A hypothetical upper bound on the heights of the solutions of a Diophantine equation with a finite number of solutions

Apoloniusz Tyszka

Abstract

Let \( f(1) = 1 \), and let \( f(n + 1) = 2^{2f(n)} \) for every positive integer \( n \). We consider the following hypothesis: if a system \( S \subseteq \{ x_i \cdot x_j = x_k : i, j, k \in \{1, \ldots, n\} \} \cup \{ x_i + 1 = x_k : i, k \in \{1, \ldots, n\} \} \) has only finitely many solutions in non-negative integers \( x_1, \ldots, x_n \), then each such solution \( (x_1, \ldots, x_n) \) satisfies \( x_1, \ldots, x_n \leq f(2n) \). We prove: (1) the hypothesis implies that there exists 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; (2) the hypothesis implies that there exists an algorithm for listing the Diophantine equations with infinitely many solutions in non-negative integers; (3) the hypothesis implies that the question whether or not a given Diophantine equation has only finitely many rational solutions is decidable by a single query to an oracle that decides whether or not a given Diophantine equation has a rational solution; (4) the hypothesis implies that the question whether or not a given Diophantine equation has only finitely many integer solutions is decidable by a single query to an oracle that decides whether or not a given Diophantine equation has an integer solution; (5) the hypothesis implies that if a set \( M \subseteq \mathbb{N} \) has a finite-fold Diophantine representation, then \( M \) is computable.

Key words and phrases: computable upper bound on the heights of rational solutions, computable upper bound on the moduli of integer solutions, Diophantine equation with a finite number of solutions, finite-fold Diophantine representation, single query to an oracle that decides whether or not a given Diophantine equation has an integer solution, single query to an oracle that decides whether or not a given Diophantine equation has a rational solution.

2010 Mathematics Subject Classification: 11U05.

1 Introduction and basic lemmas

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 \( \max(h(x_1), \ldots, h(x_n)) \). In this article, we present a hypothesis which positively solves the following two open problems:

Open Problem 1. Is there an algorithm which takes as input a Diophantine equation, returns an integer, and this integer is greater than the moduli of integer (non-negative integer, positive integer) solutions, if the solution set is finite?
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 rational solutions, if the solution set is finite?

Lemma 1. For every non-negative integers b and c, \( b + 1 = c \) if and only if \( 2^{2b} \cdot 2^{2b} = 2^{2c} \).

2 A hypothesis on the arithmetic of non-negative integers

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

Let \( f(1) = 1 \), and let \( f(n + 1) = 2^{2f(n)} \) for every positive integer \( n \). Let \( \theta(1) = 0 \), and let \( \theta(n + 1) = 2^{2\theta(n)} \) for every positive integer \( n \).

Hypothesis 1. If a system \( S \subseteq G_n \) has only finitely many solutions in non-negative integers \( x_1, \ldots, x_n \), then each such solution \( (x_1, \ldots, x_n) \) satisfies \( x_1, \ldots, x_n \leq f(2n) \).

Observations 1 and 2 justify Hypothesis 1.

Observation 1. For every system \( S \subseteq G_n \) which involves all the variables \( x_1, \ldots, x_n \), the following new system

\[
\left\{ \bigcup_{x_i \cdot x_j = x_k \in S} \{ x_i \cdot x_j = x_k \} \right\} \cup \left\{ 2^{2x_k} = y_k : k \in \{1, \ldots, n\} \right\} \cup \left\{ \bigcup_{x_i + 1 = x_k \in S} \{ y_i \cdot y_i = y_k \} \right\}
\]

is equivalent to \( S \). If the system \( S \) has only finitely many solutions in non-negative integers \( x_1, \ldots, x_n \), then the new system has only finitely many solutions in non-negative integers \( x_1, \ldots, x_n, y_1, \ldots, y_n \).

Proof. It follows from Lemma 1.

Observation 2. For every positive integer \( n \), the following system

\[
\begin{cases} 
  x_1 \cdot x_i = x_1 \\
  \forall i \in \{1, \ldots, n-1\} \quad 2^{2x_i} = x_{i+1} \quad \text{(if } n > 1) 
\end{cases}
\]

has exactly two solutions in non-negative integers, namely \((\theta(1), \ldots, \theta(n))\) and \((f(1), \ldots, f(n))\). The second solution has greater height.

Observations 1 and 2, in substantially changed forms, remain true for solutions in non-negative rationals, see [6].

3 Algebraic lemmas

Lemma 2. (cf. [7, p. 100]) For every non-negative real numbers \( x, y, z \), \( x + y = z \) if and only if

\[
((z + 1)x + 1)((z + 1)(y + 1) + 1) = (z + 1)^2(x(y + 1) + 1) + 1 \quad (1)
\]

Proof. The left side of equation 1 minus the right side of equation 1 equals \((z + 1)(x + y - z)\). □
Let $\alpha$, $\beta$, and $\gamma$ denote variables.

**Lemma 3.** In non-negative integers, the equation $x + y = z$ is equivalent to a system which consists of equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$.

**Proof.** It follows from Lemma 2. \[\square\]

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

**Condition 1.** For every non-negative integers $\tilde{x}_1, \ldots, \tilde{x}_p$,

$$D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0 \iff \exists \tilde{x}_{p+1}, \ldots, \tilde{x}_n \in \mathbb{N} (\tilde{x}_1, \ldots, \tilde{x}_p, \tilde{x}_{p+1}, \ldots, \tilde{x}_n) \text{ solves } T$$

**Condition 2.** If non-negative integers $\tilde{x}_1, \ldots, \tilde{x}_p$ satisfy $D(\tilde{x}_1, \ldots, \tilde{x}_p) = 0$, then there exists a unique tuple $(\tilde{x}_{p+1}, \ldots, \tilde{x}_n) \in \mathbb{N}^{n-p}$ 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 the equation $D(x_1, \ldots, x_p) = 0$ and the system $T$ have the same number of solutions in non-negative integers.

**Proof.** We write down the polynomial $D(x_1, \ldots, x_p)$ and replace each coefficient by the successor of its absolute value. Let $\tilde{D}(x_1, \ldots, x_p)$ denote the obtained polynomial. The polynomials $D(x_1, \ldots, x_p) + \tilde{D}(x_1, \ldots, x_p)$ and $\tilde{D}(x_1, \ldots, x_p)$ have positive integer coefficients. The equation $D(x_1, \ldots, x_p) = 0$ is equivalent to

$$D(x_1, \ldots, x_p) + \tilde{D}(x_1, \ldots, x_p) + 1 = \tilde{D}(x_1, \ldots, x_p) + 1$$

There exist a positive integer $a$ and a finite non-empty list $A$ such that

$$D(x_1, \ldots, x_p) + \tilde{D}(x_1, \ldots, x_p) + 1 = \left(\sum_{(i_1, j_1, \ldots, i_k, j_k) \in A} x_{i_1}^{j_1} \cdots x_{i_k}^{j_k} + 1\right) + \ldots + 1 \quad (2)$$

and all the numbers $k, i_1, j_1, \ldots, i_k, j_k$ belong to $\mathbb{N} \setminus \{0\}$. There exist a positive integer $b$ and a finite non-empty list $B$ such that

$$\tilde{D}(x_1, \ldots, x_p) + 1 = \left(\sum_{(i_1, j_1, \ldots, i_k, j_k) \in B} x_{i_1}^{j_1} \cdots x_{i_k}^{j_k} + 1\right) + \ldots + 1 \quad (3)$$

and all the numbers $k, i_1, j_1, \ldots, i_k, j_k$ belong to $\mathbb{N} \setminus \{0\}$. By Lemma 3, we can equivalently express the equality of the right sides of equations (2) and (3) using only equations of the forms $\alpha + 1 = \gamma$ and $\alpha \cdot \beta = \gamma$. Consequently, we can effectively find the system $T$. \[\square\]

Lemma 4 remains true for solutions in non-negative rationals, see [6].

### 4 Hypothetical upper bounds on the heights of the solutions

**Theorem 1.** If we assume Hypothesis 7 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.

**Proof.** It follows from Lemma 4. \[\square\]
Theorem 2. If we assume Hypothesis 1 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.

Proof. We apply Theorem 1 to the equation \(D(x_1 + 1, \ldots, x_p + 1) = 0\). Next, we increase the computed bound by 1. □

Theorem 3. If we assume Hypothesis 1 and a Diophantine equation \(D(x_1, \ldots, x_p) = 0\) has only finitely many integer solutions, then an upper bound for their moduli can be computed by applying Theorem 1 to the equation

\[
\prod_{(i_1, \ldots, i_p) \in \{1, 2\}^p} D((-1)^i_1 \cdot x_1, \ldots, (-1)^i_p \cdot x_p) = 0
\]

Lemma 5. (Corollary 2, p. 25) If \(a\) and \(b\) are two relatively prime positive integers, then every integer \(n > ab\) can be written in the form \(n = ax + by\), where \(x\), \(y\) are positive integers.

Lemma 6. For every non-negative integers \(c\) and \(d\), the following system

\[
\begin{align*}
\{ \quad cx + (d + 1)y &= (d + 1)c + 1 \\
x + y + u &= (d + 1)c + 1
\end{align*}
\]

has at most finitely many solutions in non-negative integers \(x\), \(y\), \(u\). For every non-negative integers \(c\) and \(d\), system (4) is solvable in non-negative integers \(x\), \(y\), \(u\) if and only if \(c\) and \(d + 1\) are relatively prime.

Proof. The equality \(x + y + u = (d + 1)c + 1\) implies that \(x, y, u \leq (d + 1)c + 1\). Hence, at most finitely many non-negative integers \(x, y, u\) satisfy system (4). The equality

\[
 cx + (d + 1)y = (d + 1)c + 1
\]

gives \(cx + (d + 1)(y - c) = 1\). Hence, the integers \(c\) and \(d + 1\) are relatively prime. Conversely, assume that \(c\) and \(d + 1\) are relatively prime. By this, if \(c = 0\), then \(d = 0\). In this case, system (4) has exactly one solution in non-negative integers, namely \(\{ x = 0 \quad y = 1 \quad u = 0 \}\). If \(c > 0\), then Lemma 5 implies that there exist positive integers \(x\) and \(y\) that satisfy equation (5). We set \(u = (c - 1)x + dy\). Then,

\[
x + y + u = x + y + (c - 1)x + dy = cx + (d + 1)y = (d + 1)c + 1
\]

□

Theorem 4. Hypothesis 1 implies that there exists a computable upper bound on the heights of the rationals that solve a Diophantine equation with a finite number of solutions.

Proof. Let \(W(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]\), and let

\[
\widetilde{W}(x_1, \ldots, x_n) = \prod_{(i_1, \ldots, i_n) \in \{1, 2\}^p} W((-1)^i_1 \cdot x_1, \ldots, (-1)^i_n \cdot x_n)
\]
If the equation \( W(x_1, \ldots, x_n) = 0 \) has only finitely many solutions in rationals \( x_1, \ldots, x_n \), then the equation \( \bar{W}(x_1, \ldots, x_n) = 0 \) has only finitely many solutions in non-negative rationals \( x_1, \ldots, x_n \). By Lemma 6, it means that the system
\[
\begin{align*}
\bar{W} \left( \frac{y_1}{z_1 + 1}, \ldots, \frac{y_n}{z_n + 1} \right) &= 0 \\
\forall i \in \{1, \ldots, n\} \quad y_i s_i + (z_i + 1) t_i &= (z_i + 1) y_i + 1 \\
\forall i \in \{1, \ldots, n\} \quad s_i + t_i + u_i &= (z_i + 1) y_i + 1
\end{align*}
\] (6)
has only finitely many solutions in non-negative integers \( y_1, z_1, s_1, t_1, u_1, \ldots, y_n, z_n, s_n, t_n, u_n \). System (6) is equivalent to a single Diophantine equation. By Lemma 4, this equation is equivalent to a system of equations of the forms \( \alpha \cdot \beta = \gamma \) and \( \alpha + 1 = \gamma \). Next, we apply Theorem 1. □

5 Finite-fold Diophantine representations

The Davis-Putnam-Robinson-Matiyasevich theorem states that every recursively enumerable set \( M \subseteq \mathbb{N}^n \) has a Diophantine representation, that is
\[
(a_1, \ldots, a_n) \in M \iff \exists x_1, \ldots, x_m \in \mathbb{N} \quad W(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \tag{R}
\]
for some polynomial \( W \) with integer coefficients, see [3]. 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 \( (a_1, \ldots, a_n) \in M \), see [3]. The representation (R) is said to be finite-fold, if for every \( a_1, \ldots, a_n \in \mathbb{N} \) the equation \( W(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \) has only finitely many solutions \( (x_1, \ldots, x_m) \in \mathbb{N}^m \). Yuri Matiyasevich conjectured that each recursively enumerable set \( M \subseteq \mathbb{N}^n \) has a finite-fold Diophantine representation, see [1] pp. 341–342], [4] p. 42], and [5] p. 745]. Currently, he seems agnostic on his conjecture, see [5] p. 749]. In [9] p. 581], the author explains why Matiyasevich’s conjecture although widely known is less widely accepted. Matiyasevich’s conjecture implies a negative answer to Open Problem 1, see [4] p. 42].

Lemma 7. Let \( W(x, x_1, \ldots, x_m) \in \mathbb{Z}[x, x_1, \ldots, x_m] \). We claim that the function
\[
\mathbb{N} \ni b \mapsto W(b, x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]
\]
is computable.

Theorem 5. Hypothesis 1 implies that if a set \( M \subseteq \mathbb{N} \) has a finite-fold Diophantine representation, then \( M \) is computable.

Proof. Let a set \( M \subseteq \mathbb{N} \) have a finite-fold Diophantine representation. It means that there exists a polynomial \( W(x, x_1, \ldots, x_m) \) with integer coefficients such that
\[
\forall b \in \mathbb{N} \quad (b \in M \iff \exists x_1, \ldots, x_m \in \mathbb{N} \quad W(b, x_1, \ldots, x_m) = 0)
\]
and for every \( b \in \mathbb{N} \) the equation \( W(b, x_1, \ldots, x_m) = 0 \) has only finitely many solutions \( (x_1, \ldots, x_m) \in \mathbb{N}^m \). By Lemma 7 and Theorem 1 there is a computable function \( \xi : \mathbb{N} \to \mathbb{N} \) such that for each \( b, x_1, \ldots, x_m \in \mathbb{N} \) the equality \( W(b, x_1, \ldots, x_m) = 0 \) implies \( \max(x_1, \ldots, x_m) \leq \xi(b) \). Hence, we can decide whether or not a non-negative integer \( b \) belongs to \( M \) by checking whether or not the equation \( W(b, x_1, \ldots, x_m) = 0 \) has an integer solution in the box \([0, \xi(b)]^m\). □

Theorem 5 remains true if we change the bound \( f(2n) \) in Hypothesis 1 to any other computable bound \( \delta(n) \).
6 Theorems on relative decidability


Proof. It follows from Theorem [1]. □

Corollary 1. Hypothesis [1] implies that \( d(\inf, N) \leq 0' \), where \( d(\inf, N) \) denotes the Turing degree of the set of Diophantine equations with infinitely many solutions in non-negative integers.

Lemma 8. A Diophantine equation \( D(x_1, \ldots, x_p) = 0 \) is solvable in non-negative integers \( x_1, \ldots, x_p \) if and only if the equation \( D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0 \) has infinitely many solutions in non-negative integers \( x_1, \ldots, x_{p+1} \).

Corollary [1], Lemma [8] and the Davis-Putnam-Robinson-Matiyasevich theorem imply the next theorem.

Theorem 7. Hypothesis [1] implies that \( d(\inf, N) = 0' \).

Theorem 8. ([1] p. 372) Matiyasevich’s conjecture on finite-fold Diophantine representations implies that \( d(\inf, N) = 0'' \).


Hypothesis 2. There exists an algorithm which takes as input a Diophantine equation \( D(x_1, \ldots, x_p) = 0 \) and returns an integer \( b \geq 2 \), where \( b \) is greater than the number of rational solutions, if the solution set is finite.

Guess ([2] p. 16). The question whether or not a Diophantine equation has only finitely many rational solutions is decidable with an oracle for deciding whether or not a Diophantine equation has a rational solution.

Originally, Minhyong Kim formulated the Guess as follows: for rational solutions, the finiteness problem is decidable relative to the existence problem.

Theorem 9. ([6]) Hypothesis [2] implies that the question whether or not a given Diophantine equation has only finitely many rational solutions is decidable by a single query to an oracle that decides whether or not a given Diophantine equation has a rational solution.

Corollary 2. ([6]) Hypothesis [2] implies that the question whether or not a given Diophantine equation has only finitely many rational solutions is decidable by a single query to an oracle that decides whether or not a given Diophantine equation has an integer solution.


Hypothesis 3. There exists an algorithm which takes as input a Diophantine equation \( D(x_1, \ldots, x_p) = 0 \) and returns an integer \( r \geq 2 \), where \( r \) is greater than the moduli of integer solutions, if the solution set is finite.

Hypothesis 4. There exists an algorithm which takes as input a Diophantine equation $D(x_1, \ldots, x_p) = 0$ and returns an integer $c \geq 2$, where $c$ is greater than the number of integer solutions, if the solution set is finite.

Theorem 10. Hypothesis 4 implies Hypothesis 3.

Proof. Assume that a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has only finitely many integer solutions. Then, the equation

$$D^2(x_1, \ldots, x_p) + \left( \left( x_1^2 + \ldots + x_p^2 \right) - \left( y_1^2 + y_2^2 + y_3^2 + y_4^2 \right) - \left( z_1^2 + z_2^2 + z_3^2 + z_4^2 \right) \right)^2 = 0 \quad (7)$$

has only finitely many integer solutions. By Lagrange’s four-square theorem, every integer $p$-tuple $(a_1, \ldots, a_p)$ with $D(a_1, \ldots, a_p) = 0$ implies the existence of $a_1^2 + \ldots + a_p^2 + 1$ integer solutions of equation (7). The inequality $|a_1|, \ldots, |a_p| < a_1^2 + \ldots + a_p^2 + 1$ completes the proof. □

The conclusion of the next theorem contradicts the following conjecture of Yuri Matiyasevich ([2, p. 16]): the finiteness problem for integral points is undecidable relative to the existence problem.

Theorem 11. Hypothesis 4 implies that the question whether or not a given Diophantine equation has only finitely many integer solutions is decidable by a single query to an oracle that decides whether or not a given Diophantine equation has an integer solution.

Proof. Assuming that Hypothesis 4 holds, Lagrange’s four-square theorem guarantees that the execution of the flowchart below decides whether or not a Diophantine equation $D(x_1, \ldots, x_p) = 0$ has only finitely many integer solutions.

```
Start

Input a Diophantine equation $D(x_1, \ldots, x_p) = 0$

Compute the bound $c$

Does the equation

$$\left( \sum_{k=1}^{c} D^2(x_{1,k}, \ldots, x_{p,k}) \right) + \left( \prod_{1 \leq u < v \leq c} \sum_{i=1}^{p} (x_{i,u} - x_{i,v})^2 \right) - s^2 - t^2 - u^2 - v^2 - 1 \right)^2 = 0$$

have an integer solution?

Yes

Print "The equation $D(x_1, \ldots, x_p) = 0$ has infinitely many integer solutions"

No

Print "The equation $D(x_1, \ldots, x_p) = 0$ has only finitely many integer solutions"

Stop
```
**Corollary 3.** Hypothesis $[1]$ implies that $d(f, \mathbb{Z}) \leq 0'$, where $d(f, \mathbb{Z})$ denotes the Turing degree of the set of Diophantine equations which have only finitely many integer solutions.

**Lemma 9.** A Diophantine equation $D(x_1, \ldots, x_p) = 0$ is solvable in integers $x_1, \ldots, x_p$ if and only if the equation $D(x_1, \ldots, x_p) + 0 \cdot x_{p+1} = 0$ has infinitely many solutions in integers $x_1, \ldots, x_{p+1}$.

Corollary 3, Lemma 9, and the Davis-Putnam-Robinson-Matiyasevich theorem imply the next theorem.

**Theorem 12.** Hypothesis $[7]$ implies that $d(f, \mathbb{Z}) = 0'$.

**References**


[9] A. Tyszka, *All functions g: \( \mathbb{N} \rightarrow \mathbb{N} \) which have a single-fold Diophantine representation are dominated by a limit-computable function f: \( \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \) 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](http://dx.doi.org/10.1007/978-3-319-18275-9_24).

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