ satisfy $W(x_1, x_2, x_3, \dots, x_m) = 0$. By Lemma 1, there is a formula $\Phi(x_1, x_2, x_3, \dots, x_s)$ such that

(7) $s \geq \max(m, 3)$ and $\Phi(x_1, x_2, x_3, \dots, x_s)$ is a conjunction of formulae of the forms $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ $(i, j, k \in \{1, \dots, s\})$ which equivalently expresses that $W(x_1, x_2, x_3, \dots, x_m) = 0$ and each x_i $(i = 1, \dots, m)$ is a sum of four squares.

Let S denote the following system

$$\begin{cases}
a \cdot a = A \\
b \cdot b = B \\
c \cdot c = C \\
d \cdot d = D \\
A + B = u_1 \\
C + D = u_2 \\
u_1 + u_2 = u_3 \\
\tilde{a} \cdot \tilde{a} = \tilde{A} \\
\tilde{b} \cdot \tilde{b} = \tilde{B} \\
\tilde{c} \cdot \tilde{c} = \tilde{C} \\
\tilde{d} \cdot \tilde{d} = \tilde{D} \\
\tilde{A} + \tilde{B} = \tilde{u}_1 \\
\tilde{C} + \tilde{D} = \tilde{u}_2 \\
\tilde{u}_1 + \tilde{u}_2 = \tilde{u}_3 \\
u_3 + \tilde{u}_3 = x_2 \\
t_1 = 1 \\
t_1 + t_1 = t_2 \\
t_2 \cdot t_2 = t_3 \\
t_3 \cdot t_3 = t_4 \\
\dots \\
t_{s-1} \cdot t_{s-1} = t_s \\
t_s \cdot t_s = t_{s+1} \\
t_{s+1} \cdot t_{s+1} = x_1 \\
\text{all equations occurring in } \Phi(x_1, x_2, x_3, \dots, x_s)
\end{cases}$$

with $2s + 23$ variables. The system S equivalently expresses the following conjunction:

$$\left(\left(a^2 + b^2 + c^2 + d^2\right) + \left(\tilde{a}^2 + \tilde{b}^2 + \tilde{c}^2 + \tilde{d}^2\right) = x_2\right) \wedge \left(x_1 = 2^{2^s}\right) \wedge \Phi(x_1, x_2, x_3, \dots, x_s)$$

Conditions (6)-(7) and Lagrange's four-square theorem imply that the system S is satisfiable over integers and has only finitely many integer solutions. Let L denote the number of integer solutions to S. If an integer tuple solves S, then $x_1 = 2^{2^s}$ and $x_2 = g(x_1) = g\left(2^{2^s}\right)$. Since the equation $u_3 + \tilde{u}_3 = x_2$ belongs to S and Lagrange's four-square theorem holds, $L \geq g\left(2^{2^s}\right) + 1$. The definition of f implies that

$$L \leq f\,(2s + 23) \tag{8}$$

Since g majorizes f,

$$f\,(2s + 23) < g\,(2s + 23) + 1 \tag{9}$$

Since $s \geq 3$ and g is non-decreasing,

$$g\,(2s + 23) + 1 \leq g\left(2^{2^s}\right) + 1 \tag{10}$$

Inequalities (8)-(10) imply that $L < g\left(2^{2^s}\right) + 1$, a contradiction. □

Theorem 2. *If the question of the title has a positive answer, then there is a computable strictly increasing function* $g : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ *such that* g *majorizes* f *and a finite-fold Diophantine representation of* g *does not exist.*

Proof. For each positive integer r, there are only finitely many Diophantine equations whose lengths are not greater than r, and these equations can be algorithmically constructed. This and the assumption that the question of the title has a positive answer imply that there exists a computable function $\delta : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ such that for each positive integer r and for each Diophantine equation whose length is not greater than r, $\delta(r)$ is greater than the number of integer solutions if the solution set is finite. There is a computable function $\psi : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ such that each subsystem of E_n is equivalent to a Diophantine equation whose length is not greater than $\psi(n)$. The function

$$\mathbb{N} \setminus \{0\} \ni n \stackrel{h}{\longmapsto} \delta(\psi(n)) \in \mathbb{N} \setminus \{0\}$$

is computable. The definition of f implies that h majorizes f. The function

$$\mathbb{N} \setminus \{0\} \ni n \stackrel{g}{\longmapsto} \sum_{i=1}^{n} h(i) \in \mathbb{N} \setminus \{0\}$$

is computable and strictly increasing. Since g majorizes h and h majorizes f, g majorizes f. By Theorem 1, a finite-fold Diophantine representation of g does not exist. □

References

[1] 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.

[2] 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`.

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

[4] 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.

[5] 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`.

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

[7] 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.

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