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

Apoloniusz TYSZKA

A conjecture on rational arithmetic which allows us to compute an upper bound for the heights of rational solutions of a Diophantine equation with a finite number of solutions

Preprint Nr MD 086
(otrzymany dnia 13.05.2016)

Kraków
2016

A conjecture on rational arithmetic which allows us to compute an upper bound for the heights of rational solutions of a Diophantine equation with a finite number of solutions

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

***Abstract*—The height of a rational number $\frac{p}{q}$ is denoted by $h\left(\frac{p}{q}\right)$ and equals $\max(|p|,|q|)$ provided $\frac{p}{q}$ is written in lowest terms. The height of a rational tuple $(x_1,\ldots,x_n)$ is denoted by $h(x_1,\ldots,x_n)$ and equals $\max(h(x_1),\ldots,h(x_n))$. Let $G_n = \{x_i+1=x_k,\ x_i \cdot x_j = x_k:\ i,j,k \in \{1,\ldots,n\}\}$. We conjecture that if a system $S \subseteq G_n$ has only finitely many solutions in rationals $x_1,\ldots,x_n$, then each such solution $(x_1,\ldots,x_n)$ satisfies $h(x_1,\ldots,x_n) \leqslant \begin{cases} 1 & (\text{if } n=1) \\ 2^{2^{n-2}} & (\text{if } n \geqslant 2) \end{cases}$. The conjecture implies that there is an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the heights of rational solutions, if the solution set is finite. Let**

$$f(n) = \begin{cases} 1 & \text{if} \quad n=1 \\ 2^{2^{n-2}} & \text{if} \quad n \in \{2,3,4,5\} \\ \left(2+2^{2^{n-4}}\right)^{2^{n-4}} & \text{if} \quad n \in \{6,7,8,\ldots\} \end{cases}$$

We conjecture that if a system $T \subseteq G_n$ has only finitely many solutions in integers $x_1,\ldots,x_n$, then each such solution $(x_1,\ldots,x_n)$ satisfies $|x_1|,\ldots,|x_n| \leqslant f(n)$. This conjecture implies that there is an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the heights of integer (non-negative integer, positive integer, rational) solutions, if the solution set is finite.

***Index Terms*—Diophantine equation which has only finitely many integer (rational) solutions, finite-fold Diophantine representation, integer (rational) arithmetic, upper bound for the heights of integer (rational) solutions.**

THE height of a rational number $\frac{p}{q}$ is denoted by $h\left(\frac{p}{q}\right)$ and equals $\max(|p|,|q|)$ provided $\frac{p}{q}$ is written in lowest terms. The height of a rational tuple $(x_1,\ldots,x_n)$ is denoted by $h(x_1,\ldots,x_n)$ and equals $\max(h(x_1),\ldots,h(x_n))$. We attempt to formulate a conjecture which implies a positive answer to the following open problem:

Problem 1. *Is there an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the heights of rational solutions, if the solution set is finite?*

Theorem 1. *Only $x_1=0$ and $x_1=1$ solve the equation $x_1 \cdot x_1 = x_1$ in integers (rationals, real numbers, complex numbers). For each integer $n \geqslant 2$, the following system*

$$\begin{cases} x_1 \cdot x_1 &= x_1 \\ x_1 + 1 &= x_2 \\ x_1 \cdot x_2 &= x_2 \\ \forall i \in \{2,\ldots,n-1\}\ x_i \cdot x_i &= x_{i+1} \ (\text{if } n \geqslant 3) \end{cases}$$

has exactly one integer (rational, real, complex) solution, namely $\left(1,2,4,16,256,\ldots,2^{2^{n-3}},2^{2^{n-2}}\right)$.

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

Conjecture 1. *If a system $S \subseteq G_n$ has only finitely many solutions in rationals $x_1,\ldots,x_n$, then each such solution $(x_1,\ldots,x_n)$ satisfies $h(x_1,\ldots,x_n) \leqslant \begin{cases} 1 & (\text{if } n=1) \\ 2^{2^{n-2}} & (\text{if } n \geqslant 2) \end{cases}$.*

Theorem 1 implies that the bound $\begin{cases} 1 & (\text{if } n=1) \\ 2^{2^{n-2}} & (\text{if } n \geqslant 2) \end{cases}$ cannot be decreased. Conjecture 1 fails for solutions in integers instead of solutions in rationals, see Corollary 2 and Corollary 4.

Let $\mathcal{R}$ denote the class of all rings, and let $\mathcal{R}ng$ denote the class of all rings $\mathbf{K}$ that extend $\mathbb{Z}$. Let

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

Lemma 1. *([13, p. 720]) Let $D(x_1,\ldots,x_p) \in \mathbb{Z}[x_1,\ldots,x_p]$. Assume that $\deg(D,x_i) \geqslant 1$ 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 $\mathbf{K} \in \mathcal{R}ng \cup \{\mathbb{N},\mathbb{N}\setminus\{0\}\}$, then*

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

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

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

Lemma 2. *([8, p. 100]) If $\boldsymbol{L} \in \mathcal{R} \cup \{\mathbb{N}, \mathbb{N} \setminus \{0\}\}$ and $x, y, z \in \boldsymbol{L}$, then $z(x + y - z) = 0$ if and only if*

$$(zx + 1)(zy + 1) = z^2(xy + 1) + 1$$

Lemma 3. *If $\boldsymbol{L} \in \mathcal{R} \cup \{\mathbb{N}, \mathbb{N} \setminus \{0\}\}$ and $x, y, z \in \boldsymbol{L}$, then $x + y = z$ if and only if*

$$(zx + 1)(zy + 1) = z^2(xy + 1) + 1 \tag{1}$$

and

$$((z+1)x+1)((z+1)(y+1)+1) = (z+1)^2(x(y+1)+1)+1 \tag{2}$$

We can express equations (1) and (2) as a system $\mathcal{F}$ such that $\mathcal{F}$ involves x, y, z and 20 new variables and $\mathcal{F}$ consists of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$.

Proof. By Lemma 2, equation (1) is equivalent to

$$z(x + y - z) = 0 \tag{3}$$

and equation (2) is equivalent to

$$(z + 1)(x + (y + 1) - (z + 1)) = 0 \tag{4}$$

The conjunction of equations (3) and (4) is equivalent to $x + y = z$. The new 20 variables express the following 20 polynomials:

$$zx, \quad zx + 1, \quad zy, \quad zy + 1, \quad z^2, \quad xy, \quad xy + 1,$$
$$z^2(xy + 1), \quad z^2(xy + 1) + 1, \quad z + 1, \quad (z + 1)x,$$
$$(z + 1)x + 1, \quad y + 1, \quad (z + 1)(y + 1), \quad (z + 1)(y + 1) + 1,$$
$$(z + 1)^2, \quad x(y + 1), \quad x(y + 1) + 1,$$
$$(z + 1)^2(x(y + 1) + 1), \quad (z + 1)^2(x(y + 1) + 1) + 1.$$

□

Lemma 4. *Let $D(x_1, \ldots, x_p) \in \mathbb{Z}[x_1, \ldots, x_p]$. Assume that $\deg(D, x_i) \geqslant 1$ for each $i \in \{1, \ldots, p\}$. We can compute a positive integer $n > p$ and a system $T \subseteq G_n$ which satisfies the following two conditions:*

`Condition 1.` *If $\boldsymbol{K} \in \mathcal{R}ng \cup \{\mathbb{N}, \mathbb{N} \setminus \{0\}\}$, then*

$$\forall \tilde{x}_1, \ldots, \tilde{x}_p \in \boldsymbol{K} \ \Big(D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \Longleftrightarrow$$
$$\exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \boldsymbol{K} \ (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \text{ solves } T\Big)$$

`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 $\boldsymbol{K}$.

Proof. Let the system $T \subseteq E_n$ is given by Lemma 1. For every $\boldsymbol{L} \in \mathcal{R} \cup \{\mathbb{N}, \mathbb{N} \setminus \{0\}\}$,

$$\forall x \in \boldsymbol{L} \ \Big(x = 1 \Longleftrightarrow \big(x \cdot x = x \wedge x \cdot (x + 1) = x + 1\big)\Big)$$

Therefore, if there exists $m \in \{1, \ldots, n\}$ such that the equation $1 = x_m$ belongs to T, then we introduce a new variable y and replace in T each equation of the form $1 = x_k$ by the equations $x_k \cdot x_k = x_k$, $x_k + 1 = y$, $x_k \cdot y = y$. Next, we apply Lemma 3 to each equation of the form $x_i + x_j = x_k$ that belongs to T and replace in T each such equation by an equivalent system of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. □

Corollary 1. *Conjecture 1 implies that there is an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the heights of rational solutions, if the solution set is finite.*

For many Diophantine equations we know that the number of rational solutions is finite by Faltings' theorem. Faltings' theorem tell us that certain curves have finitely many rational points, but no known proof gives any bound on the sizes of the numerators and denominators of the coordinates of those points, see [3, p. 722]. In all such cases Conjecture 1 allows us to compute such a bound. If this bound is small enough, that allows us to find all rational solutions by an exhaustive search. For example, the equation $x_1^5 - x_1 = x_2^2 - x_2$ has only finitely many rational solutions ([7, p. 212]). The known rational solutions are: $(-1, 0)$, $(-1, 1)$, $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$, $(2, -5)$, $(2, 6)$, $(3, -15)$, $(3, 16)$, $(30, -4929)$, $(30, 4930)$, $\left(\frac{1}{4}, \frac{15}{32}\right)$, $\left(\frac{1}{4}, \frac{17}{32}\right)$, $\left(-\frac{15}{16}, -\frac{185}{1024}\right)$, $\left(-\frac{15}{16}, \frac{1209}{1024}\right)$, and the existence of other solutions is an open question, see [10, pp. 223–224]. The system

$$\begin{cases} x_3 + 1 = x_2 \\ x_2 \cdot x_3 = x_4 \\ x_5 + 1 = x_1 \\ x_1 \cdot x_1 = x_6 \\ x_6 \cdot x_6 = x_7 \\ x_7 \cdot x_5 = x_4 \end{cases}$$

is equivalent to $x_1^5 - x_1 = x_2^2 - x_2$. By Conjecture 1, $h\left(x_1^4\right) = h(x_7) \leqslant h(x_1, \ldots, x_7) \leqslant 2^{2^{7-2}} = 2^{32}$. Therefore, $h(x_1) \leqslant \left(2^{32}\right)^{\frac{1}{4}} = 256$. Assuming Conjecture 1, the following *MuPAD* code finds all rational solutions of the equation $x_1^5 - x_1 = x_2^2 - x_2$.

```
solutions:={}:
for i from -256 to 256 do
for j from 1 to 256 do
x:=i/j:
y:=4*x^5-4*x+1:
p:=numer(y):
q:=denom(y):
if numlib::issqr(p) and numlib::issqr(q) then
z1:=sqrt(p/q):
z2:=-sqrt(p/q):
y1:=(z1+1)/2:
y2:=(z2+1)/2:
solutions:=solutions union {[x,y1],[x,y2]}:
end_if:
end_for:
```

```
    end_for:
    print(solutions):
```

The code solves the equivalent equation

$$4x_1^5 - 4x_1 + 1 = (2x_2 - 1)^2$$

and displays the already presented solutions.

MuPAD is a general-purpose computer algebra system. The commercial version of *MuPAD* is no longer available as a stand-alone product, but only as the *Symbolic Math Toolbox* of *MATLAB*. Fortunately, the presented code can be executed by *MuPAD Light*, which was offered for free for research and education until autumn 2005.

Lemma 5. *([9, p. 391]) If 2 has an odd exponent in the prime factorization of a positive integer n, then n can be written as the sum of three squares of integers.*

Lemma 6. *For each positive rational number z, z or 2z can be written as the sum of three squares of rational numbers.*

Proof. We find positive integers p and q with $z = \frac{p}{q}$. If 2 has an odd exponent in the prime factorization of pq, then by Lemma 5 there exist integers i_1, i_2, i_3 such that $pq = i_1^2 + i_2^2 + i_3^2$. Hence,

$$z = \left(\frac{i_1}{q}\right)^2 + \left(\frac{i_2}{q}\right)^2 + \left(\frac{i_3}{q}\right)^2$$

If 2 has an even exponent in the prime factorization of pq, then by Lemma 5 there exist integers j_1, j_2, j_3 such that $2pq = j_1^2 + j_2^2 + j_3^2$. Hence,

$$2z = \left(\frac{j_1}{q}\right)^2 + \left(\frac{j_2}{q}\right)^2 + \left(\frac{j_3}{q}\right)^2$$

□

Lemma 7. *A rational number z can be written as the sum of three squares of rational numbers if and only if there exist rational numbers r, s, t such that* $z = r^2\left(s^2\left(t^2+1\right)+1\right)$.

Proof. Let $H(r,s,t) = r^2\left(s^2\left(t^2+1\right)+1\right)$. Of course,

$$H(r,s,t) = r^2 + (rs)^2 + (rst)^2$$

We prove that for each rational numbers a, b, c there exist rational numbers r, s, t such that $a^2+b^2+c^2 = H(r,s,t)$. Without the loss of generality we can assume that $|a| \leqslant |b| \leqslant |c|$. If $b = 0$, then $a = 0$ and $a^2+b^2+c^2 = H(c,0,0)$. If $b \neq 0$, then $c \neq 0$ and $a^2+b^2+c^2 = H\left(c, \frac{b}{c}, \frac{a}{b}\right)$. □

Lemma 8. *([1, p. 125]) The equation* $x^3 + y^3 = 4981$ *has infinitely many solutions in positive rationals and each such solution* (x,y) *satisfies* $h(x,y) > 10^{16 \cdot 10^6}$.

Theorem 2. *There exists a system* $\mathcal{T} \subseteq G_{28}$ *such that* $\mathcal{T}$ *has infinitely many solutions in rationals* $x_1, \ldots, x_{28}$ *and each such solution* $(x_1, \ldots, x_{28})$ *has height greater than* $2^{2^{27}}$.

Proof. We define:

$$\Omega = \left\{\rho \in \mathbb{Q} \cap (0,\infty) : \exists y \in \mathbb{Q}\ (\rho \cdot y)^3 + y^3 = 4981\right\}$$

Let Ω_1 denote the set of all positive rationals ρ such that the system

$$\begin{cases} (\rho \cdot y)^3 + y^3 &= 4981 \\ \rho^3 &= a^2+b^2+c^2 \end{cases}$$

is soluble in rationals. Let Ω_2 denote the set of all positive rationals ρ such that the system

$$\begin{cases} (\rho \cdot y)^3 + y^3 &= 4981 \\ 2\rho^3 &= a^2+b^2+c^2 \end{cases}$$

is soluble in rationals. Lemma 8 implies that the set Ω is infinite. By Lemma 6, $\Omega = \Omega_1 \cup \Omega_2$. Therefore, Ω_1 is infinite (Case 1) or Ω_2 is infinite (Case 2).

Case 1. In this case the system

$$\begin{cases} x^3 + y^3 &= 4981 \\ \frac{x^3}{y^3} &= a^2+b^2+c^2 \end{cases}$$

has infinitely many rational solutions. By this and Lemma 7, the system

$$\begin{cases} x^3 + y^3 &= 4981 \\ \frac{x^3}{y^3} &= r^2\left(s^2\left(t^2+1\right)+1\right) \end{cases}$$

has infinitely many rational solutions. We transform the above system into an equivalent system $\mathcal{T} \subseteq G_{27}$ in such a way that the variables $x_1, \cdots, x_{27}$ correspond to the following rational expressions:

$$x,\ y,\ x^2,\ x^3,\ y^2,\ y^3,\ \tfrac{x^3}{y^3},\ \tfrac{x^3}{y^3}+1,$$
$$1,\ 2,\ 4,\ 16,\ 17,\ 289,\ \tfrac{289}{4},\ \tfrac{289}{4}+1,\ 293,\ 4981,$$
$$t,\ t^2,\ t^2+1,\ s,\ s^2,\ s^2(t^2+1),\ s^2(t^2+1)+1,\ r,\ r^2.$$

The system $\mathcal{T}$ has infinitely many solutions in rationals $x_1, \ldots, x_{27}$. Lemma 8 implies that each rational tuple $(x_1, \ldots, x_{27})$ that solves $\mathcal{T}$ satisfies

$$h(x_1, \ldots, x_{27}) \geqslant h\left(x_1^3, x_2^3\right) = \left(h(x_1,x_2)\right)^3 > 10^{48 \cdot 10^6} > 2^{2^{27}}$$

Since $G_{27} \subseteq G_{28}$, $\mathcal{T} \subseteq G_{28}$ and the proof for Case 1 is complete.

Case 2. In this case the system

$$\begin{cases} x^3 + y^3 &= 4981 \\ 2 \cdot \frac{x^3}{y^3} &= a^2+b^2+c^2 \end{cases}$$

has infinitely many rational solutions. By this and Lemma 7, the system

$$\begin{cases} x^3 + y^3 &= 4981 \\ 2 \cdot \frac{x^3}{y^3} &= r^2\left(s^2\left(t^2+1\right)+1\right) \end{cases}$$

has infinitely many rational solutions. We transform the above system into an equivalent system $\mathcal{T} \subseteq G_{28}$ in such a way that the variables $x_1, \ldots, x_{28}$ correspond to the following rational expressions:

$$x,\ y,\ x^2,\ x^3,\ y^2,\ y^3,\ \tfrac{x^3}{y^3},\ 2 \cdot \tfrac{x^3}{y^3},\ \tfrac{x^3}{y^3}+1,$$
$$1,\ 2,\ 4,\ 16,\ 17,\ 289,\ \tfrac{289}{4},\ \tfrac{289}{4}+1,\ 293,\ 4981,$$
$$t,\ t^2,\ t^2+1,\ s,\ s^2,\ s^2(t^2+1),\ s^2(t^2+1)+1,\ r,\ r^2.$$

The system $\mathcal{T}$ has infinitely many solutions in rationals $x_1, \ldots, x_{28}$. Lemma 8 implies that each rational tuple $(x_1, \ldots, x_{28})$ that solves $\mathcal{T}$ satisfies

$$h(x_1, \ldots, x_{28}) \geqslant h\left(x_1^3, x_2^3\right) = \left(h(x_1, x_2)\right)^3 > 10^{48 \cdot 10^6} > 2^{2^{27}}$$

□

Theorem 3. *Lemmas 2 and 3 are not necessary for proving that in the rational domain each Diophantine equation is equivalent to a system of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$.*

Proof. By Lemma 1, an arbitrary Diophantine equation is equivalent to a system $T \subseteq E_n$. where n and T can be computed. If there exists $m \in \{1, \ldots, n\}$ such that the equation $1 = x_m$ belongs to T, then we introduce a new variable t and replace in T each equation of the form $1 = x_k$ by the equations $x_k \cdot x_k = x_k$, $x_k + 1 = t$, and $x_k \cdot t = t$. For each rational number y, we have $y^2 + 1 \neq 0$ and $y(y^2 + 1) + 1 \neq 0$. Hence, for each rational numbers x, y, z,

$$x + y = z \iff x(y^2 + 1) + y(y^2 + 1) = z(y^2 + 1) \iff$$

$$x(y^2 + 1) + y(y^2 + 1) + 1 = z(y^2 + 1) + 1 \iff$$

$$\left(y(y^2 + 1) + 1\right) \cdot \left(\frac{x(y^2 + 1)}{y(y^2 + 1) + 1} + 1\right) = z(y^2 + 1) + 1$$

We transform the last equation into an equivalent system $W \subseteq G_{12}$ in such a way that the variables $x_1, \ldots, x_{12}$ correspond to the following rational expressions:

$$x,\ y,\ z,\ y^2,\ y^2 + 1,\ y(y^2 + 1),\ y(y^2 + 1) + 1,\ x(y^2 + 1),$$

$$\frac{x(y^2 + 1)}{y(y^2 + 1) + 1},\ \frac{x(y^2 + 1)}{y(y^2 + 1) + 1} + 1,\ z(y^2 + 1),\ z(y^2 + 1) + 1.$$

In this way, we replace in T each equation of the form $x_i + x_j = x_k$ by an equivalent system of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. □

The next theorem provides a similar result which also enable us to prove Corollary 1 without using Lemma 4.

Theorem 4. *For solutions in a field, each system $S \subseteq E_n$ is equivalent to $T_1 \vee \cdots \vee T_p$, where each T_i is a system of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$.*

Proof. Acting as in the proof of Theorem 3, we eliminate from S all equations of the form $1 = x_k$. Let m denote the number of equations of the form $x_i + x_j = x_k$ that belong to S. We can assume that $m > 0$. Let the variables y, z, t, w, s, and r are new. Let

$$S_1 = \left(S \setminus \{x_i + x_j = x_k\}\right) \cup$$

$$\{x_i + 1 = y,\quad x_k + 1 = y,\quad x_j + 1 = z,\quad z \cdot x_j = x_j\}$$

and let

$$S_2 = \left(S \setminus \{x_i + x_j = x_k\}\right) \cup$$

$$\{t \cdot x_j = x_i,\quad t + 1 = w,\quad w \cdot x_j = x_k,\quad x_j + 1 = s,\quad r \cdot x_j = s\}$$

The system S_1 expresses that $x_i + x_j = x_k$ and $x_j = 0$. The system S_2 expresses that $x_i + x_j = x_k$ and $x_j \neq 0$. Therefore, $S \Longleftrightarrow (S_1 \vee S_2)$. We have described a procedure which transforms S into S_1 and S_2. We iterate this procedure for S_1 and S_2 and finally obtain the systems $T_1, \ldots, T_{2^m}$ without equations of the form $x_i + x_j = x_k$. The systems $T_1, \ldots, T_{2^m}$ satisfy $S \Longleftrightarrow (T_1 \vee \cdots \vee T_{2^m})$ and they contain only equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. □

Theorem 5. *For each positive integer m, the following system*

$$\begin{cases} \forall i \in \{1, \ldots, m\}\ x_i \cdot x_i & = & x_{i+1} \\ x_{m+2} + 1 & = & x_1 \\ x_{m+3} + 1 & = & x_{m+2} \\ x_{m+3} \cdot x_{m+4} & = & x_{m+1} \\ x_{m+5} \cdot x_{m+5} & = & x_{m+5} \\ x_{m+5} + 1 & = & x_{m+6} \\ x_{m+5} \cdot x_{m+6} & = & x_{m+6} \\ x_{m+6} \cdot x_{m+7} & = & x_1 \\ x_{m+6} \cdot x_{m+8} & = & x_{m+9} \\ x_{m+9} + 1 & = & x_{m+4} \end{cases}$$

has exactly two integer solutions. The first solution is given by

$$\begin{array}{rcl} \forall i \in \{1, \ldots, m+1\}\ x_i & = & \left(2 - 2^{2^m}\right)^{2^{i-1}} \\ x_{m+2} & = & 1 - 2^{2^m} \\ x_{m+3} & = & -2^{2^m} \\ x_{m+4} & = & -\left(1 - 2^{2^m} - 1\right)^{2^m} \\ x_{m+5} & = & 1 \\ x_{m+6} & = & 2 \\ x_{m+7} & = & 1 - 2^{2^m} - 1 \\ x_{m+8} & = & \dfrac{-\left(1 - 2^{2^m} - 1\right)^{2^m} - 1}{2} \\ x_{m+9} & = & -\left(1 - 2^{2^m} - 1\right)^{2^m} - 1 \end{array}$$

The second solution is given by

$$\begin{array}{rcl} \forall i \in \{1, \ldots, m+1\}\ x_i & = & \left(2 + 2^{2^m}\right)^{2^{i-1}} \\ x_{m+2} & = & 1 + 2^{2^m} \\ x_{m+3} & = & 2^{2^m} \\ x_{m+4} & = & \left(1 + 2^{2^m} - 1\right)^{2^m} \\ x_{m+5} & = & 1 \\ x_{m+6} & = & 2 \\ x_{m+7} & = & 1 + 2^{2^m} - 1 \\ x_{m+8} & = & \dfrac{\left(1 + 2^{2^m} - 1\right)^{2^m} - 1}{2} \\ x_{m+9} & = & \left(1 + 2^{2^m} - 1\right)^{2^m} - 1 \end{array}$$

Proof. The equations

$$\begin{aligned} x_{m+5} \cdot x_{m+5} &= x_{m+5} \\ x_{m+5} + 1 &= x_{m+6} \\ x_{m+5} \cdot x_{m+6} &= x_{m+6} \\ x_{m+6} \cdot x_{m+7} &= x_1 \\ x_{m+6} \cdot x_{m+8} &= x_{m+9} \\ x_{m+9} + 1 &= x_{m+4} \end{aligned}$$

imply that $x_{m+5} = 1$, $x_{m+6} = 2$, $x_1 = 2x_{m+7}$, and $x_{m+4} = 2x_{m+8} + 1$. The equations

$$\begin{aligned} \forall i \in \{1, \ldots, m\} \; x_i \cdot x_i &= x_{i+1} \\ x_{m+2} + 1 &= x_1 \\ x_{m+3} + 1 &= x_{m+2} \\ x_{m+3} \cdot x_{m+4} &= x_{m+1} \end{aligned}$$

imply that

$$(x_1 - 2) \cdot x_{m+4} = x_1^{2^m} \tag{5}$$

From equation (5) and the polynomial identity

$$x_1^{2^m} = 2^{2^m} + (x_1 - 2) \cdot \sum_{k=0}^{2^m - 1} 2^{2^m - 1 - k} \cdot x_1^k$$

we conclude that $x_1 - 2$ divides 2^{2^m}. Since $x_1 = 2x_{m+7}$ and $x_{m+4} = 2x_{m+8} + 1$, equation (5) gives

$$(x_1 - 2) \cdot (2x_{m+8} + 1) = 2^{2^m} \cdot x_{m+7}^{2^m} \tag{6}$$

Since $2x_{m+8} + 1$ is odd, equation (6) implies that 2^{2^m} divides $x_1 - 2$. Since $x_1 - 2$ and 2^{2^m} divide each other, $x_1 = 2 \pm 2^{2^m}$. □

Corollary 2. *For every integer $n > 137$, there exists a system $W \subseteq G_n$ such that W has exactly two solutions in integers $x_1, \ldots, x_n$ and they belong to $\mathbb{Z}^n \setminus [-2^{2^{n-2}}, 2^{2^{n-2}}]^n$.*

Proof. We define W as the system from Theorem 5, where $m = n - 9$. Therefore, $n = m + 9$. Since $n > 137$, $m > 128$. The first solution of W has height $(2 - 2^m)^{2^m}$. The height of the second solution is greater, and equals $(2 + 2^m)^{2^m}$. Since $m > 128$, $|2 - 2^m| > 2^{128}$. Consequently,

$$(2 - 2^m)^{2^m} > \left(2^{128}\right)^{2^m} = 2^{2^{(m+9)-2}}$$

□

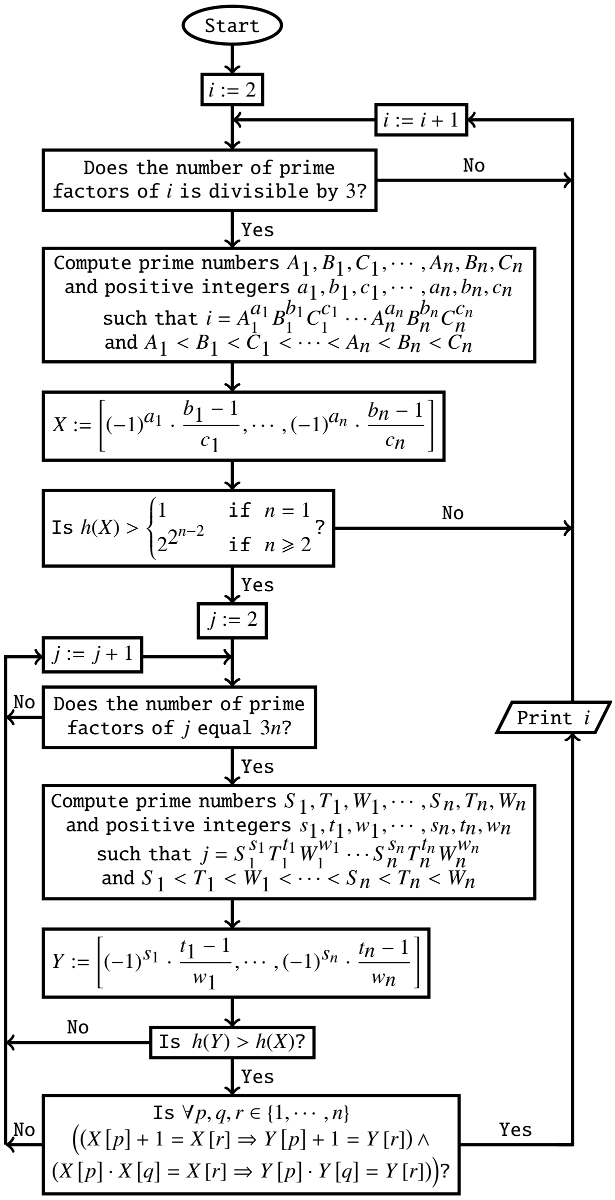
Conjecture 1 is equivalent to the following conjecture on rational arithmetic: if rational numbers $x_1, \ldots, x_n$ satisfy

$$h(x_1, \ldots, x_n) > \begin{cases} 1 & \text{(if } n = 1) \\ 2^{2^{n-2}} & \text{(if } n \geqslant 2) \end{cases}$$

then there exist rational numbers $y_1, \ldots, y_n$ such that $h(x_1, \ldots, x_n) < h(y_1, \ldots, y_n)$ and for every $i, j, k \in \{1, \ldots, n\}$

$$(x_i + 1 = x_k \Longrightarrow y_i + 1 = y_k) \;\wedge (x_i \cdot x_j = x_k \Longrightarrow y_i \cdot y_j = y_k)$$

Theorem 6. *Conjecture 1 is true if and only if the execution of Flowchart 1 prints infinitely many numbers.*



Flowchart 1: An infinite-time computation which decides whether or not Conjecture 1 is true

Proof. Let Γ_3 denote the set of all integers $i \geqslant 2$ whose number of prime factors is divisible by 3. The claimed equivalence is true because the algorithm from Flowchart 1 applies a surjective function from Γ_3 to $\bigcup_{n=1}^{\infty} \mathbb{Q}^n$. □

Corollary 3. *Conjecture 1 can be written in the form $\forall x \in \mathbb{N} \; \exists y \in \mathbb{N} \; \phi(x, y)$, where $\phi(x, y)$ is a computable predicate.*

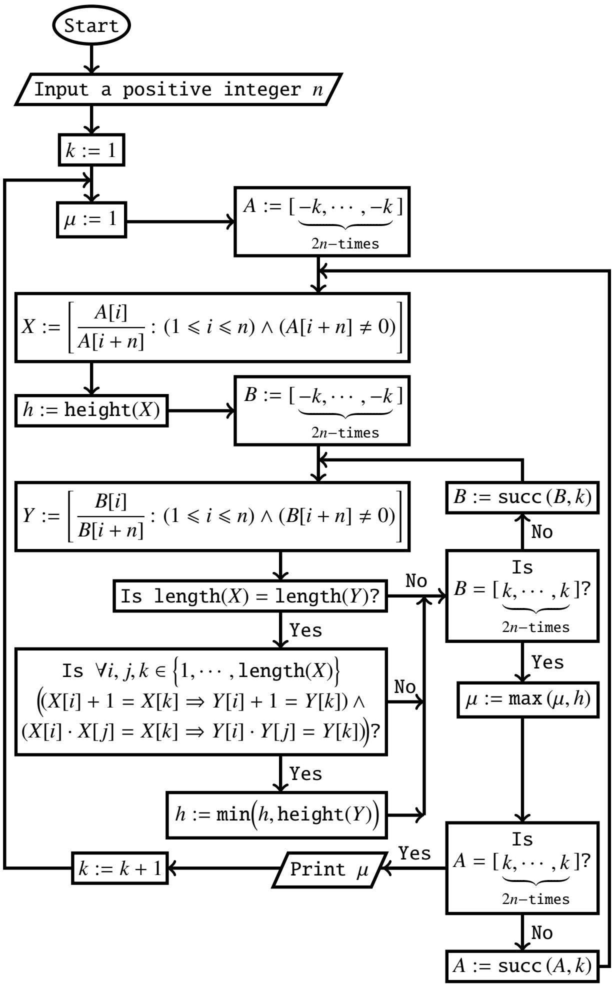
For a positive integer n, let $\mu(n)$ denote the smallest positive integer m such that each system $S \subseteq G_n$ soluble in rationals $x_1, \ldots, x_n$ has a rational solution $(x_1, \ldots, x_n)$ whose height is not greater than m. Obviously, $\mu(1) = 1$. Theorem 1 implies that $\mu(n) \geqslant 2^{2^{n-2}}$ for every integer $n \geqslant 2$. Theorem 2 implies that $\mu(28) > 2^{2^{27}}$.

Theorem 7. *The function $\mu : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ is computable in the limit.*

Proof. Let us agree that the empty tuple has height 0. For a positive integer w and a tuple

$$(x_1, \ldots, x_n) \in ([-w, w] \cap \mathbb{Z})^n \setminus \{\underbrace{(w, \ldots, w)}_{n\text{-times}}\}$$

let $\mathrm{succ}\left((x_1, \ldots, x_n), w\right)$ denote the successor of $(x_1, \ldots, x_n)$ in the co-lexicographic order on $([-w, w] \cap \mathbb{Z})^n$. Flowchart 2 illustrates an infinite-time computation of $\mu(n)$.



Flowchart 2: An infinite-time computation of $\mu(n)$

□

The following problem is open:

Problem 2. *Is there an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the heights of integer (non-negative integer, positive integer) solutions, if the solution set is finite?*

We attempt to formulate a conjecture on integer arithmetic which implies positive answers to Problems 1 and 2.

Theorem 8. *For every positive integer n, the following system*

$$\begin{cases} \forall i \in \{1, \ldots, n\}\ x_i \cdot x_i &= x_{i+1} \\ x_{n+2} + 1 &= x_1 \\ x_{n+3} + 1 &= x_{n+2} \\ x_{n+3} \cdot x_{n+4} &= x_{n+1} \end{cases}$$

has only finitely many integer solutions. Each integer solution $(x_1, \ldots, x_{n+4})$ satisfies $|x_1|, \ldots, |x_{n+4}| \leqslant \left(2 + 2^{2^n}\right)^{2^n}$. The bound $\left(2 + 2^{2^n}\right)^{2^n}$ is attained by the following solution:

$$\begin{cases} \forall i \in \{1, \ldots, n+1\}\ x_i &= \left(2 + 2^{2^n}\right)^{2^{i-1}} \\ x_{n+2} &= 1 + 2^{2^n} \\ x_{n+3} &= 2^{2^n} \\ x_{n+4} &= \left(1 + 2^{2^n} - 1\right)^{2^n} \end{cases}$$

Proof. The system equivalently expresses that $(x_1 - 2) \cdot x_{n+4} = x_1^{2^n}$. From this and the polynomial identity

$$x_1^{2^n} = 2^{2^n} + (x_1 - 2) \cdot \sum_{k=0}^{2^n - 1} 2^{2^n - 1 - k} \cdot x_1^k$$

we obtain that $x_{n+3} = x_1 - 2$ divides 2^{2^n} and $x_{n+4} = \dfrac{x_1^{2^n}}{x_1 - 2}$. Hence, $x_1 \in \left[2 - 2^{2^n}, 2 + 2^{2^n}\right] \cap \mathbb{Z}$, the system has only finitely many integer solutions, and $|x_1|, \ldots, |x_{n+4}| \leqslant \left(2 + 2^{2^n}\right)^{2^n}$. □

Lemma 9. *For every integer $n \geqslant 6$,*

$$\left(2 + 2^{2^{n-4}}\right)^{2^{n-4}} > 2^{2^{n-2}}$$

Lemma 9 and Theorem 8 imply the next corollary.

Corollary 4. *For every integer $n \geqslant 6$, there exists a system $S \subseteq G_n$ such that S has only finitely many solutions in integers $x_1, \ldots, x_n$ and at least one such solution does not belong to $[-2^{2^{n-2}}, 2^{2^{n-2}}]^n$.*

Let

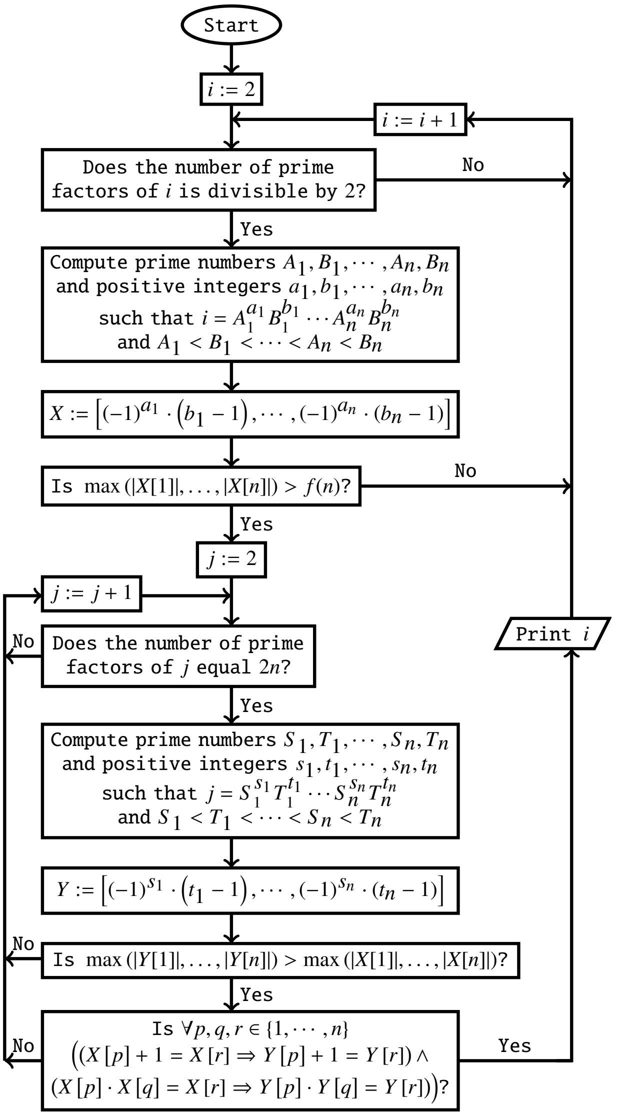
$$f(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2^{2^{n-2}} & \text{if } n \in \{2, 3, 4, 5\} \\ \left(2 + 2^{2^{n-4}}\right)^{2^{n-4}} & \text{if } n \in \{6, 7, 8, \ldots\} \end{cases}$$

Conjecture 2. *If a system $T \subseteq G_n$ has only finitely many solutions in integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $|x_1|, \ldots, |x_n| \leqslant f(n)$.*

Theorems 1 and 8 imply that the function f cannot be decreased. Conjecture 2 is equivalent to the following conjecture on integer arithmetic: if integers $x_1, \ldots, x_n$ satisfy $\max(|x_1|, \ldots, |x_n|) > f(n)$, then there exist integers $y_1, \ldots, y_n$ such that $\max(|x_1|, \ldots, |x_n|) < \max(|y_1|, \ldots, |y_n|)$ and for every $i, j, k \in \{1, \ldots, n\}$

$$(x_i + 1 = x_k \Longrightarrow y_i + 1 = y_k) \ \wedge \ (x_i \cdot x_j = x_k \Longrightarrow y_i \cdot y_j = y_k)$$

Theorem 9. *Conjecture 2 is true if and only if the execution of Flowchart 3 prints infinitely many numbers.*



Flowchart 3: An infinite-time computation which decides whether or not Conjecture 2 is true

Proof. Let Γ_2 denote the set of all integers $i \geqslant 2$ whose number of prime factors is divisible by 2. The claimed equivalence is true because the algorithm from Flowchart 3 applies a surjective function from Γ_2 to $\bigcup_{n=1}^{\infty} \mathbb{Z}^n$. □

Corollary 5. *Conjecture 2 can be written in the form $\forall x \in \mathbb{N}\ \exists y \in \mathbb{N}\ \psi(x, y)$, where $\psi(x, y)$ is a computable predicate.*

Conjecture 2 is less plausible than Conjecture 1 as the arithmetic of integers is much more complicated than the arithmetic of rationals. The last remark is confirmed by the proof of Theorem 8, where we find the set of all integers x_1 such that $x_1 - 2$ divides $x_1^{2^n}$. This set is not trivial, whereas in rationals $x_1 - 2$ divides $x_1^{2^n}$ if and only if $x_1 \neq 2$.

Theorem 10. *If we assume Conjecture 2 and a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has only finitely many integer solutions, then an upper bound for their modulus can be computed.*

Proof. It follows from Lemma 4. □

Corollary 6. *If we assume Conjecture 2 and a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has only finitely many solutions in non-negative integers, then an upper bound for these solutions can be computed by applying Theorem 10 to the equation*

$$D^2(x_1, \ldots, x_p) + \sum_{i=1}^{p} \left(x_i - x_{i,1}^2 - x_{i,2}^2 - x_{i,3}^2 - x_{i,4}^2\right)^2 = 0$$

Proof. It follows from Lagrange's four-square theorem. □

Corollary 7. *If we assume Conjecture 2 and a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has only finitely many solutions in positive integers, then an upper bound for these solutions can be computed by applying Theorem 10 to the equation*

$$D^2(x_1, \ldots, x_p) + \sum_{i=1}^{p} \left(x_i - 1 - x_{i,1}^2 - x_{i,2}^2 - x_{i,3}^2 - x_{i,4}^2\right)^2 = 0$$

Proof. It follows from Lagrange's four-square theorem. □

Lemma 10. *([13, p. 720]) If there is a computable upper bound for the modulus of integer solutions to a Diophantine equation with a finite number of integer solutions, then there is a computable upper bound for the heights of rational solutions to a Diophantine equation with a finite number of rational solutions.*

Theorem 11. *Conjecture 2 implies that there is a computable upper bound for the heights of rational solutions to a Diophantine equation with a finite number of rational solutions.*

Proof. It follows from Theorem 10 and Lemma 10. □

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

$$(a_1, \ldots, a_n) \in \mathcal{M} \Longleftrightarrow$$

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

for some polynomial W with integer coefficients, see [4]. The polynomial W can be computed, if we know the 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]. 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 $(x_1, \ldots, x_m) \in \mathbb{N}^m$. Yu. Matiyasevich conjectures that each recursively enumerable set $\mathcal{M} \subseteq \mathbb{N}^n$ has a finite-fold Diophantine representation, see [2, pp. 341–342], [5, p. 42], and [6, p. 745]. Currently, he seems very much agnostic on his conjecture, see [6, p. 749]. Matiyasevich's conjecture implies a negative answer to each of the three questions in Problem 2, see [5, p. 42].

Theorem 12. *(cf. [13, p. 721]) Conjecture 2 implies that if a set $\mathcal{M} \subseteq \mathbb{N}^n$ has a finite-fold Diophantine representation, then $\mathcal{M}$ is computable.*

Proof. Let a set $\mathcal{M} \subseteq \mathbb{N}^n$ has a finite-fold Diophantine representation. It means that there exists a polynomial $W(x_1, \ldots, x_n, x_1, \ldots, x_m)$ with integer coefficients such that

$$\forall b_1 \ldots b_n \in \mathbb{N} \ \Big((b_1, \ldots, b_n) \in \mathcal{M} \Longleftrightarrow$$

$$\exists x_1, \ldots, x_m \in \mathbb{N} \ \ W(b_1, \ldots, b_n, x_1, \ldots, x_m) = 0\Big)$$

and for any $b_1, \ldots, b_n \in \mathbb{N}$ the equation $W(b_1, \ldots, b_n, x_1, \ldots, x_m) = 0$ has only finitely many solutions $(x_1, \ldots, x_m) \in \mathbb{N}^m$. By Corollary 6, there is a computable function $g\colon \mathbb{N}^n \to \mathbb{N}$ such that for each $b_1 \ldots, b_n, x_1, \ldots, x_m \in \mathbb{N}$ the equality $W(b_1, \ldots, b_n, x_1, \ldots, x_m) = 0$ implies $\max(x_1, \ldots, x_m) \leqslant g(b_1, \ldots, b_n)$. Hence, we can decide whether or not the tuple $(b_1, \ldots, b_n)$ belongs to $\mathcal{M}$ by checking whether or not the equation $W(b_1, \ldots, b_n, x_1, \ldots, x_m) = 0$ has an integer solution in the box $[0, g(b_1, \ldots, b_n)]^m$. □

For a positive integer n, let $\tau(n)$ denote the smallest non-negative integer b such that for each system $T \subseteq G_n$ which has only finitely many solutions in integers $x_1, \ldots, x_n$, all these solutions belong to $[-b, b]^n$. By Theorems 1 and 8, $f(n) \leqslant \tau(n)$ for every positive integer n. Conjecture 2 implies that $f(n) = \tau(n)$ for every positive integer n.

Lemma 11. *There exists a system $\mathcal{H} \subseteq G_{71}$ such that for every integer x_1,*

$$x_1 \geqslant 0 \Longleftrightarrow \exists x_2, \ldots, x_{71} \in \mathbb{Z} \ (x_1, x_2, \ldots, x_{71}) \ \textit{solves } \mathcal{H}$$

and the set

$$\Big\{(x_2, \ldots, x_{71}) \in \mathbb{Z}^{70} : \ \ (x_1, x_2, \ldots, x_{71}) \ \textit{solves } \mathcal{H}\Big\}$$

is finite.

Proof. By Lagrange's four-square theorem, for each integer x_1,

$$x_1 \geqslant 0 \Longleftrightarrow \exists \ a, \ b, \ c, \ d \in \mathbb{Z} \quad a^2 + b^2 + c^2 + d^2 = x_1$$

We express the equation $a^2 + b^2 + c^2 + d^2 = x_1$ as the following system:

$$\begin{cases} a \cdot a &= a_1 \\ b \cdot b &= b_1 \\ c \cdot c &= c_1 \\ d \cdot d &= d_1 \\ a_1 + b_1 &= e_1 \\ c_1 + d_1 &= f_1 \\ e_1 + f_1 &= x_1 \end{cases}$$

We apply Lemma 3 for $\boldsymbol{L} = \mathbb{Z}$ and replace the last three equations by an equivalent system $\mathcal{P}$ which consists of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. We define $\mathcal{H}$ as

$$\{a \cdot a = a_1, \ b \cdot b = b_1, \ c \cdot c = c_1, \ d \cdot d = d_1\} \cup \mathcal{P}$$

The system $\mathcal{H}$ involves x_1, a, b, c, d and $23 + 23 + 20$ other variables. □

Theorem 13. *(cf. [12, Theorem 4]) If a function $\theta\colon \mathbb{N} \to \mathbb{N}$ has a finite-fold Diophantine representation, then there exists a positive integer m such that $\theta(n) < \tau(n)$ for every integer $n > m$.*

Proof. There exists 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,

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

and for each non-negative integers x_1, x_2 at most finitely many tuples $(x_3, \ldots, x_r)$ of non-negative integers satisfy $W(x_1, x_2, x_3, \ldots, x_r) = 0$. By Lemma 4 for $\boldsymbol{K} = \mathbb{N}$, there is an integer $s \geqslant 3$ such that for any non-negative integers x_1, x_2,

$$\theta(x_1) = x_2 \Longleftrightarrow \exists x_3, \ldots, x_s \in \mathbb{N} \ \ \Psi(x_1, x_2, x_3, \ldots, x_s) \qquad \texttt{(E)}$$

where $\Psi(x_1, x_2, x_3, \ldots, x_s)$ is a conjunction of formulae of the forms $x_i + 1 = x_k$ and $x_i \cdot x_j = x_k$, the indices i, j, k belong to $\{1, \ldots, s\}$, and for each non-negative integers x_1, x_2 at most finitely many tuples $(x_3, \ldots, x_s)$ of non-negative integers satisfy $\Psi(x_1, x_2, x_3, \ldots, x_s)$. Let $[\cdot]$ denote the integer part function, and let an integer n is greater than $m = 142 \cdot s - 137$. Hence, $n \geqslant 142 \cdot s - 136$, and

$$n - \left[\frac{n}{2}\right] - 71 \cdot s + 68 \geqslant n - \frac{n}{2} - 71 \cdot s + 68 =$$

$$\frac{n}{2} - 71 \cdot s + 68 \geqslant \frac{142 \cdot s - 136}{2} - 71 \cdot s + 68 = 0$$

The following system T_n

$$\begin{cases} \text{all equations occurring in } \Psi(x_1, x_2, x_3, \ldots, x_s) \\ \text{(they involve } s \text{ variables)} \\ \\ \text{the equations of the forms } \alpha + 1 = \gamma \text{ and } \alpha \cdot \beta = \gamma \\ \text{which express that } (x_2 \geqslant 0) \wedge \ldots \wedge (x_s \geqslant 0) \text{ according to} \\ \text{Lemma 11 (they involve } (s-1) \cdot 70 \text{ new variables)} \\ \\ \forall i \in \left\{1, \ldots, \left[\frac{n}{2}\right] - 1\right\} \ t_i + 1 \ = \ t_{i+1} \\ \text{(these equations involve } \left[\frac{n}{2}\right] \text{ new variables)} \\ \\ t_1 \cdot t_1 \ = \ t_1 \\ t_1 \cdot t_2 \ = \ t_2 \\ t_2 \cdot t_{[\frac{n}{2}]} \ = \ u \\ u + 1 \ = \ x_1 \text{ (if } n \text{ is odd)} \\ t_1 \cdot u \ = \ x_1 \text{ (if } n \text{ is even)} \\ x_2 + 1 \ = \ y \\ \text{(the variables } u \text{ and } y \text{ are new)} \\ \\ \forall i \in \left\{1, \ldots, n - \left[\frac{n}{2}\right] - 71 \cdot s + 68)\right\} \ v_i \cdot v_i = v_i \\ \text{(these equations involve } n - \left[\frac{n}{2}\right] - 71 \cdot s + 68 \\ \text{new variables)} \end{cases}$$

has exactly n variables. Indeed,

$$s + \Big((s-1) \cdot 70\Big) + \left[\frac{n}{2}\right] + \mathrm{card}(\{u, y\}) + \Big(n - \left[\frac{n}{2}\right] - 71 \cdot s + 68\Big) = n$$

By the equivalence (E), the system T_n is soluble in integers. The system T_n implies that $2 \cdot \left[\frac{n}{2}\right] = u$, $n = x_1$, and

$$\theta(n) = \theta(x_1) = x_2 < x_2 + 1 = y$$

Since T_n has at most finitely many integer solutions, $y \leqslant \tau(n)$. Hence, $\theta(n) < \tau(n)$. □

The results of [11] concern the following older conjecture: if a system $T \subseteq G_n$ has only finitely many solutions in positive integers $x_1, \ldots, x_n$, then each such solution $(x_1, \ldots, x_n)$ satisfies $x_1, \ldots, x_n \leqslant f(n)$. The older conjecture seems to be stronger than Conjecture 2. Only by this reason, Conjecture 2 is more suitable for further investigations.

References

[1] A. Bremner, *Positively prodigious powers or how Dudeney done it?* Math. Mag. 84 (2011), no. 2, 120–125, http://dx.doi.org/10.4169/math.mag.84.2.120.

[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., Providence, RI, 1996, 269–324.

[3] T. Gowers, J. Barrow-Green, I. Leader (eds), *The Princeton companion to mathematics,* Princeton University Press, Princeton, 2008.

[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,* in: Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math. 270, Amer. Math. Soc., Providence, RI, 2000, 1–47.

[6] Yu. Matiyasevich, *Towards finite-fold Diophantine representations,* J. Math. Sci. (N. Y.) vol. 171, no. 6, 2010, 745–752, http://dx.doi.org/10.1007%2Fs10958-010-0179-4.

[7] M. Mignotte and A. Pethő, *On the Diophantine equation $x^p - x = y^q - y$,* Publ. Mat. 43 (1999), no. 1, 207–216.

[8] J. Robinson, *Definability and decision problems in arithmetic,* J. Symbolic Logic 14 (1949), 98–114; reprinted in: The collected works of Julia Robinson (ed. S. Feferman), Amer. Math. Soc., Providence, RI, 1996, 7–23.

[9] W. Sierpiński, *Elementary theory of numbers,* 2nd ed. (ed. A. Schinzel), PWN (Polish Scientific Publishers) and North-Holland, Warsaw-Amsterdam, 1987.

[10] S. Siksek, *Chabauty and the Mordell–Weil Sieve,* in: Advances on Superelliptic Curves and Their Applications (eds. L. Beshaj, T. Shaska, E. Zhupa), 194–224, IOS Press, Amsterdam, 2015, http://dx.doi.org/10.3233/978-1-61499-520-3-194.

[11] A. Tyszka, *A hypothetical way to compute an upper bound for the heights of solutions of a Diophantine equation with a finite number of solutions,* Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (eds. M. Ganzha, L. Maciaszek, M. Paprzycki), *Annals of Computer Science and Information Systems*, vol. 5, 709–716, IEEE Computer Society Press, 2015, http://dx.doi.org/10.15439/2015F41.

[12] A. Tyszka, *All functions $g\colon \mathbb{N} \to \mathbb{N}$ which have a single-fold Diophantine representation are dominated by a limit-computable function $f\colon \mathbb{N} \setminus \{0\} \to \mathbb{N}$ which is implemented in MuPAD and whose computability is an open problem,* in: Computation, cryptography, and network security (eds. N. J. Daras and M. Th. Rassias), Springer, Cham, Switzerland, 2015, 577–590, http://dx.doi.org/10.1007/978-3-319-18275-9_24.

[13] 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, http://dx.doi.org/10.1016/j.ipl.2013.07.004.