DOI: 10.2478/auom-2013-0059
An. Şt. Univ. Ovidius Constanţa
VERSITA
Vol. 21(3),2013, 289–293

A new characterization of computable functions

Apoloniusz Tyszka

Abstract

Let $E_n = \{x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k :\ i, j, k \in \{1, \ldots, n\}\}$. We present two algorithms. The first accepts as input any computable function $f : \mathbb{N} \to \mathbb{N}$ and returns a positive integer $m(f)$ and a computable function g which to each integer $n \geq m(f)$ assigns a system $S \subseteq E_n$ such that S is satisfiable over integers and each integer tuple $(x_1, \ldots, x_n)$ that solves S satisfies $x_1 = f(n)$. The second accepts as input any computable function $f : \mathbb{N} \to \mathbb{N}$ and returns a positive integer $w(f)$ and a computable function h which to each integer $n \geq w(f)$ assigns a system $S \subseteq E_n$ such that S is satisfiable over non-negative integers and each tuple $(x_1, \ldots, x_n)$ of non-negative integers that solves S satisfies $x_1 = f(n)$.

Let

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

and 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], [5, pp. 3–4], [1, pp. 386–387, proof of Theorem 1], and [3, pp. 262–263, proof of Theorem 7.5]. The following result strengthens Skolem's theorem.

Lemma ([7]). *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:*

Key Words: computable function, Davis-Putnam-Robinson-Matiyasevich theorem.
2010 Mathematics Subject Classification: Primary 03D20; Secondary 11U09.
Received: October 2012
Revised:January 2013
Accepted: January 2013

Condition 1. *If* $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N},\ \mathbb{N} \setminus \{0\}\}$*, 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* $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N},\ \mathbb{N} \setminus \{0\}\}$*, 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 $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N},\ \mathbb{N} \setminus \{0\}\}$*, the equation* $D(x_1, \ldots, x_p) = 0$ *and the system* T *have the same number of solutions in* $\boldsymbol{K}$*.*

For $\boldsymbol{K} \in \mathcal{R}ng$, the Lemma is proved in [8]. For concrete Diophantine equations, it is possible to find much smaller equivalent systems of equations of the forms $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$, see [2].

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

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

for some polynomial W with integer coefficients, see [5] and [4]. 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 [5] and [4].

Theorem 1. *There is an algorithm which accepts as input any computable function* $f : \mathbb{N} \to \mathbb{N}$ *and returns a positive integer* $m(f)$ *and a computable function* g *which to each integer* $n \geq m(f)$ *assigns a system* $S \subseteq E_n$ *such that* S *is satisfiable over integers and each integer tuple* $(x_1, \ldots, x_n)$ *that solves* S *satisfies* $x_1 = f(n)$*.*

Proof. By the Davis-Putnam-Robinson-Matiyasevich theorem, the function f has a Diophantine representation. It means that there is a polynomial $W(x_1, x_2, x_3, \ldots, x_r)$ with integer coefficients such that for each non-negative integers x_1, x_2,

$$x_1 = f(x_2) \Longleftrightarrow \exists x_3, \ldots, x_r \in \mathbb{N}\ \ W(x_1, x_2, x_3, \ldots, x_r) = 0 \qquad \text{(E1)}$$

By the equivalence (E1) and Lagrange's four-square theorem, for any integers x_1, x_2, the conjunction $(x_2 \geq 0) \wedge (x_1 = f(x_2))$ holds true if and only if there exist integers

$$a, b, c, d, \alpha, \beta, \gamma, \delta, x_3, x_{3,1}, x_{3,2}, x_{3,3}, x_{3,4}, \ldots, x_r, x_{r,1}, x_{r,2}, x_{r,3}, x_{r,4}$$

such that

$$W^2(x_1, x_2, x_3, \ldots, x_r) + (x_1 - a^2 - b^2 - c^2 - d^2)^2 + (x_2 - \alpha^2 - \beta^2 - \gamma^2 - \delta^2)^2 +$$

$$(x_3 - x_{3,1}^2 - x_{3,2}^2 - x_{3,3}^2 - x_{3,4}^2)^2 + \ldots + (x_r - x_{r,1}^2 - x_{r,2}^2 - x_{r,3}^2 - x_{r,4}^2)^2 = 0$$

By the Lemma for $\boldsymbol{K} = \mathbb{Z}$, there is an integer $s \geq 3$ such that for any integers x_1, x_2,

$$\Big(x_2 \geq 0 \wedge x_1 = f(x_2)\Big) \Longleftrightarrow \exists x_3, \ldots, x_s \in \mathbb{Z}\ \ \Psi(x_1, x_2, x_3, \ldots, x_s) \qquad \texttt{(E2)}$$

where the formula $\Psi(x_1, x_2, x_3, \ldots, x_s)$ is algorithmically determined as a conjunction of formulae of the forms:

$$x_i = 1, \quad x_i + x_j = x_k, \quad x_i \cdot x_j = x_k \quad (i, j, k \in \{1, \ldots, s\})$$

Let $m(f) = 4 + 2s$, and let $[\cdot]$ denote the integer part function. For each integer $n \geq m(f)$,

$$n - \left[\frac{n}{2}\right] - 2 - s \geq m(f) - \left[\frac{m(f)}{2}\right] - 2 - s \geq m(f) - \frac{m(f)}{2} - 2 - s = 0$$

Let S denote the following system

$$\begin{cases} \text{all equations occurring in } \Psi(x_1, x_2, x_3, \ldots, x_s) \\ \quad n - \left[\frac{n}{2}\right] - 2 - s \text{ equations of the form } z_i = 1 \\ \qquad\qquad\qquad\qquad t_1 = 1 \\ \qquad\qquad\qquad\qquad t_1 + t_1 = t_2 \\ \qquad\qquad\qquad\qquad t_2 + t_1 = t_3 \\ \qquad\qquad\qquad\qquad \ldots \\ \qquad\qquad\qquad\qquad t_{[\frac{n}{2}]-1} + t_1 = t_{[\frac{n}{2}]} \\ \qquad\qquad\qquad\qquad t_{[\frac{n}{2}]} + t_{[\frac{n}{2}]} = w \\ \qquad\qquad\qquad\qquad w + y = x_2 \\ \qquad\qquad\qquad\qquad y + y = y \text{ (if } n \text{ is even)} \\ \qquad\qquad\qquad\qquad y = 1 \text{ (if } n \text{ is odd)} \end{cases}$$

with n variables. By the equivalence (E2), the system S is satisfiable over integers. If an integer n-tuple $(x_1, x_2, x_3, \ldots, x_s, \ldots, w, y)$ solves S, then by the equivalence (E2),

$$x_1 = f(x_2) = f(w + y) = f\left(2 \cdot \left[\frac{n}{2}\right] + y\right) = f(n)$$

□

A simpler proof, not using Lagrange's four-square theorem, suffices if we consider solutions in non-negative integers.

Theorem 2. *There is an algorithm which accepts as input any computable function $f : \mathbb{N} \to \mathbb{N}$ and returns a positive integer $w(f)$ and a computable function h which to each integer $n \geq w(f)$ assigns a system $S \subseteq E_n$ such that S is satisfiable over non-negative integers and each tuple $(x_1, \ldots, x_n)$ of non-negative integers that solves S satisfies $x_1 = f(n)$.*

Proof. We omit the construction of S because a similar construction is carried out in the proof of Theorem 1. The rest of the proof follows from the Lemma for $\boldsymbol{K} = \mathbb{N}$. □

For a function $f : \mathbb{N} \to \mathbb{N}$, let $\mathbb{Z}(f)$ denote the smallest $m \in \{1, 2, 3, \ldots\} \cup \{\infty\}$ such that for any integer $n \geq m$ there exists a system $S \subseteq E_n$ such that S is satisfiable over integers and each integer tuple $(x_1, \ldots, x_n)$ that solves S satisfies $x_1 = f(n)$.

For a function $f : \mathbb{N} \to \mathbb{N}$, let $\mathbb{N}(f)$ denote the smallest $w \in \{1, 2, 3, \ldots\} \cup \{\infty\}$ such that for any integer $n \geq w$ there exists a system $S \subseteq E_n$ such that S is satisfiable over non-negative integers and each tuple $(x_1, \ldots, x_n)$ of non-negative integers that solves S satisfies $x_1 = f(n)$.

The definition of $\mathbb{Z}(f)$ immediately implies that $\mathbb{Z}(f) = 1$ for any $f : \mathbb{N} \to \{0, 1\}$. By this and Theorem 1, we have the following.

Theorem 3. *For any $f : \mathbb{N} \to \mathbb{N}$, if f is computable, then $\mathbb{Z}(f) < \infty$, but not vice versa.*

The analogous theorem holds for $\mathbb{N}(f)$.

References

[1] J. L. Britton, *Integer solutions of systems of quadratic equations,* Math. Proc. Cambridge Philos. Soc. 86 (1979), no. 3, 385–389.

[2] 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.

[3] M. Davis, *Hilbert's tenth problem is unsolvable,* Amer. Math. Monthly 80 (1973), no. 3, 233–269.

[4] 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.

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

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

[7] A. Tyszka, *Conjecturally computable functions which unconditionally do not have any finite-fold Diophantine representation,* Inform. Process. Lett. 113 (2013), no. 19-21, 719–722.

[8] A. Tyszka, *Does there exist an algorithm which to each Diophantine equation assigns an integer which is greater than the modulus of integer solutions, if these solutions form a finite set?* Fund. Inform. 125(1): 95–99, 2013.

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