arXiv:1011.4103v1 [math.LO] 17 Nov 2010

A hypothetical answer to the question of when a sufficiently large number of elements confirm that the set is infinite

Apoloniusz Tyszka

Abstract. We present a conjecture on integer arithmetic which implies that there is an algorithm that for each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}$ given by a Diophantine representation computes a positive integer $t(\mathcal{M})$ with the following property: if there exists $m \in \mathcal{M}$ with $m > t(\mathcal{M})$, then $\mathcal{M}$ is infinite.

Key words and phrases: Davis-Putnam-Robinson-Matiyasevich theorem, Diophantine representation, recursively enumerable set.

2010 Mathematics Subject Classification: 03B30, 03D25, 11U99.

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 [1]. We present a conjecture on integer arithmetic which implies that there is an algorithm that for each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}$ given by a Diophantine representation computes a positive integer $t(\mathcal{M})$ with the following property: if there exists $m \in \mathcal{M}$ with $m > t(\mathcal{M})$, then $\mathcal{M}$ is infinite.

Conjecture ([2]). For each integers $x_1, \ldots, x_n$ there exist integers $y_1, \ldots, y_n$ such that

$$(2^{2^{n-1}} < |x_1| \Longrightarrow |x_1| < |y_1|) \wedge$$

$$(\forall i, j, k \in \{1, \ldots, n\} \; (x_i + x_j = x_k \Longrightarrow y_i + y_j = y_k)) \wedge \tag{$S\,1$}$$

$$\forall i, j, k \in \{1, \ldots, n\} \; (x_i \cdot x_j = x_k \Longrightarrow y_i \cdot y_j = y_k) \tag{$S\,2$}$$

For $n \geq 2$, the bound $2^{2^{n-1}}$ cannot be decreased because for

$$(x_1, \ldots, x_n) = (2^{2^{n-1}}, 2^{2^{n-2}}, 2^{2^{n-3}}, \ldots, 256, 16, 4, 2)$$

the conjunction of statements $(S\,1)$ and $(S\,2)$ guarantees that

$$(y_1, \ldots, y_n) = (0, \ldots, 0) \vee (y_1, \ldots, y_n) = (2^{2^{n-1}}, 2^{2^{n-2}}, 2^{2^{n-3}}, \ldots, 256, 16, 4, 2)$$

For a Diophantine equation $D(x_1, \ldots, x_p) = 0$, let M denote the maximum of the absolute values of its coefficients. Let $\mathcal{T}$ denote the family of all polynomials $W(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$ whose all coefficients belong to the interval $[-M, M]$ and $\deg(W, x_i) \leq d_i = \deg(D, x_i)$ for each $i \in \{1, \ldots, p\}$. Here we consider the degrees of $W(x_1, \ldots, x_p)$ and $D(x_1, \ldots, x_p)$ with respect to the variable x_i. It is easy to check that

$$\mathrm{card}(\mathcal{T}) = (2M + 1)^{(d_1 + 1) \cdot \ldots \cdot (d_p + 1)}$$

To each polynomial that belongs to $\mathcal{T} \setminus \{x_1, \ldots, x_p\}$ we assign a new variable x_i with $i \in \{p + 1, \ldots, \mathrm{card}(\mathcal{T})\}$. Then, $D(x_1, \ldots, x_p) = x_q$ for some $q \in \{1, \ldots, \mathrm{card}(\mathcal{T})\}$. Let $\mathcal{H}$ denote the family of all equations of the form

$$x_i = 1,\ x_i + x_j = x_k,\ x_i \cdot x_j = x_k \ \ (i, j, k \in \{1, \ldots, \mathrm{card}(\mathcal{T})\})$$

which are polynomial identities in $\mathbb{Z}[x_1, \ldots, x_p]$. If some variable x_m is assigned to a polynomial $W(x_1, \ldots, x_p) \in \mathcal{T}$, then for each ring $\boldsymbol{K}$ extending $\mathbb{Z}$ the system $\mathcal{H}$ implies $W(x_1, \ldots, x_p) = x_m$. This observation proves the following Lemma.

Lemma. The system $\mathcal{H} \cup \{x_q + x_q = x_q\}$ is algorithmically determinable. For each ring $\boldsymbol{K}$ extending $\mathbb{Z}$, the equation $D(x_1, \ldots, x_p) = 0$ is equivalent to the system $\mathcal{H} \cup \{x_q + x_q = x_q\}$. Formally, this equivalence can be written as

$$\forall x_1, \ldots, x_p \in \boldsymbol{K} \Big(D(x_1, \ldots, x_p) = 0 \Longleftrightarrow \exists x_{p+1}, \ldots, x_{\mathrm{card}(\mathcal{T})} \in \boldsymbol{K}$$

$$(x_1, \ldots, x_p, x_{p+1}, \ldots, x_{\mathrm{card}(\mathcal{T})}) \text{ solves the system } \mathcal{H} \cup \{x_q + x_q = x_q\} \Big)$$

Theorem. The Conjecture implies that there is an algorithm that for each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}$ given by a Diophantine representation computes a threshold number $t(\mathcal{M}) \in \mathbb{N}$ with the following property: if there exists $x_1 \in \mathcal{M}$ with $x_1 > t(\mathcal{M})$, then $\mathcal{M}$ is infinite.

Proof. There is a polynomial $W(x, x_1, \ldots, x_m)$ with integer coefficients for which the formula

$$\exists x_1 \ldots \exists x_m \ W(x, x_1, \ldots, x_m) = 0$$

defines $\mathcal{M}$ in $\mathbb{N}$. By Lagrange's four-square theorem, the formula

$$\exists a, b, c, d, x_1, a_1, b_1, c_1, d_1, \ldots, x_m, a_m, b_m, c_m, d_m \quad W^2(x, x_1, \ldots, x_m) +$$

$$(x - a^2 - b^2 - c^2 - d^2)^2 + (x_1 - a_1^2 - b_1^2 - c_1^2 - d_1^2)^2 + \ldots + (x_m - a_m^2 - b_m^2 - c_m^2 - d_m^2)^2 = 0$$

defines $\mathcal{M}$ in $\mathbb{Z}$. By the Lemma, $\mathcal{M}$ is defined in $\mathbb{Z}$ by a formula

$$\exists x_2 \ldots \exists x_n \; \Omega(x_1, x_2, \ldots, x_n)$$

where $\Omega(x_1, x_2, \ldots, x_n)$ is a conjunction of formulae of the form $x_i = 1$, $x_i + x_j = x_k$, $x_i \cdot x_j = x_k$ $(i, j, k \in \{1, \ldots, n\})$ and n can be algorithmically computed. We put $t(\mathcal{M}) = 2^{2^{n-1}}$. Assume that $x_1 \in \mathcal{M}$ and $x_1 > t(\mathcal{M})$. Then, there exist integers $x_2, \ldots, x_n$ satisfying

$$(2^{2^{n-1}} < x_1) \wedge \Omega(x_1, x_2, \ldots, x_n)$$

We apply the Conjecture to the tuple $(x_1, x_2, \ldots, x_n)$ and obtain an integer tuple $(y_1, y_2, \ldots, y_n)$ whose elements satisfy

$$(2^{2^{n-1}} < x_1 < y_1) \; \wedge \; \Omega(y_1, y_2, \ldots, y_n)$$

By repeating this argument and applying induction, we complete the proof.

□

Assuming the Conjecture, we can use the Theorem to prove that a particular recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}$ is infinite. Of course, we disregard here the time for finding $x_1 \in \mathcal{M}$ with $x_1 > t(\mathcal{M})$. For example, the largest known twin prime is much smaller than the threshold number computed for the set $\{p \in \mathbb{N} : (p \text{ is prime }) \wedge (p + 2 \text{ is prime})\}$.

References

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

[2] A. Tyszka, *Two hypothetical properties of integer arithmetic and their consequences for Diophantine problems*, `http://arxiv.org/abs/0901.2093`.

Apoloniusz Tyszka
Technical Faculty
Hugo Kołłątaj University
Balicka 116B, 30-149 Kraków, Poland
E-mail address: `rttyszka@cyf-kr.edu.pl`