J. Syst. Sci. Complex., 37 (2024), in press.

MIXED QUANTIFIER PREFIXES OVER DIOPHANTINE EQUATIONS WITH INTEGER VARIABLES

ZHI-WEI SUN

Abstract. In this paper we first review the history of Hilbert's Tenth Problem, and then study mixed quantifier prefixes over Diophantine equations with integer variables. For example, we prove that $\forall^2\exists^4$ over $\mathbb{Z}$ is undecidable, that is, there is no algorithm to determine for any $P(x_1,\ldots,x_6)\in\mathbb{Z}[x_1,\ldots,x_6]$ whether

$$\forall x_1\forall x_2\exists x_3\exists x_4\exists x_5\exists x_6(P(x_1,\ldots,x_6)=0),$$

where $x_1,\ldots,x_6$ are integer variables. We also have some similar undecidable results with universal quantifies bounded, for example, $\exists^2\forall^2\exists^2$ over $\mathbb{Z}$ with $\forall$ bounded is undecidable. We conjecture that $\forall^2\exists^2$ over $\mathbb{Z}$ is undecidable.

1. Introduction

In 1900, at the Paris conference of ICM, D. Hilbert presented 23 famous mathematical problems. Many of them are questions of others, however the tenth one is due to Hilbert himself. In modern language, *Hilbert's Tenth Problem* (HTP) asks for an effective algorithm to test whether an arbitrary polynomial equation

$$P(z_1,\ldots,z_n)=0$$

(with integer coefficients) has solutions over the ring $\mathbb{Z}$ of the integers, where n is an arbitrary positive integer. However, the concept of algorithm or computation was vague in 1900.

Let $\mathbb{N}=\{0,1,2,\ldots\}$ and call each $n\in\mathbb{N}$ a *natural number*. What kind of number-theoretic functions into $\mathbb{N}$ (with natural number variables) are computable? This was investigated by logicians in the 1930s.

We first introduce the basic functions:

(1) *Zero function*: $O(x)=0$ (for all $x\in\mathbb{N}$).

(2) *Successor function*: $S(x)=x+1$.

(3) *Projection functions*: $I_{nk}(x_1,\ldots,x_n)=x_k$ $(1\leqslant k\leqslant n)$

Key words and phrases. Undecidability, Diophantine equations, Hilbert's tenth problem, mixed quantifiers.

2020 *Mathematics Subject Classification.* Primary 03D35, 11U05; Secondary 03D25, 11D99.

The research is supported by the National Natural Science Foundation of China (grant no. 12371004), and the main results date back to the author's PhD thesis (Nanjing University, 1992).

For number-theoretic functions $g(y_1,\ldots,y_m)$ and $h_i(x_1,\ldots,x_n)$ $(1\leqslant i\leqslant m)$, we define their *composition* as follows:

$$f(x_1,\ldots,x_n)=g(h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n))$$

Given number-theoretic functions $g(x_1,\ldots,x_n)$ and $h(x_1,\ldots,x_n,y,z)$, we define

$$\begin{cases}f(x_1,\ldots,x_n,0)=g(x_1,\ldots,x_n),\\ f(x_1,\ldots,x_n,y+1)=h(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,y)),\end{cases}$$

and say that f is obtained from g and h via *primitive recursion*.

For a number-theoretic function $g(x_1,\ldots,x_n,y)$, we define

$$f(x_1,\ldots,x_n)=\mu y\geqslant 0\,(g(x_1,\ldots,x_n,y)=0)$$

as the least $y\in\mathbb{N}$ with $g(x_1,\ldots,x_n,y)=0$; if $g(x_1,\ldots,x_n,y)\neq 0$ for all $y\in\mathbb{N}$, then $f(x_1,\ldots,x_n)$ is undefined. We say that f is obtained from the function g via the *μ-operator*.

The *partial recursive functions* are the basic functions and those obtained from the basic functions by applying composition, primitive recursion and the μ-operator a finite number of times. For any partial recursive function f, it is easy to see that if $f(x_1,\ldots,x_n)$ is defined then the value $f(x_1,\ldots,x_n)$ is effectively computable by intuition.

In 1936 A. Turing introduced the notion of Turing machine which is an abstract machine that manipulates symbols on a infinite strip of tape according to a finite table of rules (i.e., a program) involving four kinds of basic operations: Write 1, change 1 to 0 (blank), move to the left unit (L), move to the right unit (R). A function $f(x_1,\ldots,x_n)$ is *Turing computable* if there is a program according to which the Turing machine with initial inputs $x_1,\ldots,x_n$ finally stops and yields the value $f(x_1,\ldots,x_n)$ as output if $f(x_1,\ldots,x_n)$ is defined, and never stops if $f(x_1,\ldots,x_n)$ is undefined.

The partial recursive functions and Turing computable functions were proved to be equivalent by S. C. Kleene in 1936. The following thesis was proposed by A. Church in the same year.

Church's Thesis. *If a function f into $\mathbb{N}$ with natural number variables is effectively computable by intuition, then it must be a partial recursive function (equivalently, a Turing computable function).*

Church's Thesis has been widely accepted after 1936. So we have the exact definition of computable functions which refer to the partial recursive functions or Turing computable functions, and hence HTP has its accurate meaning.

A subset A of $\mathbb{N}$ is said to be an *r.e. (recursively enumerable) set* (or *a semi-decidable set*) if the function

$$f_A(x)=\begin{cases}1 & \text{if } x\in A,\\ \text{undefined} & \text{if } x\in\mathbb{N}\setminus A.\end{cases}$$

is a partial recursive function. It is easy to show that

$$\begin{aligned} & A \subseteq \mathbb{N} \text{ is an r.e. set} \\ \Longleftrightarrow\ & A \text{ is the domain of a partial recursive function} \\ \Longleftrightarrow\ & A \text{ is the emptyset or the range of a total recursive function } f(x). \end{aligned}$$

A set $A \subseteq \mathbb{N}$ is called *decidable* or *recursive*, if the characteristic function

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \in \mathbb{N} \setminus A. \end{cases}$$

is Turing computable (or recursive). Clearly, A is recursive if and only if both A and $\mathbb{N} \setminus A$ are r.e. sets. A well known result in the theory of computability states that there is a nonrecursive r.e. set (cf. [1, pp. 140-141]).

From now on, variables range over $\mathbb{Z}$ unless specified. Let $P(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$. Then

$$\begin{aligned} & \exists z_1 \ldots \exists z_n \, (P(z_1, \ldots, z_n) = 0) \\ \Longleftrightarrow\ & \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 \left(\prod_{\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}} P(\varepsilon_1 x_1, \ldots, \varepsilon_n x_n) = 0 \right). \end{aligned}$$

On the other hand, by Lagrange's four-square theorem (each $m \in \mathbb{N}$ can be written as the sum of four squares), we have

$$\begin{aligned} & \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 \, (P(x_1, \ldots, x_n) = 0) \\ \Longleftrightarrow\ & \exists u_1 \exists v_1 \exists y_1 \exists z_1 \ldots \exists u_n \exists v_n \exists y_n \exists z_n \\ & (P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + y_n^2 + z_n^2) = 0) \end{aligned}$$

So HTP has the following equivalent form (HTP over $\mathbb{N}$): Is there an algorithm to decide for any polynomial $P(x_1, \ldots, x_n)$ with integer coefficients whether the Diophantine equation $P(x_1, \ldots, x_n) = 0$ has solutions with $x_1, \ldots, x_n \in \mathbb{N}$?

A relation $R(a_1, \ldots, a_m)$ with $a_1, \ldots, a_m \in \mathbb{N}$ is said to be *Diophantine* if there is a polynomial $P(t_1, \ldots, t_m, x_1, \ldots, x_n)$ with integer coefficients such that

$$R(a_1, \ldots, a_m) \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0 \, (P(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0).$$

A set $A \subseteq \mathbb{N}$ is Diophantine if and only if the predicate $a \in A$ is Diophantine. It is easy to see that any Diophantine set A is an r.e. set. In fact, for a given element $a \in \mathbb{N}$ we may search for the natural number solutions of the Diophantine equation associated with A. If it has a solution, then we will find one and let the computer stop and give the output 1. If it has no solution, the computer will never stop.

In 1944 E. L. Post thought that HTP begs for an unsolvability proof (i.e., HTP might be undecidable), motivated by this M. Davis [3] published in 1953 the following important hypothesis.

Davis Daring Hypothesis. *Any r.e. set $A \subseteq \mathbb{N}$ is Diophantine.*

Under this hypothesis, for any nonrecursive r.e. set A there is a polynomial $P(x,x_1,\ldots,x_n)$ such that for any $a\in\mathbb{N}$ we have

$$a\in A\iff \exists x_1\geqslant 0\ldots\exists x_n\geqslant 0\,(P(a,x_1,\ldots,x_n)=0).$$

Thus Davis Daring Hypothesis implies that HTP over $\mathbb{N}$ is undecidable.

The *exponential Diophantine equations* over $\mathbb{N}$ have the form

$$E_1(x_1,\ldots,x_m)=E_2(x_1,\ldots,x_m),$$

where E_1 and E_2 are expressions constructed from variables and particular natural numbers using addition, multiplication, and exponentiation. Here is an example of exponential Diophantine equation:

$$x^{2^y}+y^2+y^{y^z}=5z^{x^x+3z}.$$

A relation $R(a_1,\ldots,a_m)$ with $a_1,\ldots,a_m\in\mathbb{N}$ is said to be *exponential Diophantine* if there is an exponential Diophantine equation

$$E(t_1,\ldots,t_m,x_1,\ldots,x_n)=0$$

over $\mathbb{N}$ such that

$$R(a_1,\ldots,a_m)\iff\exists x_1\geqslant 0\ldots\exists x_n\geqslant 0\,(E(a_1,\ldots,a_m,x_1,\ldots,x_n)=0).$$

A set $A\subseteq\mathbb{N}$ is called exponential Diophantine if the predicate $a\in A$ is Diophantine. The following important result concerning exponential Diophantine equations was established by Davis, H. Putnam and J. Robinson [5] in 1961.

Davis-Putnam-Robinson Theorem. *Any r.e. set is exponential Diophantine. Thus there is no algorithm to decide for any given exponential Diophantine equation whether it has solutions over* $\mathbb{N}$.

Based on this result, in 1970 Y. Matiyasevich [9] utilized the Fibonacci sequence to prove that the exponential relation $a=b^c$ (with $a,b,c\in\mathbb{N}$) is Diophantine. This, together with the Davis-Putnam-Robinson Theorem, led him to prove the Davis Daring Hypothesis completely. Thus, HTP was finally solved negatively in 1970. The reader may consult Davis [4] or Matiyasevich [13] for a popular introduction to the negative solution of HTP.

In 1975 Matiyasevich proved further that any r.e. set $A\subseteq\mathbb{N}$ has a Diophantine representation over $\mathbb{N}$ with only 9 unknowns, the detailed proof of this 9 unknowns theorem appeared in J. P. Jones [8].

Note that a system of finitely many Diophantine equations over $S\subseteq\mathbb{Z}$ is equivalent to a single Diophantine equation over S. In fact, if $P_i(z_1,\ldots,z_n)\in\mathbb{Z}[z_1,\ldots,z_n]$ for all $i=1,\ldots,k$, then

$$\begin{aligned}&P_1(z_1,\ldots,z_n)=0\wedge\ldots\wedge P_k(z_1,\ldots,z_n)=0\\\iff&P_1^2(z_1,\ldots,z_n)+\ldots+P_k^2(z_1,\ldots,z_n)=0.\end{aligned}$$

For $i=1,\ldots,n$, let each ρ_i be one of the two quantifiers $\forall$ and $\exists$. If there is no algorithm to determine for any $P(x_1,\ldots,x_n)\in\mathbb{Z}[x_1,\ldots,x_n]$ whether

$$\rho_1x_1\geqslant 0\cdots\rho_nx_n\geqslant 0\,(P(a,x_1,\ldots,x_n)=0),$$

then we say that $\rho_1 \cdots \rho_n$ over $\mathbb{N}$ is undecidable. For example, $\exists^9$ over $\mathbb{N}$ is undecidable by the 9 unknowns theorem, but it is open whether $\exists^8$ over $\mathbb{N}$ is decidable or not. We may also consider $\rho_1 \cdots \rho_n$ over $\mathbb{N}$ with $\forall$ bounded, for example, Matiyasevich [11] proved that $\exists\forall\exists^2$ over $\mathbb{N}$ with $\forall$ bounded is undecidable, that is, there is no algorithm to determine for any $P(x) \in \mathbb{Z}[x]$ and $Q(x_1, \ldots, x_4) \in \mathbb{Z}[x_0, \ldots, x_4]$ whether

$$\exists x_1 \geqslant 0 \forall x_2 \in [0, P(x_1)] \exists x_3 \geqslant 0 \exists x_4 \geqslant 0 \, (Q(a, x_1, \ldots, x_4) = 0).$$

After the negation solution of Hilbert's tenth problem, it is natural to ask the following question: For what kinds of mixed quantifier prefixes $\rho_1 \cdots \rho_n$, $\rho_1, \cdots \rho_n$ over $\mathbb{N}$ (with $\forall$ bounded or unbounded) is undecidable? After a series of efforts due to Matiyasevich [10, 11], Matiyasevich and Robinson [14, 15], and Jones [7], the only open cases are $\forall\exists^2$, $\exists\forall\exists$, and $\exists\forall\exists$ with $\forall$ bounded. J. M. Rojas [20, Conjecture 3] conjectured that $\exists\forall\exists$ over $\mathbb{N}$ is decidable.

Both $\exists$ over $\mathbb{N}$ and $\exists$ over $\mathbb{Z}$ are decidable in polynomial time (see, e.g., [15, p. 525]). In fact, if $a_0, a_1, \ldots, a_n$ and z are integers with $a_0 z \neq 0$ and $\sum_{i=0}^{n} a_i z^{n-i} = 0$, then

$$|z|^n \leqslant |a_0 z^n| \leqslant \sum_{i=1}^{n} |a_i| \cdot |z|^{n-i} \leqslant \sum_{i=1}^{n} |a_i| \cdot |z|^{n-1}$$

and hence

$$|z| \leqslant \sum_{i=1}^{n} |a_i|.$$

In 1987 S. P. Tung [27] showed that for each $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ the problem to determine

$$\forall x_1 \cdots \forall x_n \exists x_{n+1} \, (P(x_1, \ldots, x_n, x_{n+1}) = 0)$$

with P a general polynomial in $\mathbb{Z}[x_1, \ldots, x_{n+1}]$ is co-NP-complete.

For a finite sequence of quantifiers $\rho_1, \ldots, \rho_n$, we say that $\rho_1 \cdots \rho_n$ over $\mathbb{Z}$ is undecidable if there is no algorithm to determine for any $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ whether

$$\rho_1 x_1 \cdots \rho_n x_n \, (P(x_1, \ldots, x_n) = 0). \tag{1.1}$$

What kinds of $\rho_1 \cdots \rho_n$ over $\mathbb{Z}$ are undecidable? In 1985 Tung [26] proved that $\exists^{27}$ and $\forall^{27}\exists^2$ over $\mathbb{Z}$ are undecidable. We may also consider $\rho_1 \cdots \rho_n$ over $\mathbb{Z}$ with $\forall$ bounded. We say that $\rho_1 \cdots \rho_n$ over $\mathbb{Z}$ with $\forall$ bounded is undecidable if there is no general algorithm to determine whether (1.1) with $\rho_j x_j$ (for those $1 \leqslant j \leqslant n$ with $\rho_j = \forall$) replaced by

$$\forall x_j \in [P_j(x_i : 1 \leqslant i < j \ \& \ \rho_i = \exists), Q_j(x_i : 1 \leqslant i < j \ \& \ \rho_i = \exists)]$$

holds or not, where P and those P_j and Q_j with $\rho_j = \forall$ are polynomials with integer coefficients. For example, $\exists\forall^2\exists$ over $\mathbb{Z}$ is undecidable if and only if

there is no algorithm to determine for $P_1(x), P_2(x), P_3(x), P_4(x) \in \mathbb{Z}[x]$ and $Q(x_1,\ldots,x_4)\in\mathbb{Z}[x_1,\ldots,x_4]$ whether

$$\exists x_1\forall x_2\in[P_1(x_1),P_2(x_1)]\forall x_3\in[P_3(x_1),P_4(x_1)]\exists x_4(Q(x_1,x_2,x_3,x_4)=0).$$

Clearly, if $\rho_1\cdots\rho_n$ over $\mathbb{Z}$ (with $\forall$ bounded or not) is decidable, then so is $\rho_{i_1}\rho_{i_2}\cdots\rho_{i_m}$ over $\mathbb{Z}$ with $1\leqslant i_1<i_2<\ldots<i_m$. Also, $\forall\rho_1\cdots\rho_n$ over $\mathbb{Z}$ with $\forall$ bounded is decidable if and only if $\rho_1\cdots\rho_n$ over $\mathbb{Z}$ with $\forall$ bounded is decidable. Note also that $\rho_1,\cdots\rho_n$ over $\mathbb{Z}$ is undecidable (with $\forall$ unbounded or bounded) if and only if $\rho_1\cdots\rho_n\forall$ over $\mathbb{Z}$ is undecidable. In fact, for the polynomial

$$P(x_1,\ldots,x_n,t)=\sum_{i=0}^k P_i(x_1,\ldots,x_n)t^i \text{ with } P_i(x_1,\ldots,x_n)\in\mathbb{Z}[x_1,\ldots,x_n],$$

we have

$$\forall t(P(x_1,\ldots,x_n,t)=0)\iff\sum_{i=0}^k P_i(x_1,\ldots,x_n)^2=0$$

for all $x_1,\ldots,x_n\in\mathbb{Z}$; if $P_*(x_1,\ldots,x_n),P^*(x_1,\ldots,x_n)\in\mathbb{Z}[x_1,\ldots,x_n]$, then for any $x_1,\ldots,x_n\in\mathbb{Z}$ we have

$$\begin{aligned}&\forall t\in[P_*(x_1,\ldots,x_n),P^*(x_1,\ldots,x_n)](P(x_1,\ldots,x_n,t)=0)\\ \iff&\sum_{0\leqslant r\leqslant P^*(x_1,\ldots,x_n)-P_*(x_1,\ldots,x_n)}\left(\sum_{i=0}^k P_i(x_1,\ldots,x_n)(P_*(x_1,\ldots,x_n)+r)^i\right)^2=0\\ \iff&\sum_{0\leqslant r\leqslant P^*(x_1,\ldots,x_n)-P_*(x_1,\ldots,x_n)}\sum_{j=0}^{2k}\bar{P}_j(x_1,\ldots,x_n)r^j=0,\end{aligned}$$

where $\bar{P}_j(x_1,\ldots,x_n)$ $(0\leqslant j\leqslant 2k)$ are suitable polynomials with integer coefficients. For any $j,m\in\mathbb{N}$, it is well known (cf. [6, pp. 228-231]) that

$$\sum_{r=0}^m r^j=\frac{1}{j+1}\sum_{r=0}^m(B_{j+1}(r+1)-B_{j+1}(r))=\frac{B_{j+1}(m+1)-B_{j+1}(0)}{j+1},$$

where $B_{j+1}(x)$ denotes the Bernoulli polynomial (with rational number coefficients) of degree $j+1$.

Based on the work [22], the author [24] proved that for any r.e. set A there is a polynomial $P(x_0,\ldots,x_9)\in\mathbb{Z}[x_0,\ldots,x_9]$ such that for any $a\geqslant 0$ we have

$$a\in A\iff\exists x_1\cdots\exists x_8\exists x_9\geqslant 0\,(P(a,x_1,\ldots,x_9)=0).$$

(See also the book [25] for a complete proof.) This implies Matiyasevich's 9 unknowns theorem since

$$a\in A\iff\exists x_1\geqslant 0\cdots\exists x_9\geqslant 0\left(\prod_{\varepsilon_1,\ldots,\varepsilon_8\in\{\pm1\}}P(a,\varepsilon_1x_1,\ldots,\varepsilon_8x_8,x_9)=0\right).$$

As a consequence of this result, the author [24] obtained the 11 unknowns theorem ($\exists^{11}$ over $\mathbb{Z}$ is undecidable) and also the undecidability of $\forall^{10}\exists^2$ and $\forall^9\exists^3$ over $\mathbb{Z}$. For their applications, one may consult [2, 17, 16, 19, 28]. The author [24, Conjecture 1.8] conjectured that there is no algorithm to determine for any $P(x,y,z) \in \mathbb{Z}[x,y,z]$ whether the equation $P(x^2,y^2,z^2) = 0$ has integer solutions, which implies that $\exists^3$ over $\mathbb{Z}$ is undecidable.

Now we state the main result of this paper.

Theorem 1.1. (i) *All those*

$$\forall\exists^7,\ \forall^2\exists^4,\ \exists\forall\exists^4,\ \exists\forall^2\exists^3,\ \exists^2\forall\exists^3,\ \forall\exists\forall\exists^3,$$
$$\forall\exists^2\forall^2\exists^2,\ \forall^2\exists\forall^2\exists^2, \forall\exists\forall^3\exists^2,\ \exists^2\forall^3\exists^2,\ \exists\forall\exists\forall^2\exists^2,\ \exists\forall^6\exists^2$$

over $\mathbb{Z}$ are undecidable.

(ii) *All those*

$$\exists\forall\exists^4,\ \exists\forall^2\exists^3,\ \exists^2\forall\exists^3,\ \exists^2\forall^2\exists^2, \exists\forall\exists\forall\exists^2,\ \exists\forall^5\exists^2$$

over $\mathbb{Z}$ with $\forall$ bounded are undecidable.

Remark 1.1. In 1991 the author learnt from Tung that R. M. Robinson was the first person to ask for such undecidable results over $\mathbb{Z}$.

Given a finite sequence of quantifiers $\rho_1, \ldots, \rho_n$, we say that a set $A \subseteq \mathbb{N}$ has a $\rho_1 \cdots \rho_n$-representation over $\mathbb{Z}$ if there is a polynomial $P(x_0, \ldots, x_n) \in \mathbb{Z}[x_0, \ldots, x_n]$ such that for any $a \in \mathbb{N}$ we have

$$a \in A \iff \rho_1 x_1 \cdots \rho_n x_n \, (P(a, x_1, \ldots, x_n) = 0).$$

Similarly, we may define $\rho_1 \cdots \rho_n$-representations over $\mathbb{Z}$ with $\forall$ bounded. The author [24] actually proved that any r.e. set $A \subseteq \mathbb{N}$ has a $\exists^{11}$-representation over $\mathbb{Z}$, and any co-r.e. set (i.e., the complement of an r.e. set $A \subseteq \mathbb{N}$) has a $\forall^{10}\exists^2$-representation, and a $\forall^9\exists^3$-representation over $\mathbb{Z}$. By B.-K. Oh and the author [18, Corollary 1.1], the set

$$S = \{2n+1 : \ n \in \mathbb{Z}^+, \text{ and } 2n+1 \text{ is not a prime congruent to 3 modulo 4}\}$$

has a surprising $\exists^3$-representation over $\mathbb{Z}$: $a \in \mathbb{N}$ belongs to S if and only if

$$\exists x \exists y \exists z \, (a^2 = (2x+1)^2 + 8(2y+1)^2 + 8(2z+1)^2).$$

For a subset A of $\mathbb{N}$, we write $\bar{A}$ for $\mathbb{N} \setminus A$, the complement of A in $\mathbb{N}$. Theorem 1.1 follows immediately from our following three theorems.

Theorem 1.2. *Let $A \subseteq \mathbb{N}$ be an r.e. set.*

(i) *A has a $\exists^2\forall\exists^3$-representation over $\mathbb{Z}$. Also, we may replace $\exists^2\forall\exists^3$ by either of $\exists^2\forall^3\exists^2$ and $\exists\forall\exists\forall^2\exists^2$. Also, $\bar{A}$ has a $\forall^2\exists^4$-representation, a $\forall\exists\forall\exists^3$-representation, and a $\forall^2\exists\forall^2\exists^2$-representation over $\mathbb{Z}$.*

(ii) *A has a $\exists^2\forall^2\exists^2$-representation over $\mathbb{Z}$ with $\forall$ bounded. Also, we may replace $\exists^2\forall^2\exists^2$ by either of $\exists^2\forall\exists^3$ and $\exists\forall\exists\forall\exists^2$.*

Theorem 1.3. *Let $A \subseteq \mathbb{N}$ be an r.e. set.*

(i) *A has a $\exists\forall\exists^4$-representation over $\mathbb{Z}$, and also a $\exists\forall\exists^4$-representation over $\mathbb{Z}$ with $\forall$ bounded.*

(ii) *$\bar{A}$ has a $\forall\exists\forall^3\exists^2$-representation over $\mathbb{Z}$.*

Theorem 1.4. *Let $A\subseteq\mathbb{N}$ be an r.e. set.*

(i) *A has a $\exists\forall^2\exists^3$-representation over $\mathbb{Z}$, and also a $\exists\forall^2\exists^3$-representation over $\mathbb{Z}$ with $\forall$ bounded. Also, A has a $\exists\forall^6\exists^2$-representation over $\mathbb{Z}$, and a $\exists\forall^5\exists^2$-representation over $\mathbb{Z}$ with $\forall$ bounded.*

(ii) *$\bar{A}$ has a $\forall\exists^7$-representation over $\mathbb{Z}$ and also a $\forall\exists^2\forall^2\exists^2$-representation over $\mathbb{Z}$.*

In Section 2 we will prove an auxiliary theorem. Sections 3-5 will be devoted to our proofs of Theorems 1.2-1.4, respectively.

Although we have Theorem 1.1, there are many finite sequences of quantifiers (such as $\forall\exists^k$ $(k=2,3,4,5,6)$, and $\exists\forall^m\exists\forall^n\exists$ $(m\in\{2,3,4\}$ and $n\in\mathbb{N})$ with $\forall$ bounded or not) for which we don't know whether they are undecidable over $\mathbb{Z}$.

It is believed that $\exists^3$ over $\mathbb{Z}$ might be undecidable (cf. [15]). We pose here a conjecture for further research.

Conjecture 1.1. *$\forall^2\exists^2$ over $\mathbb{Z}$ is undecidable.*

We mention that HTP over the field $\mathbb{Q}$ of rational numbers is a difficult open problem. Also, for a general number field K (which is a finite extension of the field $\mathbb{Q}$), HTP over the ring O_K of all algebraic integers in K, remains open. The reader may consult [2, 21] for certain progress.

Our theorems in this paper should have some potential applications. For example, in the spirits of [2, 15, 28], if one investigates mixed quantifiers over Diophantine equations with variables ranging over the rational field $\mathbb{Q}$ or the Gaussian ring $\mathbb{Z}[i]$, our results on mixed quantifiers over $\mathbb{Z}$ will be useful.

2. An auxiliary theorem

In this section we adapt Matiyasevich and Robinson's ideas in [14, 15] to establish an auxiliary theorem on representations of r.e. sets over $\mathbb{Z}$ which will be helpful to our later proofs of Theorems 1.2-1.4.

Lemma 2.1. *Let $B\geqslant b>0$ and $0<n_0<\ldots<n_\nu$. Then an integer c has the form $\sum_{i=0}^{\nu}z_iB^{n_i}$ with $z_i\in\{0,\ldots,b-1\}$ for all $i=0,\ldots,\nu$ if and only if every interval $[\sigma_i,\tau_i]$ $(i=0,\ldots,\nu+1)$ contains at least an integer, where*

$$\sigma_0=\frac{c}{B^{n_0}},\ \sigma_i=\frac{c+1-bB^{n_{i-1}}}{B^{n_i}}\ (i=1,\ldots,\nu),\ \sigma_{\nu+1}=\frac{c+1-bB^{n_\nu}}{(b^2+c^2)B^{n_\nu}},$$
$$\tau_i=\frac{c}{B^{n_i}}\ (i=0,1,\ldots,\nu)\ \text{and}\ \tau_{\nu+1}=\frac{c}{(b^2+c^2)B^{n_\nu}}.$$

Proof. We first prove the "only if" direction. Suppose that $c = \sum_{i=0}^{\nu} z_i B^{n_i}$ with $z_i \in \{0, \dots, b-1\}$ for all $i = 0, \dots, \nu$. For any $j = 0, \dots, \nu$, we have

$$\begin{aligned}\sum_{i=0}^{j} z_i B^{n_i} \leqslant & (b-1)B^{n_j} + \sum_{0 \leqslant i < j} (b-1)B^{n_i} \\ \leqslant & (b-1)B^{n_j} + \sum_{k=0}^{n_j-1} (B-1)B^k = (b-1)B^{n_j} + B^{n_j} - 1 = bB^{n_j} - 1\end{aligned}$$

In particular, $0 \leqslant c = \sum_{i=0}^{\nu} z_i B^{n_i} \leqslant bB^{n_\nu} - 1$ and hence $\sigma_{\nu+1} \leqslant 0 \leqslant \tau_{\nu+1}$. Set

$$x_i = \sum_{j=i}^{\nu} z_j B^{n_j - n_i} \qquad \text{for } i = 0, 1, \dots, \nu.$$

Then $x_0 = \sigma_0$, and

$$x_i = \frac{c - \sum_{j=0}^{i-1} z_j B^{n_j}}{B^{n_i}} \geqslant \frac{c - (bB^{n_{i-1}} - 1)}{B^{n_i}} = \sigma_i$$

for all $i = 1, \dots, \nu$. Also,

$$x_i \leqslant \sum_{j=0}^{\nu} z_j B^{n_j - n_i} = \frac{c}{B^{n_i}} = \tau_i$$

for all $i = 0, \dots, \nu$. Therefore, each interval $[\sigma_i, \tau_i]$ $(i = 0, \dots, \nu+1)$ contains the integer x_i. This proves the "only if" direction.

Now we consider the "if" direction. Suppose that there are integers $x_0, \dots, x_{\nu+1}$ with $\sigma_i \leqslant x_i \leqslant \tau_i$ for all $i = 0, \dots, \nu+1$. Since

$$|c + 1 - bB^{n_\nu}| \leqslant bB^{n_\nu} - 1 + |c| < (b^2 + c^2)B^{n_\nu},$$

we have $|\sigma_{\nu+1}| < 1$. Note also that $|\tau_{\nu+1}| < 1$. As

$$-1 < \sigma_{\nu+1} \leqslant x_{\nu+1} \leqslant \tau_{\nu+1} < 1,$$

we must have $x_{\nu+1} = 0$. From $\sigma_{\nu+1} \leqslant 0 \leqslant \tau_{\nu+1}$, we get $0 \leqslant c < bB^{n_\nu} \leqslant B^{n_\nu+1}$. No matter $B > 1$ or $B = 1$, we can write

$$c = \sum_{k=0}^{n_\nu} c_k B^k$$

with $c_{n_\nu} \in \{0, \dots, b-1\}$ and $c_k \in \{0, \dots, B-1\}$ for all $k = 0, \dots, n_\nu - 1$.

As $\sigma_0 = \tau_0$, we have $\sigma_0 = x_0 \in \mathbb{Z}$ and hence $B^{n_0} \mid c$. Thus $c_k = 0$ for all $k = 0, \dots, n_0 - 1$.

Let $1 \leqslant i \leqslant \nu$. As $\sigma_i \leqslant x_i \leqslant \tau_i$, we have

$$0 \leqslant c - x_i B^{n_i} \leqslant bB^{n_{i-1}} - 1 \leqslant BB^{n_{i-1}} - 1 < B^{n_{i-1}+1} \leqslant B^{n_i}$$

and hence $c - x_i B^{n_i}$ is the least nonnegative residue of c modulo B^{n_i}. Thus

$$\sum_{k=0}^{n_i-1} c_k B^k = c - x_i B^{n_i} < bB^{n_{i-1}}.$$

It follows that $c_{n_{i-1}} < b$ and $c_{n_{i-1}+1} = \dots = c_{n_i-1} = 0$.

By the above, we have $c=\sum_{i=0}^{\nu}z_iB^{n_i}$ with $z_i=c_{n_i}\in\{0,\ldots,b-1\}$ for all $i=0,\ldots,\nu$. This ends our proof of the "if" direction. □

Lemma 2.2. *Let $\sigma_0,\tau_0,\ldots,\sigma_k,\tau_k$ be real numbers with $0\leqslant\tau_i-\sigma_i\leqslant 1$ for all $i=0,\ldots,k$. Let W be an integer with*

$$W\geqslant 1+\max\{\tau_i-\tau_{i+1}:\ i=0,\ldots,k-1\}.$$

(i) *For any integer t with $t\leqslant\tau_0-1$ or $t\geqslant\tau_k+kW$, we have*

$$\prod_{i=0}^{k}(t-\sigma_i-iW)(t+1-\tau_i-iW)\geqslant 0. \tag{2.1}$$

(ii) *Every interval $[\sigma_i,\tau_i]$ $(0\leqslant i\leqslant k)$ contains an integer if and only if (2.3) holds for all $t\in\mathbb{Z}$.*

Proof. Set $\sigma_i'=\sigma_i+iW$ and $\tau_i'=\tau_i+iW$ for all $i=0,\ldots,k$. Note that

$$\tau_i'-1\leqslant\sigma_i'\leqslant\tau_i'.$$

If $0\leqslant i<k$, then

$$\tau_i'=\tau_i+iW\leqslant\tau_{i+1}-1+W+iW=\tau_{i+1}'-1\leqslant\sigma_{i+1}'.$$

Let $t\in\mathbb{Z}$ and $0\leqslant j\leqslant k$. Suppose that $(t-\sigma_j')(t+1-\tau_j')<0$, which is equivalent to $\tau_j'-1<t<\sigma_j'$. For $0\leqslant i<j$ we have $\sigma_i'\leqslant\tau_{i+1}'-1\leqslant\cdots\leqslant\tau_j'-1<t$. If $j<i\leqslant k$, then $t<\sigma_j'\leqslant\tau_{j+1}'-1\leqslant\cdots\leqslant\tau_i'-1\leqslant\sigma_i'$. Thus $(t-\sigma_i')(t+1-\tau_i')>0$ for all $i=0,\ldots,k$ with $i\neq j$, and hence

$$\prod_{i=0}^{k}(t-\sigma_i')(t+1-\tau_i')<0.$$

Therefore,

$$\begin{aligned}&\prod_{i=0}^{k}(t-\sigma_i')(t+1-\tau_i')\geqslant 0\\ \iff&(t-\sigma_j')(t+1-\tau_j')\geqslant 0\text{ for all }j=0,\ldots,k\\ \iff&t\notin\bigcup_{j=0}^{k}(\tau_j'-1,\sigma_j').\end{aligned}$$

(i) If $t\leqslant\tau_0-1$, then $t\leqslant\tau_0'-1\leqslant\tau_1'-1\leqslant\cdots\leqslant\tau_k'-1$ and hence $\prod_{i=0}^{k}(t-\sigma_i')(t+1-\tau_i')\geqslant 0$ by the above. Similarly, if $t\geqslant\tau_k+kW$ then $\sigma_0'\leqslant\sigma_1'\leqslant\cdots\leqslant\sigma_k'\leqslant\tau_k'\leqslant t$ and hence $\prod_{i=0}^{k}(t-\sigma_i')(t+1-\tau_i')\geqslant 0$.

(ii) For any $i=0,\ldots,k$, clearly $(\tau_i-1,\sigma_i)\cup[\sigma_i,\tau_i]=(\tau_i-1,\tau_i]$ contains a unique integer. So

$$\begin{aligned}&[\sigma_i,\tau_i]\text{ contains an integer for all }i=0,\ldots,k\\ \iff&(\tau_i-1,\sigma_i)\text{ contains no integer for all }i=0,\ldots,k\\ \iff&(\tau_i'-1,\sigma_i')\text{ contains no integer for all }i=0,\ldots,k\\ \iff&\prod_{i=0}^{k}(t-\sigma_i')(t+1-\tau_i')\geqslant 0\quad\text{for all }t\in\mathbb{Z}.\end{aligned}$$

In view of the above, we have completed the proof of Lemma 2.2. □

Lemma 2.3. *Let δ and L be positive integers. Suppose that $z_0,\ldots,z_\nu\in\mathbb{N}$ and*

$$P(z_0,\ldots,z_\nu)=\sum_{\substack{i_0,\ldots,i_\nu\in\mathbb{N}\\ i_0+\cdots+i_\nu\leqslant\delta}}a_{i_0,\ldots,i_\nu}z_0^{i_0}\ldots z_\nu^{i_\nu}$$

with $a_{i_0,\ldots,i_\nu}\in\mathbb{Z}$ and $|a_{i_0,\ldots,i_\nu}|\leqslant L$. Let B be any integer greater than $2(1+z_0+\cdots+z_\nu)^\delta\delta!L$. Then $P(z_0,\ldots,z_\nu)=0$ if and only if

$$\frac{2C(B)D(B)-B^{(\delta+1)^{\nu+1}}}{2B^{(\delta+1)^{\nu+1}+1}}\leqslant z\leqslant\frac{2C(B)D(B)+B^{(\delta+1)^{\nu+1}}}{2B^{(\delta+1)^{\nu+1}+1}}\tag{2.2}$$

for some integer z, where $C(x)=(1+\sum_{i=0}^{\nu}z_ix^{(\delta+1)^i})^\delta$ and

$$D(x)=\sum_{\substack{i_0,\ldots,i_\nu\in\mathbb{N}\\ i_0+\cdots+i_\nu\leqslant\delta}}i_0!\ldots i_\nu!(\delta-i_0-\cdots-i_\nu)!a_{i_0,\ldots,i_\nu}x^{(\delta+1)^{\nu+1}-\sum_{j=0}^{\nu}i_j(\delta+1)^j}.$$

Proof. Write

$$C(x)=\sum_{i=0}^{\delta(\delta+1)^\nu}c_ix^i\text{ and }D(x)=\sum_{j=0}^{(\delta+1)^{\nu+1}}d_jx^j.$$

Then $c_i\geqslant 0$, and also $|d_j|\leqslant\delta!L$ since the multi-nomial coefficient

$$\binom{\delta}{i_0,\ldots,i_\nu,\delta-i_0-\cdots-i_\nu}=\frac{\delta!}{i_0!\ldots i_\nu!(\delta-i_0-\cdots-i_\nu)!}\geqslant 1$$

for all $i_0,\ldots,i_\nu\in\mathbb{N}$ with $i_0+\cdots+i_\nu\leqslant\delta$. Write

$$C(x)D(x)=\sum_{k=0}^{(2\delta+1)(\delta+1)^\nu}r_kx^k.$$

Then

$$r_k=\sum_{\substack{0\leqslant i\leqslant\delta(\delta+1)^\nu\\ 0\leqslant j\leqslant(\delta+1)^{\nu+1}\\ i+j=k}}c_id_j$$

and

$$|r_k|\leqslant\sum_{i=0}^{\delta(\delta+1)^\nu}c_i\delta!L=C(1)\delta!L=(1+z_0+\cdots+z_\nu)^\delta\delta!L<\frac{B}{2}.$$

By the multi-nomial theorem,

$$C(x)=\sum_{\substack{i_0,\ldots,i_\nu\in\mathbb{N}\\ i_0+\cdots+i_\nu\leqslant\delta}}\binom{\delta}{i_0,\ldots,i_\nu,\delta-i_0-\cdots-i_\nu}z_0^{i_0}\ldots z_\nu^{i_\nu}x^{\sum_{j=0}^\nu i_j(\delta+1)^j}.$$

Therefore

$$r_{(\delta+1)^{\nu+1}}=\sum_{\substack{i_0,\ldots,i_\nu\in\mathbb{N}\\ i_0+\cdots+i_\nu\leqslant\delta}}\delta!a_{i_0,\ldots,i_\nu}z_0^{i_0}\ldots z_\nu^{i_\nu}=\delta!P(z_0,\ldots,z_\nu).$$

Suppose that $P(z_0,\ldots,z_\nu)=0$. Then $r_{(\delta+1)^{\nu+1}}=0$. For the integer

$$z=\sum_{k=(\delta+1)^{\nu+1}+1}^{(2\delta+1)(\delta+1)^\nu}r_kB^{k-1-(\delta+1)^{\nu+1}},$$

we have

$$C(B)D(B)-zB^{(\delta+1)^{\nu+1}+1}=\sum_{k=0}^{(\delta+1)^{\nu+1}-1}r_kB^k$$

and hence

$$\begin{aligned}\left|C(B)D(B)-zB^{(\delta+1)^{\nu+1}+1}\right|&\leqslant\sum_{k=0}^{(\delta+1)^{\nu+1}-1}|r_k|B^k\\&\leqslant\frac{B-1}{2}\sum_{k=0}^{(\delta+1)^{\nu+1}-1}B^k\leqslant\frac{B^{(\delta+1)^{\nu+1}}}{2}.\end{aligned}$$

Therefore (2.2) is valid.

Now we assume that (2.2) holds for some $z\in\mathbb{Z}$. We want to show that $P(z_0,\ldots,z_\nu)=0$. By (2.2) we have

$$\left|C(B)D(B)-zB^{(\delta+1)^{\nu+1}+1}\right|\leqslant\frac{1}{2}B^{(\delta+1)^{\nu+1}}.$$

Let

$$S:=r_{(\delta+1)^{\nu+1}}+\sum_{k=(\delta+1)^{\nu+1}+1}^{(2\delta+1)(\delta+1)^\nu}r_kB^{k-(\delta+1)^{\nu+1}}-Bz.$$

Then

$$\begin{aligned}SB^{(\delta+1)^{\nu+1}}=&r_{(\delta+1)^{\nu+1}}B^{(\delta+1)^{\nu+1}}+\sum_{k=(\delta+1)^{\nu+1}+1}^{(2\delta+1)(\delta+1)^\nu}r_kB^k-zB^{(\delta+1)^{\nu+1}+1}\\=&C(B)D(B)-\sum_{k=0}^{(\delta+1)^{\nu+1}-1}r_kB^k-zB^{(\delta+1)^{\nu+1}+1}\end{aligned}$$

and hence

$$|SB^{(\delta+1)^{\nu+1}}| \leqslant |C(B)D(B) - zB^{(\delta+1)^{\nu+1}+1}| + \sum_{k=0}^{(\delta+1)^{\nu+1}-1} |r_k|B^k$$
$$\leqslant \frac{B^{(\delta+1)^{\nu+1}}}{2} + \frac{B-1}{2}\sum_{k=0}^{(\delta+1)^{\nu+1}-1} B^k = B^{(\delta+1)^{\nu+1}} - \frac{1}{2}.$$

Therefore we must have $S = 0$. It follows that $B \mid r_{(\delta+1)^{\nu+1}}$. As

$$\left|r_{(\delta+1)^{\nu+1}}\right| < \frac{B}{2},$$

we have

$$\delta! P(z_0, \ldots, z_\nu) = r_{(\delta+1)^{\nu+1}} = 0$$

and hence $P(z_0, \ldots, z_\nu) = 0$.

In view of the above, we have completed the proof of Lemma 2.3. □

Lemma 2.3 and its proof also appeared in the author's recent book [25, pp. 117-119] in Chinese.

Now we present our auxiliary theorem.

Theorem 2.4. *Let $A \subseteq \mathbb{N}$ be any r.e. set. Then, there are $L[x] \in \mathbb{Z}[x]$ and $M(x, y, z, t) \in \mathbb{Z}[x, y, z, t]$ satisfying the following* (i)-(iii).

(i) *$L(a) > 0$ for all $a \in \mathbb{Z}$.*

(ii) *There are $k_0, k_1, k_2 \in \mathbb{Z}^+$ such that $M(a, b, c, t) \geqslant 0$ whenever a, b, c, t are integers with $a \geqslant 0$, $b > 1$, and $t < -c^2 \vee t > R(a, c)$, where $R(a, c) = k_0(1 + c)^{2k_1} L(a) + k_2$.*

(iii) *For any $a \in \mathbb{N}$ and any infinite subset S of $\mathbb{N}$, we have*

$$a \in A \iff \exists b \in S \exists c \forall t\, (M(a, b, c, t) \geqslant 0).$$

(iv) *For any infinite subset S of $\mathbb{N}$, there is a positive integer n such that for any $a \in A$ and $N \in \mathbb{N}$ there are $b \in S$ and $c \in \mathbb{Z}$ for which $b \geqslant N$, $b \mid c$, $0 < c < b^n$, and $M(a, b, c, t) \geqslant 0$ for all $t \in \mathbb{Z}$.*

Proof. By Matiyasevich's theorem [9], there is a polynomial $P_0(z_0, z_1, \ldots, z_\nu) \in \mathbb{Z}[z_0, \ldots, z_\nu]$ such that for any $a \in \mathbb{N}$ we have

$$a \in A \iff \exists z_1 \geqslant 0 \ldots \exists z_\nu \geqslant 0\, (P_0(a, z_1, \ldots, z_\nu) = 0).$$

Define

$$P(a, z_0, \ldots, z_\nu) = (z_0 - 1)^2 + P_0^2(a, z_1, \ldots, z_\nu),$$

and write

$$P(a, z_0, \ldots, z_\nu) = \sum_{\substack{i_0, \ldots, i_\nu \in \mathbb{N} \\ i_0 + \cdots + i_\nu \leqslant \delta}} p_{i_0, \ldots, i_\nu}(a) z_0^{i_0} \ldots z_\nu^{i_\nu},$$

where δ is a positive even number. Set

$$L(a) = \sum_{\substack{i_0, \ldots, i_\nu \in \mathbb{N} \\ i_0 + \cdots + i_\nu \leqslant \delta}} p_{i_0, \ldots, i_\nu}(a)^2.$$

Then $L(a)\geqslant p_{2,0,\ldots,0}(a)^2=1$ for all $a\in\mathbb{Z}$. As δ is even, we have

$$B(a,b):=2(\nu+1)^\delta b^\delta\delta!L(a)\geqslant 2$$

for all $a,b\in\mathbb{Z}$ with $b\neq 0$.

Now fix $a\in\mathbb{N}$ and $b\in\{2,3,\ldots\}$. Then $B(a,b)\geqslant b^\delta\geqslant b\geqslant 2$. For convenience, we set $n_j=(\delta+1)^j$ for all $j=0,\ldots,\nu+1$. Note that $P_0(a,z_1,\ldots,z_\nu)=0$ for some $z_1,\ldots,z_\nu\in\{0,\ldots,b-1\}$ if and only if $P(a,z_0,\ldots,z_\nu)=0$ for some $z_0,\ldots,z_\nu\in\{0,\ldots,b-1\}$. If $z_0,\ldots,z_\nu\in\{0,\ldots,b-1\}$, then

$$B(a,b)>2(1+(\nu+1)(b-1))^\delta\delta!L(a)\geqslant 2(1+z_0+\cdots+z_\nu)^\delta\delta!L(a).$$

Thus, in view of Lemma 2.3, $P(a,z_0,\ldots,z_\nu)=0$ for some $z_0,\ldots,z_\nu\in\{0,\ldots,b-1\}$ if and only if for some

$$c\in\left\{\sum_{i=0}^\nu z_iB(a,b)^{n_i}:\ z_0,\ldots,z_\nu\in\{0,\ldots,b-1\}\right\}$$

we have

$$\frac{2(1+c)^\delta D(a,b)-B(a,b)^{n_{\nu+1}}}{2B(a,b)^{n_{\nu+1}+1}}\leqslant z\leqslant\frac{2(1+c)^\delta D(a,b)+B(a,b)^{n_{\nu+1}}}{2B(a,b)^{n_{\nu+1}+1}}$$

for some integer z, where

$$D(a,b)=\sum_{\substack{i_0,\ldots,i_\nu\in\mathbb{N}\\ i_0+\cdots+i_\nu\leqslant\delta}}i_0!\ldots i_\nu!(\delta-i_0-\cdots-i_\nu)!p_{i_0,\ldots,i_\nu}(a)B(a,b)^{n_{\nu+1}-\sum_{j=0}^\nu i_jn_j}.$$

Combining this with Lemma 2.1, we see that $P_0(a,z_1,\ldots,z_\nu)=0$ for some $z_0,\ldots,z_\nu\in\{0,\ldots,b-1\}$ if and only if for some $c\in\mathbb{Z}$, every interval $[\sigma_i,\tau_i]$ $(i=0,\ldots,\nu+2)$ contains an integer, where

$$\sigma_0=\tau_0=\frac{c}{B(a,b)},$$

$$\sigma_i=\frac{c+1-bB(a,b)^{n_{i-1}}}{B(a,b)^{n_i}}\text{ and }\tau_i=\frac{c}{B(a,b)^{n_i}}\ (i=1,\ldots,\nu),$$

$$\sigma_{\nu+1}=\frac{c+1-bB(a,b)^{n_\nu}}{(b^2+c^2)B(a,b)^{n_\nu}}\text{ and }\tau_{\nu+1}=\frac{c}{(b^2+c^2)B(a,b)^{n_\nu}},$$

$$\sigma_{\nu+2}=\frac{2(1+c)^\delta D(a,b)-B(a,b)^{n_{\nu+1}}}{2B(a,b)^{n_{\nu+1}+1}}\text{ and }\tau_{\nu+2}=\frac{2(1+c)^\delta D(a,b)+B(a,b)^{n_{\nu+1}}}{2B(a,b)^{n_{\nu+1}+1}}.$$

Observe that

$$|\tau_i-\tau_{i+1}|=\left(\frac{1}{B(a,b)^{n_i}}-\frac{1}{B(a,b)^{n_{i+1}}}\right)|c|\leqslant\frac{|c|}{B(a,b)^{n_i}}\leqslant\frac{|c|}{2}$$

for all $i=0,\ldots,\nu-1$, and

$$|\tau_\nu-\tau_{\nu+1}|=\left(1-\frac{1}{b^2+c^2}\right)\frac{|c|}{B(a,b)^{n_\nu}}\leqslant\frac{|c|}{B(a,b)^{n_\nu}}\leqslant\frac{|c|}{2}.$$

Note also that

$$|D(a,b)| \leqslant \sum_{i=0}^{n_{\nu+1}} \delta!L(a)B(a,b)^i = \delta!L(a)\frac{B(a,b)^{n_{\nu+1}+1}-1}{B(a,b)-1} \leqslant \delta!L(a)B(a,b)^{n_{\nu+1}+1}$$

and hence

$$\begin{aligned}\tau_{\nu+1}-\tau_{\nu+2} \leqslant& \frac{c/(b^2+c^2)}{B(a,b)^{n_\nu}} - \left(\frac{1}{2B(a,b)} - \delta!L(a)(1+c)^\delta\right)\\ \leqslant& \frac{1}{2bB(a,b)^{n_\nu}} - \frac{1}{2B(a,b)} + \delta!L(a)(1+c)^\delta \leqslant 1+\delta!L(a)(1+c)^\delta.\end{aligned}$$

Let $W = 2+(1+c)^\delta\delta!L(a)$. Then $W-1 \geqslant 1+(1+c)^\delta \geqslant 1+|c+1| \geqslant |c| \geqslant |c|/2$, and hence by the above we have

$$W \geqslant 1+\max\{\tau_i-\tau_{i+1}:\ i=0,\ldots,\nu+1\}.$$

In view of the above and Lemma 2.2(ii), $P_0(a,z_1,\ldots,z_\nu)=0$ for some $z_1,\ldots,z_\nu \in \{0,\ldots,b-1\}$ if and only if for some integer c we have $Q(a,b,c,t) \geqslant 0$ for all $t\in\mathbb{Z}$, where $Q(a,b,c,t)$ denotes

$$\begin{aligned}&(B(a,b)t-c)(B(a,b)(t+1)-c)\\ &\times\prod_{i=1}^{\nu}\left(B(a,b)^{n_i}(t-iW)-c-1+bB(a,b)^{n_{i-1}}\right)\left(B(a,b)^{n_i}(t+1-iW)-c\right)\\ &\times\left((b^2+c^2)B(a,b)^{n_\nu}(t-(\nu+1)W)-c-1+bB(a,b)^{n_\nu}\right)\\ &\times\left((b^2+c^2)B(a,b)^{n_\nu}(t+1-(\nu+1)W)-c\right)\\ &\times\left(2B(a,b)^{n_{\nu+1}+1}(t-(\nu+2)W)-2(1+c)^\delta D(a,b)+B(a,b)^{n_{\nu+1}}\right)\\ &\times\left(2B(a,b)^{n_{\nu+1}+1}(t+1-(\nu+2)W)-2(1+c)^\delta D(a,b)-B(a,b)^{n_{\nu+1}}\right).\end{aligned}$$

Let S be any infinite subset of $\mathbb{N}$. By the above, for any $a\in\mathbb{N}$ we have

$$\begin{aligned}a\in A &\iff P_0(a,z_1,\ldots,z_\nu)=0 \text{ for some } z_1,\ldots,z_\nu\in\mathbb{N}\\ &\iff \exists b\in S\,(b\geqslant 2\wedge\exists z_1\in[0,b)\ldots\exists z_\nu\in[0,b)(P(a,z_1,\ldots,z_\nu)=0))\\ &\iff \exists b\in S(b^2>b\wedge\exists c\forall t(Q(a,b,c,t)\geqslant 0))\\ &\iff \exists b\in S\exists c\forall t\,(M(a,b,c,t)\geqslant 0),\end{aligned}$$

where $M(a,b,c,t)=(b^2-b)(Q(a,b,c,t)+1)-1\in\mathbb{Z}[a,b,c,t]$ does not depend on S.

Given $a\in A$ and $N\in\mathbb{N}$, we may take $b\in S$ with

$$b\geqslant\max\{N,\,2(\nu+1)^\delta\delta!L(a)\}$$

such that $P(a,z_0,\ldots,z_\nu)=0$ for some $z_0,\ldots,z_\nu\in[0,b)$ with $z_0=1$. Then $c=\sum_{i=0}^{\nu}z_iB(a,b)^{n_i}\equiv 0\pmod b$ since $b\mid B(a,b)$. By Lemmas 2.1-2.3, for any $t\in\mathbb{Z}$ we have

$$\prod_{i=0}^{\nu+2}(t-\sigma_i-iW)(t+1-\tau_i-iW)\geqslant 0\ \ \text{(i.e., } Q(a,b,c,t)\geqslant 0) \tag{2.3}$$

It follows that $M(a,b,c,t)\geqslant 0$ for all $t\in\mathbb{Z}$. Note that

$$\begin{aligned}1=z_0\leqslant c\leqslant&\sum_{i=0}^{\nu}(b-1)B(a,b)^{n_i}\leqslant(b-1)\frac{B(a,b)^{n_\nu+1}-1}{B(a,b)-1}\\<&B(a,b)^{n_\nu+1}=(2(\nu+1)^\delta b^\delta\delta!L(a))^{n_\nu+1}\leqslant(b^{\delta+1})^{n_\nu+1}=b^n,\end{aligned}$$

where $n=(\delta+1)(n_\nu+1)$ only depends on A.

Now it remains to show that (ii) in Theorem 2.4 holds. Let $a\in\mathbb{N}$, $b\in\{2,3,\ldots\}$ and $c\in\mathbb{Z}$. Then

$$-c^2-1\leqslant-|c|-1\leqslant\frac{c}{B(a,b)}-1=\tau_0-1$$

and

$$\begin{aligned}\tau_{\nu+2}+(\nu+2)W=&\frac{1}{2B(a,b)}+\frac{(1+c)^\delta D(a,b)}{B(a,b)^{n_{\nu+1}+1}}+(\nu+2)W\\\leqslant&\frac{1}{2B(a,b)}+(1+c)^\delta\delta!L(a)+(\nu+2)W\\<&1+(1+c)^\delta\delta!L(a)+(\nu+2)((1+c)^\delta\delta!L(a)+2)\\=&(\nu+3)(1+c)^\delta\delta!L(a)+2\nu+5.\end{aligned}$$

Thus, if t is an integer with $t<-c^2$ or $t>R(a,c)=(\nu+3)(1+c)^\delta\delta!L(a)+2\nu+4$ then by Lemma 2.2(i) we have (2.3) and hence $M(a,b,c,t)\geqslant 0$. This concludes our proof. □

3. Proof of Theorem 1.2

For convenience, we define $\square=\{m^2:\ m\in\mathbb{Z}\}$.

Lemma 3.1. *Let $C\in\mathbb{Z}$. Then*

$$C\geqslant 0\iff\exists x\exists y\exists z(C=x^2+y^2+z^2+z),\tag{3.1}$$

$$C\geqslant 0\iff\exists_{x\neq 0}((4C+2)x^2+1\in\square),\tag{3.2}$$

$$C\neq 0\iff\exists u\exists v(C=(2u+1)(3v+1)).\tag{3.3}$$

Proof. This is easy and known. Concerning (3.1), by the Gauss-Legendre theorem on sums of three squares, $C\geqslant 0$ if and only if $4C+1=(2x)^2+(2y)^2+(2z+1)^2$ (i.e., $C=x^2+y^2+z^2+z$) for some $x,y,z\in\mathbb{Z}$. By the theory of Pell equations, we have (3.2) which was first used by Sun [23]. As any nonzero integer has the form $\pm 3^a(3q+1)$ with $a\in\mathbb{N}$ and $q\in\mathbb{Z}$, we immediately get (3.3) which was an observation due to Tung [26]. □

Lemma 3.2. *Let $C_1,\ldots,C_n\in\mathbb{Z}$.*

(i) *We have*

$$\begin{aligned}&C_1\geqslant 0\vee\cdots\vee C_n\geqslant 0\\ \iff&\exists x\neq 0((4C_1+2)x^2+1\in\square\vee\cdots\vee(4C_n+2)x^2+1\in\square)\\ \iff&\exists u\exists v\exists w\left(\prod_{i=1}^n(2(2C_i+1)(2u+1)^2(3v+1)^2-w^2+1)=0\right).\end{aligned}$$

Also,

$$\begin{aligned}&C_1\geqslant 0\wedge\cdots\wedge C_n\geqslant 0\\ \iff&\forall x\neq 0\forall y\left(\prod_{i=1}^n((4C_i+2)x^2+y^2-1)\neq 0\right)\\ \iff&\forall x\forall y\exists u\exists v\left(x\left(\prod_{i=1}^n((4C_i+2)x^2+y^2-1)-(2u+1)(3v+1)\right)=0\right).\end{aligned}$$

(ii) *Suppose that $D_i\in\mathbb{N}$ and $|C_i|\leqslant D_i$ for all $i=1,\ldots,n$. Then*

$$\begin{aligned}&C_1\geqslant 0\wedge\cdots\wedge C_n\geqslant 0\\ \iff&\forall x\in[0,D_1\cdots D_n]\left(\prod_{i=1}^n(x+C_i+1)\neq 0\right)\\ \iff&\forall x\in[0,D_1\cdots D_n]\exists y\exists z\left(\prod_{i=1}^n(x+C_i+1)-(2y+1)(3z+1)=0\right)\end{aligned}$$

Proof. (i) The first assertion follows immediately from Lemma 3.1. As for the second assertion, it suffices to note that

$$C_i\geqslant 0\iff -C_i-1\ngeqslant 0\iff\forall x\neq 0((4(-C_i-1)+2)x^2+1\notin\square).$$

(ii) If $C_i\geqslant 0$ for all $i=1,\ldots,n$, then for any $x\geqslant 0$ we have $x+C_i+1>0$ for all $i=1,\ldots,n$, and hence $\prod_{i=1}^n(x+C_i+1)\neq 0$. If $C_i<0$ for some $1\leqslant i\leqslant n$, then for $x=-C_i-1$ we have $0\leqslant x\leqslant|C_i|\leqslant D_i\leqslant D_1\cdots D_n$. So part (ii) of Lemma 3.2 holds.

In view of the above, we have completed the proof of Lemma 3.2. □

Proof of Theorem 1.2. Take polynomials R and M (depending on A) as in Theorem 2.4, and note that $S=\{b^2+2:\ b\in\mathbb{N}\}$ is an infinite set. By Theorem 2.4, for any $a\in\mathbb{N}$ we have

$$\begin{aligned}a\in A&\iff\exists b\exists c\forall t[M(a,b^2+2,c,t)\geqslant 0]\\&\iff\exists b\exists c\forall t\in[-c^2,R(a,c)](M(a,b^2+2,c,t)\geqslant 0)\end{aligned}$$

and hence

$$a\in\bar{A}\iff\forall b\forall c\exists t\,(-M(a,b^2+2,c,t)-1\geqslant 0),$$

also $M(a,b^2+2,c,t)\geqslant 0$ whenever $t<-c^2$ or $t>R(a,c)$. Moreover, if $a\in A$ then we may require further that $c>0$ and $(b^2+2)\mid c$.

In view of the above and Lemmas 3.1-3.2, we see that A has a $\exists^2\forall\exists^3$-representation over $\mathbb{Z}$ with $\forall$ bounded or unbounded, and also a $\exists^2\forall^3\exists^2$-representation over $\mathbb{Z}$. For $a\in\mathbb{N}$, $b,c\in\mathbb{Z}$ and $t\in[-c^2,R(a,c)]$, we clearly have $|M(a,b^2+2,c,t)|\leqslant P(a,b,c)^2$ for some $P(x,y,z)\in\mathbb{Z}[x,y,z]$. So, by using Lemma 3.2(ii) we see that A also has a $\exists^2\forall^2\exists^2$-representation over $\mathbb{Z}$ with $\forall$ bounded. With the help of Lemma 3.2, $\bar{A}$ has a $\forall^2\exists^4$-representation and also a $\forall^2\exists\forall^2\exists^2$-representation over $\mathbb{Z}$.

Let $D(c,s)=(s-c^2)(s-c^2-2c)$ and $a\in\mathbb{N}$. We claim that

$$\begin{aligned}a\in A&\iff\exists s\forall t\exists c\geqslant 0\,(D(c,s)\leqslant 0\wedge M(a,(s-c^2)^2+2,c,t)\geqslant 0)\\&\iff\exists s\forall t\in[-s^2,R(a,s)]\exists c\geqslant 0\\&\qquad(D(c,s)\leqslant 0\wedge M(a,(s-c^2)^2+2,c,t)\geqslant 0).\end{aligned}$$

Now we prove the claim. If $a\in A$, then for some $b\in\mathbb{N}$ and $c\in\mathbb{Z}^+$ with $(b^2+2)\mid c$ we have $M(a,b^2+2,c,t)\geqslant 0$ for all $t\in\mathbb{Z}$. As $0\leqslant b\leqslant b^2\leqslant c\leqslant 2c$, for $s=b+c^2$ we have $c^2\leqslant s\leqslant c^2+2c$ and hence $D(c,s)\leqslant 0$, and also

$$M(a,(s-c^2)^2+2,c,t)=M(a,b^2+2,c,t)\geqslant 0$$

for all $t\in\mathbb{Z}$.

Now suppose that $s\in\mathbb{Z}$ and that for any $t\in[-s^2,R(a,s)]$ there is a number $c\in\mathbb{N}$ with $D(c,s)\leqslant 0$ and $M(a,(s-c^2)^2+2,c,t)\geqslant 0$. Note that $c^2\leqslant s\leqslant c^2+2c<(c+1)^2$. So $c=\lfloor\sqrt{s}\rfloor$ does not depend on t. Set $b=s-\lfloor\sqrt{s}\rfloor^2$. Then

$$M(a,b^2+2,c,t)=M(a,(s-c^2)^2+2,c,t)\geqslant 0$$

for all $t\in[-s^2,R(a,s)]$. If $t<-s^2$ then $t<-s\leqslant -c^2$ and hence $M(a,b^2+2,c,t)\geqslant 0$. If $t>R(a,s)$ then $t>R(a,c)$ (since $s\geqslant c^2\geqslant c\geqslant 0$) and hence $M(a,b^2+2,c,t)\geqslant 0$. Therefore $M(a,b^2+2,c,t)\geqslant 0$ for all $t\in\mathbb{Z}$, and hence $a\in A$. This concludes the proof of the claim.

In view of the proved claim, for any $a\in\mathbb{N}$ we have

$$\begin{aligned}a\in A&\iff\exists s\forall t\exists c\,(c\geqslant 0\wedge -D(c,s)\geqslant 0\wedge M(a,(s-c^2)^2+2,c,t)\geqslant 0)\\&\iff\exists s\forall t\in[-s^2,R(a,s)]\exists c\,(c\geqslant 0\wedge -D(c,s)\geqslant 0\\&\qquad\wedge M(a,(s-c^2)^2+2,c,t)\geqslant 0)\end{aligned}$$

and hence

$$\begin{aligned}a\in\bar{A}\iff\forall s\exists t\forall c\,(&-c-1\geqslant 0\vee D(c,s)-1\geqslant 0\\&\vee -M(a,(s-c^2)^2+2,c,t)-1\geqslant 0)\end{aligned}$$

Combining this with Lemma 3.2, we find that A has a $\exists\forall\exists\forall^2\exists^2$-representation over $\mathbb{Z}$ and a $\exists\forall\exists\forall\exists^2$-representation over $\mathbb{Z}$ with $\forall$ bounded. Also, $\bar{A}$ has a $\forall\exists\forall\exists^3$-representation over $\mathbb{Z}$.

In view of the above, we have completed the proof of Theorem 1.2. □

4. Proof of Theorem 1.3

Let $J_k(x_1,\dots,x_k,x)$ be the polynomial

$$\prod_{\varepsilon_1,\dots,\varepsilon_k\in\{\pm1\}}\left(x+\varepsilon_1\sqrt{x_1}+\varepsilon_2\sqrt{x_2}X+\cdots+\varepsilon_k\sqrt{x_k}X^{k-1}\right)$$

with $X=1+\sum_{j=1}^k x_j^2$. This polynomial (in $x_1,\dots,x_n,x$) with integer coefficients was introduced by Matiyasevich and Robinson [15]. For fixed $A_1,\dots,A_k\in\mathbb{Z}$, the monic polynomial $J_k(A_1,\dots,A_k,x)$ is of degree 2^k in x.

Lemma 4.1. *Let $A_1,\dots,A_k\in\mathbb{Z}$.*

(i) *We have*

$$A_1,\dots,A_k\in\square \iff \exists x(J_k(A_1,\dots,A_k,x)=0).$$

(ii) *If $S,T\in\mathbb{Z}$ and $S\neq 0$, then*

$$\begin{aligned}&A_1\in\square\wedge\cdots\wedge A_k\in\square\wedge S\mid T\\ \iff&\exists x\left(S^{2^k}J_k\left(A_1,\dots,A_k,x+\frac{T}{S}\right)=0\right).\end{aligned}$$

(iii) (Matiyasevich-Robinson Relation-Combining Theorem [15]) *If $R,S,T\in\mathbb{Z}$ and $S\neq 0$, then*

$$\begin{aligned}&A_1\in\square\wedge\cdots\wedge A_k\in\square\wedge S\mid T\wedge R>0\\ \iff&\exists n\geqslant 0\left((S^2(1-2R))^{2^k}J_k\left(A_1,\dots,A_k,T^2+W^k+\frac{S^2n+T^2}{S^2(1-2R)}\right)=0\right),\end{aligned}$$

where $W=1+\sum_{i=1}^k A_i^2$.

Remark 4.1. Parts (i) and (iii) of Lemma 4.1 were due to Matiyasevich and Robinson [15, Theorems 1-3]. Part (ii) was stated explicitly in [22, Lemma 17]; in fact, if x_0+T/S is a rational zero of the monic polynomial $J_k(A_1,\dots,A_k,x)$ then it is an integer since any rational algebraic integer must belong to $\mathbb{Z}$.

Proof of Theorem 1.3. Take polynomials R and M (depending on A) as in Theorem 2.4 and note that $S=\{4b+3:\ b\in\square\}$ is an infinite set. By Theorem 2.4, for any $a\in\mathbb{N}$ we have

$$a\geqslant 0\wedge b\in\square\wedge(t<-(c+1)^2\vee t>R(a,c+1))\Rightarrow M(a,4b+3,c+1,t)\geqslant 0$$

and

$$a\in A\iff\exists b\in\square\,\exists c\forall t(M(a,4b+3,c+1,t)\geqslant 0).$$

Moreover, if $a\in A$ then we may choose $b\in\square$ and $c\geqslant 0$ with $(4b+3)\mid(c+1)$ such that $M(a,4b+3,c+1,t)\geqslant 0$ for all $t\in\mathbb{Z}$.

Let $a\in\mathbb{N}$. We claim that

$$\begin{aligned}&a\in A\\ \iff&\exists s\forall t\exists c\,(s-c^2\in\square\wedge(4(s-c^2)+3)\mid(c+1)\\&\qquad\wedge(c+1)^2(M(a,4(s-c^2)+3,c+1,t)+1)>0)\\ \iff&\exists s\forall t\in[-(s+1)^2,R(a,s+1)]\exists c\,(s-c^2\in\square\wedge(4(s-c^2)+3)\mid(c+1)\\&\qquad\wedge(c+1)^2(M(a,4(s-c^2)+3,c+1,t)+1)>0).\end{aligned}$$

When $a\in A$, we may choose $b\in\square$ and $c\geqslant 0$ for which

$$4b+3\mid c+1\wedge\forall t(M(a,4b+3,c+1,t)\geqslant 0).$$

Take $s=b+c^2$, Then $s-c^2=b\in\square$, $4(s-c^2)+3=4b+3$ divides $c+1$, and

$$M(a,4(s-c^2)+3,c+1,t)=M(a,4b+3,c+1,t)\geqslant 0$$

for all $t\in\mathbb{Z}$. Note that $(c+1)^2(M(a,4(s-c^2)+3,c+1,t)+1)>0$.

Now we prove the remaining direction of the claim. Suppose that $s\in\mathbb{Z}$ and that for any $t\in[-(s+1)^2,R(a,s+1)]$ there is an integer $c(t)$ for which

$$\begin{aligned}&s-c(t)^2\in\square,\ (4(s-c(t)^2)+3)\mid(c(t)+1),\\&(c(t)+1)^2(M(a,4(s-c(t)^2)+3,c(t)+1,t)+1)>0.\end{aligned}$$

Clearly, $c(t)+1\neq 0$ and

$$\begin{aligned}c(t)^2\leqslant s&=(s-c(t)^2)+c(t)^2<4(s-c(t)^2)+3+c(t)^2\\&\leqslant|c(t)+1|+c(t)^2\leqslant(|c(t)|+1)^2.\end{aligned}$$

Hence $s\geqslant 0$ and $|c(t)|=\lfloor\sqrt{s}\rfloor$. Since

$$\lfloor\sqrt{s}\rfloor+1+(-\lfloor\sqrt{s}\rfloor+1)=2\not\equiv 0\ (\mathrm{mod}\ \ 4(s-c(t)^2)+3),$$

there is a unique $c\in\{\pm\lfloor\sqrt{s}\rfloor\}$ with $c+1$ divisible by $4(s-\lfloor s\rfloor^2)+3$. It follows that $c(t)=c$ for all $t\in\mathbb{Z}$. Set $b=s-c^2=s-\lfloor\sqrt{s}\rfloor^2$. Then $b\in\square$, $4b+3\mid c+1$, and $M(a,4b+3,c+1,t)\geqslant 0$ for all $t\in[-(s+1)^2,R(a,s+1)]$. If $t<-(s+1)^2$, then $t<-(\lfloor s\rfloor+1)^2\leqslant-(c+1)^2$ and hence $M(a,4b+3,c+1,t)\geqslant 0$. Note that

$$(1+(\lfloor\sqrt{s}\rfloor+1))^2\geqslant(1-\lfloor\sqrt{s}\rfloor+1)^2.$$

If $t>R(a,s+1)$, then $t>R(a,\lfloor s\rfloor+1)\geqslant R(a,c+1)$ and hence $M(a,4b+3,c+1,t)\geqslant 0$. As $b\in\square$ and $M(a,4b+3,c+1,t)\geqslant 0$ for all $t\in\mathbb{Z}$, we have $a\in A$. This concludes the proof of the claim.

Combining the proved claim with Lemma 4.1(iii) and (3.1), we get that A has a $\exists\forall\exists^4$-representation with $\forall$ bounded (or unbounded) over $\mathbb{Z}$.

By the proved claim, (3.2) and Lemma 4.1(ii), for any $a \geqslant 0$ we have

$$\begin{aligned}
&a \in A\\
\iff &\exists s\forall t\exists c(s-c^2\in\square\wedge(4(s-c^2)+3)\mid(c+1)\\
&\wedge\exists d\neq 0((4(c+1)^2(M(a,4(s-c^2)+3,c+1,t)+1)-2)d^2+1\in\square)\\
\iff &\exists s\forall t\exists c\exists d\neq 0\exists x(P(a,s,t,c,d,x)=0),
\end{aligned}$$

where P is a suitable polynomial with integer coefficients. It follows that

$$\begin{aligned}
a\in\bar{A}\iff &\forall s\exists t\forall c\forall d\neq 0\forall x(P(a,s,t,c,d,x)\neq 0)\\
\iff &\forall s\exists t\forall c\forall d\forall x\exists y\exists z(d(P(a,s,t,c,d,x)-(2y+1)(3z+1))=0)
\end{aligned}$$

with the aid of (3.3). So $\bar{A}$ has a $\forall\exists\forall^3\exists^2$-representation over $\mathbb{Z}$. This concludes our proof of Theorem 1.3. □

5. Proof of Theorem 1.4

Lemma 5.1 (Sun [23]). *There is a polynomial $P(x_1,\ldots,x_{2n+2})$ with integer coefficients such that for any $C_1,\ldots,C_n\in\mathbb{Z}$ we have*

$$\begin{aligned}
&C_1\geqslant 0\wedge\cdots\wedge C_n\geqslant 0\\
\iff &\exists x_1\cdots\exists x_{n+2}(P(C_1,\ldots,C_n,x_1,\ldots,x_{n+2})=0).
\end{aligned}$$

Lemma 5.2. *There are polynomials*

$P(x_1,\ldots,x_{2n+3})\in\mathbb{Z}[x_1,\ldots,x_{2n+3}]$ *and* $Q(x_1,\ldots,x_{2n+2})\in\mathbb{Z}[x_1,\ldots,x_{2n+2}]$ *such that for any $C_1,\ldots,C_n\in\mathbb{Z}$ we have*

$$\begin{aligned}
&C_1\geqslant 0\vee\ldots\vee C_n\geqslant 0\\
\iff &\forall x_1\ldots\forall x_n\forall x\exists y\exists z(P(C_1,\ldots,C_n,x_1,\ldots,x_n,x,y,z)=0),
\end{aligned}$$

and

$$\begin{aligned}
&C_1\geqslant 0\vee\ldots\vee C_n\geqslant 0\\
\iff &\forall x_1\in[0,D_1]\ldots\forall x_n\in[0,D_n]\exists y\exists z(Q(C_1,\ldots,C_n,x_1,\ldots,x_n,y,z)=0)
\end{aligned}$$

provided that $|C_i|\leqslant D_i$ with $D_i\in\mathbb{N}$ for all $i=1,\ldots,n$.

Proof. (i) For each $i=1,\ldots,n$, clearly

$$C_i<0\iff -C_i-1\geqslant 0\iff\exists x_i\neq 0(1-(4C_i+2)x_i^2\in\square).$$

Thus

$$\begin{aligned}
&\neg(C_1\geqslant 0\vee\cdots\vee C_n\geqslant 0)\\
\iff &C_1<0\wedge\cdots\wedge C_n<0\\
\iff &\exists x_1\neq 0(1-(4C_1+2)x_1^2\in\square)\wedge\cdots\wedge\exists x_n\neq 0(1-(4C_n+2)x_1^2\in\square)\\
\iff &\exists x_1\cdots\exists x_n(x_1\cdots x_n\neq 0\wedge(1-(4C_1+2)x_1^2\in\square)\\
&\wedge\cdots\wedge(1-(4C_n+2)x_n^2\in\square))\\
\iff &\exists x_1\cdots\exists x_n(x_1\cdots x_n\neq 0\\
&\wedge\exists x(J_n(1-(4C_1+2)x_1^2,\ldots,1-(4C_n+2)x_n^2,x)=0)
\end{aligned}$$

and hence

$$\begin{aligned}&C_1\geqslant 0\vee\cdots\vee C_n\geqslant 0\\\iff&\forall x_1\cdots\forall x_n\forall x\,(x_1\cdots x_n=0\\&\quad\vee J_n(1-(4C_1+2)x_1^2,\ldots,1-(4C_n+2)x_n^2,x)\neq 0)\\\iff&\forall x_1\cdots\forall x_n\forall x\exists y\exists z\,(x_1\cdots x_n\\&\quad\times(J_n(1-(4C_1+2)x_1^2,\ldots,1-(4C_n+2)x_n^2,x)-(2y+1)(3z+1))=0).\end{aligned}$$

(ii) We now prove the latter assertion in Lemma 5.2. Let $D_1,\ldots,D_n\in\mathbb{N}$ with $D_i\geqslant|C_i|$ for all $i=1,\ldots,n$. By Lemma 3.2,

$$C_i\geqslant 0\iff\forall x_i\in[0,D_i](x_i+C_i+1\neq 0).$$

Thus

$$\begin{aligned}&C_1\geqslant 0\vee\ldots\vee C_n\geqslant 0\\\iff&\forall x_1\in[0,D_1]\ldots\forall x_n\in[0,D_n](x_1+C_1+1\neq 0\vee\cdots\vee x_n+C_n+1\neq 0)\\\iff&\forall x_1\in[0,D_1]\ldots\forall x_n\in[0,D_n]\exists y\exists z\\&\quad((x_1+C_1+1)^2+\cdots+(x_n+C_n+1)^2=(2y+1)(3z+1)).\end{aligned}$$

This ends the proof. □

Lemma 5.3. *Let $k,m\in\mathbb{Z}$ with $k>0$, $2\mid k$ and $m\equiv 3\pmod 4$. Then there is a unique $b\in\mathbb{N}$ such that $|m-b^k|=\min_{x\in\mathbb{Z}}|m-x^k|$. Moreover, for $b\in\mathbb{Z}$ we have*

$$|m-b^k|=\min_{x\in\mathbb{Z}}|m-x^k|\iff|m-b^k|<|m-(b\pm 1)^k|.$$

Proof. If $a,b\in\mathbb{N}$ and $|m-a^k|=|m-b^k|$ but $a\neq b$, then $m-a^k=-(m-b^k)$ and hence $2m=a^k+b^k$, thus $a\equiv b\pmod 2$ and we get a contradiction since $2m$ is neither divisible by 4 nor congruent to 2 modulo 8. (Note that an odd square is congruent to 1 modulo 8.) So, there is a unique $b\in\mathbb{N}$ with $|m-b^k|=\min_{x\in\mathbb{Z}}|m-x^k|$.

If $b\in\mathbb{Z}$ and $|m-b^k|=\min_{x\in\mathbb{Z}}|m-x^k|$, then $|m-b^k|<|m-(b\pm1)^k|$ as $|b\pm1|\neq|b|$.

Suppose that $b\in\mathbb{Z}$ and $|m-b^k|<|m-(b\pm1)^k|$. If $b=0$, then $|m|\leqslant|m-1|$, hence $m\leqslant 0$ and

$$\min_{x\in\mathbb{Z}}|m-x^k|=\min_{x\in\mathbb{Z}}|-|m|-|x|^k|=|m|=|m-b^k|.$$

Now assume that $b\neq 0$. Then $|b|\pm1\geqslant 0$. Note that

$$|m-|b|^k|=|m-b^k|\leqslant|m-(|b|\pm1)^k|.$$

If $m\leqslant(|b|-1)^k$, then $m-|b|^k<m-(|b|-1)^k\leqslant 0$ and hence $|m-|b|^k|>|m-(|b|-1)^k|$ which leads to a contradiction. If $m\geqslant(|b|+1)^k$, then $m-|b|^k>m-(|b|+1)^k\geqslant 0$, which also leads to a contradiction. Therefore

$$(|b|-1)^k<m<(|b|+1)^k.$$

If $x \in \mathbb{Z}$ and $|x| = |b|$, then $|m - x^k| = |m - b^k|$ since k is even. For $x \in \mathbb{Z}$ with $|x| < |b|$, we have $m - x^k = m - |x|^k \geqslant m - (|b| - 1)^k > 0$ and hence

$$|m - x^k| \geqslant |m - (|b| - 1)^k| \geqslant |m - b^k|.$$

For $x \in \mathbb{Z}$ with $|x| > |b|$, we have $m - x^k = m - |x|^k \leqslant m - (|b| + 1)^k < 0$ and hence

$$|m - x^k| \geqslant |m - (|b| + 1)^k| \geqslant |m - b^k|.$$

So we have $|m - b^k| = \min_{x \in \mathbb{Z}} |m - x^k|$.

The proof of Lemma 5.3 is now complete. □

Proof of Theorem 1.4. Take polynomials R and M (depending on A) as in Theorem 2.4, and note that $S = \{(2x)^2 + 4 : \ x \in \mathbb{Z}\}$ is an infinite subset of $\mathbb{N}$. By Theorem 2.4, for any $a \in \mathbb{N}$ we have

$$b \in \mathbb{Z} \wedge c \in \mathbb{Z} \wedge (t < -c^2 \vee t > R(a, c) \Rightarrow M(a, b^2 + 4, c, t) \geqslant 0$$

and

$$\begin{aligned} a \in A &\iff \exists b \exists c \forall t (M(a, b^2 + 4, c, t) \geqslant 0) \\ &\iff \exists b \, (2 \mid b \wedge \exists c \forall t \, (M(a, b^2 + 4, c, t) \geqslant 0)). \end{aligned}$$

Moreover, if $a \in A$ then we may choose $b \geqslant 2$ and $0 < c < (b^2 + 4)^n$ with $(b^2 + 4) \mid c$ such that $M(a, b^2 + 4, c, t) \geqslant 0$ for all $t \in \mathbb{Z}$, where n is a positive integer only depending on A.

Note that $k = 4n$ is a positive even number. For $b, q \in \mathbb{Z}$ let

$$P^+(b, q) = (4q - 1 - (b + 1)^k)^2 - (4q - 1 - b^k)^2$$

and

$$P^-(b, q) = (4q - 1 - (b - 1)^k)^2 - (4q - 1 - b^k)^2.$$

By Lemma 5.3,

$$|4q - 1 - b^k| = \min_{x \in \mathbb{Z}} |4q - 1 - x^k| \iff P^+(b, q) > 0 \wedge P^-(b, q) > 0.$$

Let $a \in \mathbb{N}$. We claim that

$$\begin{aligned} a \in A &\iff \exists q \forall b \forall t (P^+(b, q) \leqslant 0 \vee P^-(b, q) \leqslant 0 \vee M(a, b^2 + 4, 4q - b^k, t) \geqslant 0) \\ &\iff \exists q \forall b \in [0, 8q^2 + 1] \forall t \in [-((4q - 1)^2 + 1)^2, R(a, (4q - 1)^2 + 1)] \\ &\qquad (P^+(b, q) \leqslant 0 \vee P^-(b, q) \leqslant 0 \vee M(a, b^2 + 4, 4q - b^k, t) \geqslant 0). \end{aligned}$$

Suppose that $a \in A$. Then there are $b_0, c \in \mathbb{Z}$ with

$$2 \mid b_0, \ b_0^2 + 4 \geqslant 6, \ (b_0^2 + 4) \mid c \text{ and } 0 < c < (b_0^2 + 4)^n$$

such that $M(a, b_0^2 + 4, c, t) \geqslant 0$ for all $t \in \mathbb{Z}$. As $4 \mid b_0^2$ and $4 \mid c$, $q = (b_0^k + c)/4$ is an integer. Let $m = 4q - 1$. Note that

$$0 \leqslant c - 1 < (b_0^2 + 4)^n \leqslant (2b_0^2)^n \leqslant |b_0|^{3n} \leqslant |b_0|^{4n-1},$$

$$2(c - 1) < 4n|b_0|^{4n-1} \leqslant (|b_0| + 1)^{4n} - |b_0|^{4n},$$

$$|m - b_0^{4n}| = c - 1 < (|b_0| + 1)^{4n} - (|b_0|^{4n} + c - 1) = -(m - (|b_0| + 1)^{4n}),$$

$$|m - b_0^{4n}| = c - 1 < c - 1 + |b_0|^{4n} - (|b_0| - 1)^{4n} = m - (|b_0| - 1)^{4n}.$$

Therefore $|m-b_0^k|<|m-(b_0\pm1)^k|$, hence $P^+(b_0,q)>0$ and $P^-(b_0,q)>0$. If $b\in\mathbb{Z}$ and $P^\pm(b,q)>0$, then $|m-b^k|=\min_{x\in\mathbb{Z}}|m-x^k|=|m-b_0^k|$ and hence $|b|=|b_0|$, thus $4q-b^k=b_0^k+c-b^k=c$ and

$$M(a,b^2+4,4q-b^k,t)=M(a,b^2+4,c,t)\geqslant 0$$

for all $t\in\mathbb{Z}$. So, for any $b\in\mathbb{Z}$ we have

$$P^+(b,q)\leqslant 0\vee P^-(b,q)\leqslant 0\vee\forall t(M(a,b^2+4,4q-b^k,t)\geqslant 0).$$

Now we prove another direction of the claim. Let $q\in\mathbb{Z}$ and assume that for any $b\in[0,8q^2+1]$ and $t\in[-((4q-1)^2+1)^2,R(a,(4q-1)^2+1)]$ we have

$$P^+(b,q)\leqslant 0\vee P^-(b,q)\leqslant 0\vee M(a,b^2+4,4q-b^k,t)\geqslant 0.$$

Take the unique $b\in\mathbb{N}$ with $|m-b^k|=\min_{x\in\mathbb{Z}}|m-x^k|$, where $m=4q-1$. Then $|m-b^k|<|m-(b\pm1)^k|$ and hence both $P^+(b,q)$ and $P^-(b,q)$ are positive. If $b\neq 0$, then $b^k-|m|\leqslant|b^k-m|<|0^k-m|=|m|$. No matter $b=0$ or not, we have $b^k\leqslant 2|m|-1$. Hence

$$0\leqslant b\leqslant 2|m|-1\leqslant 2(4|q|+1)-1\leqslant 8q^2+1.$$

If $t\in[-(m^2+1)^2,R(a,m^2+1)]$, then by the assumption we have $M(a,b^2+4,c,t)\geqslant 0$, where $c=4q-b^k$. Note that

$$|c|=|m+1-b^k|\leqslant|m-b^k|+1\leqslant|m-0^k|+1\leqslant m^2+1$$

and hence $|1+c|\leqslant 1+|c|\leqslant 1+(m^2+1)$. If $t<-(m^2+1)^2$ or $t>R(a,m^2+1)$, then $t<-c^2$ or $t>R(a,c)$, and hence $M(a,b^2+4,c,t)\geqslant 0$. So $M(a,b^2+4,c,t)\geqslant 0$ for all $t\in\mathbb{Z}$, and hence $a\in A$. This concludes the proof of the claim.

By the proved claim, for any $a\in\mathbb{N}$ we have

$$\begin{aligned}&a\in A\\ \iff&\exists q\forall b\forall t\,(-P^+(b,q)\geqslant 0\vee -P^-(b,q)\geqslant 0\vee M(a,b^2+4,4q-b^k,t)\geqslant 0)\\ \iff&\exists q\forall b\in[0,8q^2+1]\forall t\in[-((4q-1)^2+1)^2,R(a,(4q-1)^2+1)]\\&(-P^+(b,q)\geqslant 0\vee -P^-(b,q)\geqslant 0\vee M(a,b^2+4,4q-b^k,t)\geqslant 0).\end{aligned}$$

Clearly $|P^\pm(b,q)|\leqslant P_0(q)^2$ for all $b\in[0,8q^2+1]$, and

$$|M(a,b^2+4,4q-b^k,t)|\leqslant M_0(a,q)^2$$

for all $b\in[0,8q^2+1]$ and $t\in[-((4q-1)^2+1)^2,R(a,(4q-1)^2+1)]$, where P_0 and M_0 are suitable polynomials with integer coefficients.

Combining the last paragraph with Lemma 3.2(i), we find that A has a $\exists\forall^2\exists^3$-representation over $\mathbb{Z}$ and also a $\exists\forall^2\exists^3$-representation over $\mathbb{Z}$ with $\forall$ bounded. Combining the last paragraph with Lemma 5.2, we see that that A has a $\exists\forall^6\exists^2$-representation over $\mathbb{Z}$, and also a $\exists\forall^5\exists^2$-representation over $\mathbb{Z}$ with $\forall$ bounded.

Note that

$$a \in \bar{A} = \mathbb{N} \setminus A \iff \forall q \exists b \exists t\, (P^+(b,q) - 1 \geqslant 0 \wedge P^-(b,q) - 1 \geqslant 0 \\ \wedge -M(a, b^2+4, 4q - b^k, t) - 1 \geqslant 0).$$

Combining this with Lemma 3.2(i), we get that $\bar{A}$ has a $\forall\exists^2\forall^2\exists^2$-representation over $\mathbb{Z}$; if we apply Lemma 5.1, then we find that $\bar{A}$ has a $\forall\exists^7$-representation over $\mathbb{Z}$.

The proof of Theorem 1.4 is now complete. □

Acknowledgment. The author would like to thank the referee for helpful comments.

References

[1] N. Cutland, Computability, Cambridge Univ. Press, Cambridge, 1980.

[2] N. Daans, *Universally defining $\mathbb{Z}$ in $\mathbb{Q}$ with 10 quantifiers*, J. London Math. Soc. **109** (2024), Article ID e12864.

[3] M. Davis, *Arithmetical problems and recursively enumenrable predicates*, J. Symblic Logc **18** (1953), 33–41.

[4] M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269.

[5] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. **74(2)** (1961), 425–436.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, Grad. Texts. Math., vol. 84, Springer, New York, 1990.

[7] J. P. Jone, *Classification of quantifier prefixes over Diophantine equations*, Z. Math. Logik Grundlag. Math. **27** (1981), 403–410.

[8] J. P. Jones, *Universal Diophantine equation*, J. Symbolic Logic **47** (1982), 549–571.

[9] Y. Matiyasevich, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282; English translation with addendum, Soviet Math. Doklady **11** (1970), 354–357.

[10] Y. Matiyasevich, *On recursively unsolvability of Hilbert's tenth problem*, in: Logic, Methodology and Philosophy of Science, IV (Bucharest, 1971), Studies in Logic and Foundations of Math., Vol. 74, North-Holland, Amsterdam, 1973, 89–110.

[11] Y. Matiyasevich, *Arithmetical representation of enumerable sets with a small number of quantifiers*, J. Soviet Math. **6** (1976), 410–416.

[12] Y. Matiyasevich, *Some purely mathematical results inspired by mathematical logic*, in: Logic, Foundations of Mathematics and Computability Theory (London, Ont., 1975). Reidel, Dordrecht, 1977, Part I, 121–127.

[13] Y. Matiyasevich, Hilbert's Tenth Problem, MIT Press, Cambridge, Massachusetts, 1993.

[14] Y. Matiyasevich and J. Robinson, *Two universal 3-quantifier representations of r.e. sets*, in: Teoriya Algorifmov i Matematicheskaya Logika (a collection of papers dedicated to A. A. Markov), Vychislitel'nyi Tsentr Akademii Nauk SSSR, Moscow, 1974, pages 112–123.

[15] Y. Matiyasevich and J. Robinson, *Reduction of an arbitrary diophantine equation to one in 13 unknowns*, Acta Arith. **27** (1975), 521–553.

[16] Y. Matiyasevich and Z.-W. Sun, *On Diophantine equations over $\mathbb{Z}[i]$ with 52 unknowns*, arXiv:2002.12136, 2020.

[17] A. B. Matos, L. Paolini and L. Roversi, *The fixed point problem of a simple reversible language*, Theoret. Comput. Sci. **813** (2020), 143–154.

[18] B.-K. Oh and Z.-W. Sun, *Mixed sums of squares and triangular numbers*, J. Number Theory **129** (2009), 964–969.

[19] J. Richter-Gebert and U. H. Kortenkamp, *Complexity issues in dynamic geometry*, in: Foundations of Computational Mathematics (Hong Kong, 2000), , World Sci. Publ., River Edge, NJ, 2002, 355–404.
[20] J. M. Rojas, *Uncomputably large integral points on algebraic plane curves*? Theoret. Comput. Sci. **235** (2000), 145–162.
[21] A. Shlapentokh, Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields. New Mathematical Monographs, Vol. 7, Cambridge Univ. Press, Cambridge, 2007.
[22] Z.-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Ser. A **35** (1992), 257–269. Available from `http://maths.nju.edu.cn/~zwsun/12d.pdf`
[23] Z.-W. Sun, *A new relation-combining theorem and its application*, Z. Math. Logik Grundlag. Math. **38** (1992), 209–212.
[24] Z.-W. Sun, *Further results on Hilbert's Tenth Problem*, Sci. China Math. **64** (2021), 281–306.
[25] Z.-W. Sun, Fibonacci Numbers and Hilbert's Tenth Problem (in Chinese), Harbin Institute of Technology Press, Harbin, 2024.
[26] S. P. Tung, *On weak number theories*, Japan. J. Math. (N.S.) **11** (1985), 203–232.
[27] S. P. Tung, *Computational complexities of Diophantine equations with parameters*, J. Algorithms **8** (1987), 324–336.
[28] G.-R. Zhang and Z.-W. Sun, $\mathbb{Q}\setminus\mathbb{Z}$ *is diophantine over* $\mathbb{Q}$ *with* 32 *unknowns*, Pol. Acad. Sci. Math. **70** (2022), 93–106.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: `zwsun@nju.edu.cn`