A talk given at Hebei Noraml Univ. (May 15, 2017)
and Macau University of Science and Technology (July 17, 2017)
and Xiamen University (Jan. 15, 2018)

On Hilbert's Tenth Problem

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Jan. 15, 2018

Abstract

Hilbert's Tenth Problem (HTP) asks for an effective algorithm to test whether an arbitrary polynomial equation

$$P(x_1, \ldots, x_n) = 0$$

(with integer coefficients) has solutions over the ring of integers. This was finally solved by Matiyasevich in 1970 negatively.

In this talk we review the historical developments towards the solution of HTP as well as some related tools including coding ideas and Lucas sequences. We will also introduce some further results after the solution of HTP; for example, the speaker has shown that there is no algorithm to decide whether an arbitrary polynomial equation $P(x_1, \ldots, x_{11}) = 0$ (with integer coefficients and 11 unknowns) has integral solutions or not.

Part I. The meaning of Hilbert's Tenth Problem

Hilbert's Tenth Problem

In 1900, at the Paris conference of ICM, D. Hilbert presented 23 famous mathematical problems. He formulated his tenth problem as follows:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: `To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.`

In modern language, Hilbert's Tenth Problem (HTP) asked 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.

However, at that time the exact meaning of algorithm was not known.

Primitive recursive functions

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and call each $n \in \mathbb{N}$ a *natural number*.

Three Basic Functions:

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

Successor Function: $S(x) = x + 1$.

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

Composition:

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

Primitive Recursion:

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

Primitive recursive functions are the basic functions and those obtained from the basic functions by applying composition and primitive recursion a finite number of times.

Acknermann's function

It is easy to see that all primitive recursive functions are computable by our intuition.

Skolem's Claim (1924): All *intuitively computable* number-theoretic functions are primitive recursive functions.

In 1928 Ackermann showed that the following **Ackermann function** $A(m, n)$ is computable but not primitively recursive.

$$\begin{aligned} A(0, n) &= n + 1, \\ A(m + 1, 0) &= A(m, 1) \\ A(m + 1, n + 1) &= A(m, A(m + 1, n)). \end{aligned}$$

For example,

$$\begin{aligned} A(1, 2) &= A(0, A(1, 1)) = A(0, A(0, A(1, 0))) \\ &= A(0, A(0, A(0, 1))) = A(0, A(0, 2)) \\ &= A(0, 3) = 4. \end{aligned}$$

Partial recursive functions

μ-operator:

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

means that $f(x_1, \ldots, x_n)$ is the least natural number y such that $g(x_1, \ldots, x_n, y) = 0$. 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.

Partial recursive functions are the basic functions and those obtained from the basic functions by applying composition and μ-operator a finite number of times.

If a partial recursive function $f(x_1, \ldots, x_n)$ is defined for all $x_1, \ldots, x_n \in \mathbb{N}$, then f is called a *total recursive function*.

All primitive functions as well as the Ackermann function $A(m, n)$ are total recursive functions.

Church's Thesis

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.

In 1936 A. Turing introduced the notion of Turing machine which is an abstract machine that manipulates symbols on a strip of tape according to a table of rules (i.e., a program). 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 outut if $f(x_1, \ldots, x_n)$ is defined, and never stops if $f(x_1, \ldots, x_n)$ is undefined.

Partial recursive functions and Turing computable functions were proved to be equivalent.

Church's Thesis (1936). If a function f into $\mathbb{N}$ with natural number variables is effectively computable by intuition, then it must be a partial recursive function (or a Turing computable function).

Recursively enumerable sets

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

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

is a partial recursive function.

If A is an r.e. set containing an element a, and the program P computes the above function f, then the function

$$g(x, y) = \begin{cases} x & \text{if the program } P \text{ computes } f(x) \text{ within } y \text{ steps}, \\ a & \text{otherwise} \end{cases}$$

is a partial recursive function with $\mathrm{Ran}(g) = A$.

If A is the range of a partial recursive function $h(x_1, \ldots, x_n)$, then the function

$$f(x) = \begin{cases} 1 & \text{if } x \in \mathrm{Ran}(h) = A, \\ \text{undefined} & \text{otherwise}, \end{cases}$$

is a partial recursive function, and thus A is an r.e. set.

r.e. sets and recursive sets

Thus $A \subseteq \mathbb{N}$ is an r.e. set if and only if A is the empty set or the range of a partial recursive function.

Enumeration Theorem. There is a partial recursive function $\varphi(m, n)$ such that

$$\varphi_0, \varphi_1, \varphi_2, \ldots$$

list all the partial recursive functions of one variable. where φ_m is given by

$$\varphi_m(n) = \varphi(m, n) \ (n = 0, 1, 2, \ldots).$$

A problem or a set is *decidable* or *recursive*, if and only if its characteristic function is Turing computable (or recursive).

A set $A \subseteq \mathbb{N}$ is recursive if and only if both A and $\mathbb{N} \setminus A$ are r.e. sets.

Halting Problem is undecidable

Theorem. The set $K = \{x \in \mathbb{N} : \ x \in \mathrm{Dom}(\varphi_x)\}$ is a nonrecursive r.e. set.

Proof. As the function $\varphi_x(x) = \varphi(x, x)$ is a partial recursive function, we see that K is an r.e. set.

Suppose that K is recursive. Then the function

$$f(x) = \begin{cases} \varphi_x(x) + 1 & \text{if } x \in \mathrm{Dom}(\varphi_x), \\ 0 & \text{otherwise,} \end{cases}$$

is totally recursive, thus for some $m \in \mathbb{N}$ we have $\varphi_m = f$ and hence

$$f(m) = \varphi_m(m) \neq \varphi_m(m) + 1$$

which leads a contradiction.

Let P_x be a Turing program computing φ_x. Whether a Turing machine with input x and program P_x finally stops, is an undecidable problem which is called the halting problem.

Part II. Solution to Hilbert's Tenth Problem

Diophantine equations over $\mathbb{N}$ and $\mathbb{Z}$

Throughout this talk, variables always range over $\mathbb{Z}$.

Let $P(z_1, \ldots, z_n) \in \mathbb{Z}[z_1, \ldots, z_n]$. Then

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

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

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

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 $x_1, \ldots, x_n \in \mathbb{N}$?*

Diophantine relations and Diophantine sets

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 is an r.e. set.

Davis Daring Hypothesis

In 1944 E. L. Post thought that HTP *begs for an unsolvability proof*, i.e., HTP might be undecidable.

In 1949 Martin Davis used Gödel's coding idea to obtain that any r.e. set $A \subseteq \mathbb{N}$ has the following Davis normal form

$$a \in A \iff \exists x \geqslant 0 \forall 0 \leqslant y \leqslant x \exists z_1 \geqslant 0 \ldots \exists z_n \geqslant 0 \\ [P(a, x, y, z_1, \ldots, z_n) = 0],$$

where a is a natural number and P is a polynomial with integer coefficients.

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

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

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

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

Eliminate bounded universal quantifier

Theorem (M. Davis, H. Putnam and J. Robinson [Annals of Math. 1961]) Let $b \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, $P(y, x_1, \ldots, x_m) \in \mathbb{Z}[y, x_1, \ldots, x_m]$, and $B(b, w) = P^*(b, w, \ldots, w)$ with $P^*(y, x_1, \ldots, x_m)$ obtained by replacing each coefficient in $P(y, x_1, \ldots, x_m)$ by its absolute value. Then

$$\forall 0 \leqslant y < b \exists x_1 \geqslant 0 \ldots \exists x_m \geqslant 0 [P(y, x_1, \ldots, x_m) = 0]$$

$\Longleftrightarrow$ there exist $q, w, z_1, \ldots, z_m \in \mathbb{N}$ such that

$$q \equiv -1 \pmod{b!(b + w + B(b, w))!}, \text{ and}$$

$$\binom{q}{b} \text{ divides } \binom{z_1}{w}, \ldots \binom{z_m}{w} \text{ and } P(q, z_1, \ldots, z_m).$$

Remark. A system of finitely many Diophantine equations is equivalent to a single Diophantine equation. 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

$$P_1(z_1, \ldots, z_n) = 0 \ \& \ \ldots \ \& \ P_k(z_1, \ldots, z_n) = 0$$

$$\Longleftrightarrow P_1^2(z_1, \ldots, z_n) + \ldots + P_k^2(z_1, \ldots, z_n) = 0.$$

A Lemma

Lemma. Let $b, w \in \mathbb{Z}^+$. Suppose that $q \in \mathbb{N}$, $q \equiv -1 \pmod{b!(b+w+B(b,w))!}$ and

$$q_y = \frac{q+1}{y+1} - 1 = \frac{q-y}{y+1} \quad \text{for } y = 0, 1, \ldots, b-1.$$

Then $q_0, \ldots, q_{b-1}, w!$ are pairwise coprime, and $\prod_{y=0}^{b-1} q_y = \binom{q}{b}$.

Proof. It is easy to verify the last equality. Let $y \in \{0, \ldots, b-1\}$. As $(b!)^2 \mid q+1$, for any prime $p \leqslant b$ we have

$$q_y = b! \frac{b!}{y+1} \cdot \frac{q+1}{(b!)^2} - 1 \equiv -1 \not\equiv 0 \pmod{p}.$$

If p is a common prime divisor of q_y and $w!$, then p divides $q+1-(q-y) = y+1$, hence $p \leqslant b$ and $p \nmid q_y$ which leads a contradiction. So p_y is coprime to $w!$. If $y' \in \{0, \ldots, b-1\}$ with $y' \neq y$, and p is a prime dividing q_y and $q_{y'}$, then p divides $q-y-(q-y') = y'-y$, hence $p \leqslant b$ and $p \nmid q_y$, which leads a contradiction. So, $q_0, \ldots, q_{b-1}$ are pairwise coprime.

Proof of the Theorem

$\Rightarrow$: For each $y = 0, \ldots, b-1$ there are $x_{1,y}, \ldots, x_{m,y} \in \mathbb{N}$ with $P(y, x_{1,y}, \ldots, x_{m,y}) = 0$. Take a positive integer $w > \max\{x_{i,y} : \ 1 \leqslant i \leqslant m \ \& \ 0 \leqslant y < b\}$. Then

$$|P(y, x_{1,y}, \ldots, x_{m,y})| \leqslant B(b, w) \quad \text{for all } y = 0, \ldots, b-1.$$

Choose $q \in \mathbb{N}$ and define q_y for $0 \leqslant y < b$ as in the Lemma. Then $q_0, \ldots, q_{b-1}, w!$ are pairwise coprime by the Lemma.

By the Chinese Remainder Theorem, for each $i = 1, \ldots, m$ there is an integer $z_i \geqslant 0$ such that

$$z_i \equiv x_{i,y} \pmod{q_y} \quad \text{for all } y = 0, \ldots, b-1.$$

Thus

$$P(q, z_1, \ldots, z_m) \equiv P(y, x_{1,y}, \ldots, x_{m,y}) = 0 \pmod{q_y}$$

for all $y = 0, \ldots, b-1$, and hence $\binom{q}{b} = \prod_{y=0}^{b-1} q_y$ divides $P(q, z_1, \ldots, z_m)$. As $0 \leqslant x_{i,y} < w$ for each $0 \leqslant y < b$, q_y divides $\prod_{k=0}^{w-1}(z_i - k) = w!\binom{z_i}{w}$ and hence $q_y \mid \binom{z_i}{w}$. Thus $\binom{q}{b} = \prod_{y=0}^{b-1} q_y$ divides $\binom{z_i}{w}$.

Proof of the Theorem

$\Leftarrow$: For each $y = 0, \ldots, b-1$ define q_y as in the Lemma. By the Lemma, $q_0, \ldots, q_{b-1}, w!$ are pairwise coprime. Let p_y be a prime divisor of q_y. Then

$$p_y \mid q_y \mid \binom{q}{b} \mid \binom{z_i}{w},$$

and hence $p_y \mid z_i - x_{i,y}$ for some $0 \leqslant x_{i,y} < w$.

Let $0 \leqslant y < b$. If $p_y \leqslant B(b, w)$, then p_y divides $q + 1 - (q - y) = y + 1$, hence $p_y \leqslant b$ and $p_y \nmid q_y$ which leads a contradiction. Thus $p_y > B(b, w)$. As $p_y \mid q_y \mid q - y$ and $p_y \mid q_y \mid \binom{q}{b}$, we have

$$P(y, x_{1,y}, \ldots, x_{m,y}) \equiv P(q, z_1, \ldots, z_m) \equiv 0 \pmod{p_y}.$$

Since

$$|P(y, x_{1,y}, \ldots, x_{m,y})| \leqslant B(b, w) < p_y,$$

we obtain $P(y, x_{1,y}, \ldots, x_{m,y}) = 0$.

$z = \binom{n}{k}$ is exponential Diophantine

If $0 < k \leqslant n$ and $u > 2^n$, then

$$\frac{(u+1)^n}{u^k} = \binom{n}{k} + u \sum_{k<m\leqslant n} \binom{n}{m} u^{m-k-1} + \sum_{0\leqslant i<k} \binom{n}{i} \frac{u^i}{u^k}$$

by the binomial theorem, hence

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv \binom{n}{k} \pmod{u}$$

and thus $\binom{n}{k}$ is the least nonnegative residue of $\lfloor (u+1)^n / u^k \rfloor$ modulo u.

For $z \geqslant 0$ and $n \geqslant k > 0$, the relation $z = \binom{n}{k}$ holds if and only if there are $u, v, w, x, y \in \mathbb{N}$ such that

$$u > v,\ v = 2^n,\ z \equiv w \pmod{u},\ z < u,$$
$$x = (u+1)^n,\ y = u^k,\ yw \leqslant x < (w+1)y.$$

$z = n!$ is exponential Diophantine

If $n > 0$ and $m > (2n)^{n+1}$, then

$$n! < \frac{m^n}{\binom{m}{n}} = \frac{n!}{\prod_{r=1}^{n-1}(1 - r/m)} < \frac{n!}{(1 - n/m)^n} < n! \left(1 + \frac{2n}{m}\right)^n < n!+1$$

and thus $n! = \lfloor m^n / \binom{m}{n} \rfloor$.

For $z \geqslant 0$ and $n > 0$, the relation $z = n!$ holds if and only if there are $u, v, w, x, y \in \mathbb{N}$ such that

$$u > v,\ v = w^{n+1},\ w = 2n,\ x = u^n,\ y = \binom{u}{n},\ yz \leqslant x < (z+1)y.$$

Therefore, $z = n!$ is exponential Diophantine!

The Davis-Putnam-Robinson Theorem

Theorem (M. Davis, H. Putnam, J. Robinson, Annals of Math. 1961) 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 $\mathbb{N}$.

Proof. An r.e. set is either empty or the range of a partial recursive function.

For any $a \in \mathbb{N}$, clearly $a \in \emptyset \iff \exists x \geqslant 0(a = x)$. So it suffices to show that for any partial recursive function $f(x_1, \ldots, x_n)$ the relation $f(x_1, \ldots, x_n) = y$ with $x_1, \ldots, x_n, y \geqslant 0$ is exponential Diophantine.

$$y = O(x) \iff y = 0 \iff \exists z \geqslant 0(y(z+1) = 0),$$

$$y = S(x) \iff y = x + 1 \iff \exists z \geqslant 0((y - x - 1)(z + 1) = 0),$$

$$y = I_{nk}(x_1, \ldots, x_n) \iff y = x_k \iff \exists z \geqslant 0((y - x_k)(z+1) = 0).$$

Proof of the Davis-Putnam-Robinson Theorem

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

$$y = f(x_1, \ldots, x_n) \iff \exists t_1 \geqslant 0 \ldots \exists t_m \geqslant 0[y = g(t_1, \ldots, t_m) \text{ and } t_i = h_i(x_1, \ldots, x_n) \text{ for } i = 1, \ldots, m].$$

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

$$y = f(x_1, \ldots, x_n) \iff g(x_1, \ldots, x_n, y) = 0 \text{ and } \forall 0 \leqslant s < y \exists t \geqslant 0[g(x_1, \ldots, x_n, s) = t + 1]$$

In view of the above, with the help of the Theorem eliminating bounded universal quantifier, any r.e. set is exponential Diophantine. As the r.e. set K is not recursive, there is no effective algorithm to decide an arbitrary exponential Diophantine equation over $\mathbb{N}$ is solvable or not.

Julia Robinson's Hypothesis

A. Tarski conjectured in 1948 that $\{2^n : \ n \in \mathbb{N}\}$ is not a Diophantine set. His PhD student J. Robinson did not succeed in proving this with serious efforts.

JR Hypothesis (J. Robinson, 1950). There is a Diophantine relation $R(a, b)$ with $a, b \in \mathbb{N}$ such that

$$R(a, b) \Rightarrow b < a^a$$

and

$$\forall k > 0 \exists a \geqslant 0 \exists b \geqslant 0 [R(a, b) \ \& \ a^k < b].$$

Under this hypothesis, J. Robinson showed that the exponential relation $a^b = c$ is Diophantine and hence all r.e. sets are Diophantine. So, the JR Hypothesis implies the negative solution of HTP.

J. Robinson tried to prove her JR Hypothesis but got no success. This made her depressed and doubt her Hypothesis.

Davis' approach

In 1968 M. Davis showed that if the equation

$$9(u^2+7v^2)^2-7(x^2+7y^2)^2=2\ (u,v,x,y\in\mathbb{N})$$

only has finitely many solutions then the relation $a^b=c$ is Diophantine.

In 1972, Shanks found the first nontrivial solution of the equation with

$$u=525692038369576,\ v=155632703919101 3,$$
$$x=2484616164142152,\ y=1381783865776981.$$

Up to now, nobody can show that the Diophantine equation

$$9(u^2+7v^2)^2-7(x^2+7y^2)^2=2\ (u,v,x,y\in\mathbb{N})$$

only has finitely many solutions.

Matiyasevich's Theorem

Recall that the Fibonacci sequence $(F_n)_{n\geqslant 0}$ defined by

$$F_0 = 0,\ F_1 = 1,\ \text{ and } F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots)$$

increases exponentially.
In 1970 Yu. Matiyasevich, a 23-year-old Russian, confirmed the JR Hypothesis by showing that the relation $y = F_{2x}$ (with $x, y \in \mathbb{N}$) is Diophantine! It follows the exponential relation $a^b = c$ (with $a, b, c \in \mathbb{N}$, $a > 1$ and $c > 0$) is Diophantine, i.e. there exists a polynomial $P(a, b, c, x_1, \ldots, x_n)$ with integer coefficients such that

$$a^b = c \iff \exists x_1 \geqslant 0 \ldots \exists x_n \geqslant 0[P(a, b, c, x_1, \ldots, x_n) = 0].$$

This, together with the Davis-Putnam-Robinson work in 1961, led Matiyasevich finally confirm Davis Daring Hypothesis.

Matiyasevich's Theorem (or MDPR Theorem) (1970).
Recursively enumerable sets coincide with Diophantine sets. Thus HTP has a negative solution!

Part III. Reduction of Natural Number Unknowns

Small ν with $\exists^\nu$ over $\mathbb{N}$ undecidable

For a set $S \subseteq \mathbb{Z}$ we let $\exists^n$ over S denote the set of formulas

$$\exists x_1 \in S \ldots \exists x_n \in S[P(x_1, \ldots, x_n) = 0]$$

with $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$.

Any nonrecursive r.e. set A has a Diophantine representation:

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

It is interesting to find the least $\nu \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ such that $\exists^\nu$ over $\mathbb{N}$ is undecidable.

$\nu < 200$ (Matiyasevich, Summer of 1970)
$\nu \leqslant 35$ (J. Robinson, 1970)
$\nu \leqslant 24$ (Matiyasevich and Robinson, 1970)
$\nu \leqslant 14$ (Matiyasevich and Robinson, 1970)
$\nu \leqslant 13$ (Matiyasevich and Robinson, 1973 [Acta Arith. 27(1975)])
$\nu \leqslant 9$ (Matiyasevich, 1975; details in Jones [J. Symbolic Logic, 1982])

Matiyasevich-Robinson's Relation-Combining Theorem

Matiyasevich-Robinson's Relation-Combining Theorem [Acta Arith. 27(1975)] Let $A_1, \ldots, A_k$ and R, S, T be integers with $S \neq 0$. Then

$$A_1 \in \square \wedge \ldots \wedge A_k \in \square \wedge S \mid T \wedge R > 0$$
$$\iff \exists n \geqslant 0[M_k(A_1, \ldots, A_k, S, T, R, n) = 0],$$

where

$$M_k(x_1, \ldots, x_k, w, x, y, z)$$
$$= \prod_{\varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}} \left(x^2 + w^2 z - w^2(2y-1)\left(x^2 + X^k + \sum_{j=1}^{k} \varepsilon_j \sqrt{x_j} X^{j-1} \right) \right)$$
$$= (w^2(1-2y))^{2^k} J_k\left(x_1, \ldots, x_k, x^2 + X^k + \frac{x^2 + w^2 z}{w^2(1-2y)} \right)$$

with $X = 1 + \sum_{j=1}^{k} x_j^2$, and $J_k(x_1, \ldots, x_k, x)$ being

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

Coding idea of Matiyasevich and Robinson (1975)

Let $b \in \mathbb{N}$, $\delta \in \mathbb{Z}^+$, and

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

$$B = 2\delta!(1 + b^\delta)\left(1 + \sum_{i_0 + \ldots + i_\nu \leqslant \delta} a_{i_0, \ldots, i_\nu}^2\right) + 1,$$

$$D(x) = x^{(\delta+1)^{\nu+2}} + \sum_{i_0 + \ldots + i_\nu \leqslant \delta} c_{i_0, \ldots, i_\nu} a_{i_0, \ldots, i_\nu} x^{(\delta+1)^{\nu+1} - \sum_{s=0}^{\nu} i_s (\delta+1)^s}$$

with $c_{i_0, \ldots, i_\nu} = i_0! \ldots i_\nu! (\delta - i_0 - \ldots - i_\nu)!$. Then

$P(z_0, \ldots, z_\nu) = 0$ for some $z_0, \ldots, z_\nu \in [0, b]$

$\Longleftrightarrow$ there is a number c of the form $1 + \sum_{i=0}^{\nu} c_i B^{(\delta+1)^i}$ with $c_i \in [0, b]$

such that the coefficient of $x^{(\delta+1)^{\nu+1}}$ in $\left(1 + \sum_{i=0}^{\nu} c_i x^{(\delta+1)^i}\right)^\delta D(x)$

is zero.

Matiyasevich's idea to use binary representations

For $a, b \in \mathbb{N}$ written in base p with p prime, let $\tau_p(a, b)$ denote the number of carries occurring in the addition of a and b. Kummer noted that $\tau_p(a, b) = \operatorname{ord}_p\binom{a+b}{a}$.

Let $b, B \in 2\uparrow = \{2^n : \ n \in \mathbb{N}\}$ with $b \leqslant B$. Let $\delta, \nu \in \mathbb{Z}^+$. For $c = \sum_{j=0}^{(\delta+1)^\nu} c_j B^j$ with $c_j \in [0, B)$, and $M = \sum_{j=0}^{(\delta+1)^\nu} m_j B^j$ with

$$m_j = \begin{cases} B - b & \text{if } j = (\delta+1)^s \text{ for some } s = 1, \ldots, k, \\ B - 1 & \text{otherwise,} \end{cases}$$

$$\tau_2(c, M) = 0 \iff \tau_2(c_j, m_j) = 0 \text{ for all } j = 0, \ldots, (\delta+1)^\nu$$

$$\iff c = \sum_{i=1}^{\nu} z_i B^{(\delta+1)^i} \text{ for some } z_1, \ldots, z_k \in [0, b)$$

If $N \in 2\uparrow$ and $S, T \in [0, N)$, then

$$\tau_2(S, T) = 0 \iff N^2 \mid \binom{2R}{R}$$

where $R = (N-1)((S+T+1)N + T + 1)$.

The 9 Unknowns Theorem

The above ideas, together with some other works in the 1975 paper of Matiyasevich and Robinson, led Mtijasevich obtain the following celebrated theorem.

Matiyasevich's 9 Unknowns Theorem: $\exists^9$ over $\mathbb{N}$ is undecidable!

The detailed proof of this theorem appeared in Jones [J. Symbolic Logic, 1982].

Up to now, no one has shown that $\exists^\nu$ over $\mathbb{N}$ is undecidable for some $\nu < 9$, although A.Baker, Matiyasevich and Robinson all believed that $\exists^3$ over $\mathbb{N}$ might be undecidable.

Part IV. Find small ν with $\exists^\nu$ over $\mathbb{Z}$ undecidable

$\exists$ over $\mathbb{Z}$ is decidable

Matiyasevich and Robinson [Acta Arith. 27(1975)]: 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

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

and hence

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

Thus $\exists$ over $\mathbb{N}$ and $\exists$ over $\mathbb{Z}$ are decidable (in polynomial time).

It is not known whether $\exists^2$ over $\mathbb{Z}$ is decidable. But A. Baker proved in 1968 that if $P(x, y) \in \mathbb{Z}[x, y]$ is homogenous, irreducible and of degree at least three then for any $m \in \mathbb{Z}$ there is an effective algorithm to determine whether $P(x, y) = m$ for some $x, y \in \mathbb{Z}$.

Relative results

For any $m \in \mathbb{Z}$, by Lagrange's four-square theorem

$$m \geqslant 0 \iff \exists z_1 \exists z_2 \exists z_3 \exists z_4 [m = z_1^2 + z_2^2 + z_3^2 + z_4^2].$$

Thus

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{4n} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

By the Gauss-Legendre theorem on sums of three squares,

$$\mathbb{N} \setminus \{x^2 + y^2 + z^2 : \ x, y, z \in \mathbb{Z}\} = \{4^k(8l + 7) : \ k, l \in \mathbb{N}\}.$$

If $n \in \mathbb{N}$, then $4n + 1 = (2x)^2 + (2y)^2 + (2z + 1)^2$ for some $x, y, z \in \mathbb{Z}$, and hence $n = x^2 + y^2 + z^2 + z$. Thus, for any $m \in \mathbb{Z}$,

$$m \geqslant 0 \iff \exists x \exists y \exists z [m = x^2 + y^2 + z^2 + z].$$

It follows that

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{3n} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

Thus $\exists^{27}$ over $\mathbb{Z}$ is undecidable by the 9 unknowns theorem, as pointed out by S.P. Tung in [Japan J. Math., 11(1985)].

A new relation-combining theorem

Tung (1985) asked whether $\exists^\nu$ over $\mathbb{Z}$ is undecidable for some $\nu < 27$.

New Relation-Combining Theorem (Z.-W. Sun [Z. Math. Logik Grundlag. Math. 38(1992)]): Let $A_1, \ldots, A_k, B, C_1, \ldots, C_n, D, E$ be integers with $D \neq 0$. Then

$$\begin{aligned} & A_1, \ldots, A_k \in \square \wedge B \neq 0 \wedge C_1, \ldots, C_n \geqslant 0 \wedge D \mid E \\ \Longleftrightarrow\ & \exists z_1 \ldots \exists z_{n+2} [P(A_1, \ldots, A_k, B, C_1, \ldots, C_n, D, E, z_1, \ldots, z_{n+2}) = 0], \end{aligned}$$

where P is a suitable polynomial with integer coefficients.

This implies that

$$\exists^n \text{ over } \mathbb{N} \text{ is undecidable} \Rightarrow \exists^{2n+2} \text{ over } \mathbb{Z} \text{ is undecidable.}$$

So $\exists^{20}$ over $\mathbb{Z}$ is undecidable by the 9 unknowns theorem.

$\exists^{11}$ over $\mathbb{Z}$ is undecidable

In 1992, I announced that $\exists^{11}$ **over** $\mathbb{Z}$ **is undecidable**.

To achieve this goal, unlike others I did not simply use the relative result, instead I adapt the deep proof of the 9 unknowns theorem and made suitable variants so that we can use integer variables instead of natural number variables.

My starting point is the use of Lucas sequences with integer indices instead of the usual natural number indices. I published this initial step in Sci. China Ser. A 35(1992).

The whole proof of the undecidability of $\exists^{11}$ over $\mathbb{Z}$ is very sophisticated. It appeared in my PhD thesis in 1992. During 1992-2016, despite that many mathematicians wanted to see my detailed proof, I did not write an English version of that, since I was frequently busy with my new discoveries.

After 25 years have passed, I finally spent time to write an English paper which contains the undecidability of $\exists^{11}$ over $\mathbb{Z}$ as well as my new discoveries related to HTP. The preprint is now publicly available from `http://arxiv.org/abs/1704.03504`

Lucas sequences

Let A and B be integers. The usual Lucas sequence $u_n = u_n(A, B)$ $(n = 0, 1, 2, \ldots)$ and its companion $v_n = v_n(A, B)$ $(n = 0, 1, 2, \ldots)$ are defined as follows:

$$u_0 = 0,\ u_1 = 1,\ \text{and}\ u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots);$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and}\ v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

Note that

$$u_n(2, 1) = n,\ u_n(1, -1) = F_n,\ \text{and}\ u_n(3, 1) = F_{2n}.$$

Let

$$\alpha = \frac{A + \sqrt{\Delta}}{2}\ \text{and}\ \ \beta = \frac{A - \sqrt{\Delta}}{2}$$

be the two roots of the quadratic equation $x^2 - Ax + B = 0$ where $\Delta = A^2 - 4B$. It is well known that for any $n \in \mathbb{N}$ we have

$$(\alpha - \beta)u_n = \alpha^n - \beta^n,\ v_n = \alpha^n + \beta^n\ \text{and}\ v_n^2 - \Delta u_n^2 = 4B^n.$$

Pell's equation

Let $d \in \mathbb{Z}^+ \setminus \square$. It is well-known that the Pell equation

$$y^2 - dx^2 = 1$$

has infinitely many integral solutions. (Note that $x = 0$ and $y = \pm 1$ are trivial solutions.) Moreover,

$$\{y + \sqrt{d}x : \ x, y \in \mathbb{Z} \text{ and } y^2 - dx^2 = 1\}$$

is a multiplicative cyclic group.

For any integer $A \geqslant 2$, the solutions of the Pell equation

$$y^2 - (A^2 - 1)x^2 = 1 \ \ (x, y \in \mathbb{N})$$

are given by $x = u_n(2A, 1)$ and $y = v_n(2A, 1)$ with $n \in \mathbb{N}$. J. Robinson and his followers wrote $u_n(2A, 1)$ and $v_n(2A, 1)$ as $\psi_n(A)$ and $\chi_n(A)$ respectively.

To unify Matiyasevich's use of $F_{2n} = u_n(3, 1)$ and Robinson's use of $\psi_n(A) = u_n(2A, 1)$, we deal with Lucas sequences $(u_n(A, 1))_{n \geqslant 0}$.

On $u_n(A,1)$ with $n \in \mathbb{Z}$

We extend the sequences $u_n = u_n(A,1)$ and $v_n = v_n(A,1)$ to integer indices by letting

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n-1} + u_{n+1} = Au_n \text{ for all } n \in \mathbb{Z},$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n-1} + v_{n+1} = Av_n \text{ for all } n \in \mathbb{Z}.$$

It is easy to see that

$$u_{-n}(A,1) = -u_n(A,1) = (-1)^n u_n(-A,1)$$

and $v_{-n}(A,1) = v_n(A,1) = (-1)^n v_n(-A,1)$ for all $n \in \mathbb{Z}$.

Lemma. Let $A, X \in \mathbb{Z}$. Then

$$(A^2-4)X^2 + 4 \in \square \iff X = u_m(A,1) \text{ for some } m \in \mathbb{Z}.$$

Remark. For $n \in \mathbb{N}$ and $A \geqslant 2$, it is easy to show that

$$(A-1)^n \leqslant u_{n+1}(A,1) \leqslant A^n.$$

Diophantine representation of $C = u_B(A, 1)$ with unknowns arbitrarily large

Matiyasevich and Robinson (1975) showed that for $A > 1$ and $B, C > 0$ there is a Diophantine representation of $C = u_B(2A, 1)$ only involving three natural number variables.

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $A, B, C \in \mathbb{Z}$ with $A > 1$ and $B \geqslant 0$. Then

$$C = u_B(A, 1) \iff C \geqslant B \wedge \exists x > 0 \exists y > 0 (DFI \in \square)$$

$$\iff \exists x, y, z \geqslant 0 [DFI(C - B + 1)^2 = (z - DFI(C - B + 1))^2],$$

where

$$D = (A^2 - 4)C^2 + 4,\ E = C^2 Dx,\ F = 4(A^2 - 4)E^2 + 1,$$

$$G = 1 + CDF - 2(A + 2)(A - 2)^2 E^2,\ H = C + BF + (2y - 1)CF,$$

$$I = (G^2 - 1)H^2 + 1.$$

Moreover, if $C = u_B(A, 1)$ with $B > 0$, then for any $Z \in \mathbb{Z}^+$ there are integers $x \geqslant Z$ and $y \geqslant Z$ with $DFI \in \square$.

Diophantine representation of $C = u_B(A, 1)$ with integer unknowns

Clearly $C \geqslant B \iff \exists x \geqslant 0(C = B + x)$. However, if we use integer variables, we need three variables:

$$C \geqslant B \iff \exists x \exists y \exists z[C = B + x^2 + y^2 + z^2 + z].$$

Thus, to save the number of integer variables involved, we should try to avoid inequalities.

Note that

$$u_B(A, 1) \equiv u_B(2, 1) = B \pmod{A - 2}.$$

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let $A, B, C \in \mathbb{Z}$ with $1 < |B| < |A|/2 - 1$. Then

$$C = u_B(A, 1) \iff (A - 2 \mid C - B) \wedge \exists x \neq 0 \exists y(DFI \in \square),$$

where D, F, I are defined as before.

Diophantine representation of $W = V^B$ with integer unknowns

J. Robinson showed that $W = V^B$ (with $V > 1$ and $B, W > 0$) if and only if there is an integer $A > \max\{V^{3B}, W^B\}$ such that

$$(V^2 - 1)W\, u_B(2A, 1) \equiv V(W^2 - 1) \pmod{2AV - V^2 - 1}.$$

Lemma (Sun [Sci. China Ser. A 35(1992)]). Let B, V, W be integers with $B > 0$ and $|V| > 1$. Then $W = V^B$ if and only if there are $A, C \in \mathbb{Z}$ for which $|A| \geqslant \max\{V^{4B}, W^4\}$, $C = u_B(A, 1)$ and

$$(V^2 - 1)WC \equiv V(W^2 - 1) \pmod{AV - V^2 - 1}.$$

Remark. A, V and W in this lemma are not necessarily positive, they might be negative. We have also shown that for $B, V, W \in \mathbb{Z}$ with $B > 0$ and $|V| > 1$, the equality $W = V^B$ holds if and only if there are integers A and C for which $|A| \geqslant \max\{V^{2B}, W^2\}$, $C = u_{2B+1}(A, 1)$ and

$$(V - 1)WC \equiv VW^2 - 1 \pmod{(A^2 - 2)V - V^2 - 1}.$$

The first auxiliary theorem

Theorem 1 (Sun, arXiv:1704.03504). Let $\mathcal{A} \subseteq \mathbb{N}$ be a Diophantine set, and let p be a prime. Then, for each $a \in \mathbb{N}$, we have

$$a \in \mathcal{A} \Rightarrow \forall Z > 0 \exists f \geq Z \exists g \in [b, C)\left(b \in \square \wedge b \in p\uparrow \wedge Y \mid \binom{pX}{X}\right)$$

and

$$\exists f \neq 0 \exists g \in [0, 2C)\left(b \in \square \wedge b \in p\uparrow \wedge Y \mid \binom{pX}{X}\right) \Rightarrow a \in \mathcal{A},$$

where

$$b := 1 + (p^2 - 1)(ap + 1)f,$$

$C = p^{\alpha_1 p} b^{\alpha_2}$ for some $\alpha_1, \alpha_2 \in \mathbb{Z}^+$ only depending on $\mathcal{A}$, and X and Y are suitable polynomials in $\mathbb{Z}[a, f, g]$ such that if $a \in \mathbb{N}$, $f \in \mathbb{Z} \setminus \{0\}$, $b \in \square$ and $0 \leq g < 2C$ then

$$p + 1 \mid X, \quad X \geqslant 3b \quad \text{and} \quad Y \geqslant \max\{b, p^{4p}\}.$$

Remark. Clearly, $b \in \square \wedge f \neq 0 \Rightarrow f > 0 \wedge b > a \wedge p^2 - 1 \mid b - 1$.

The second auxiliary theorem

Theorem 2 (Sun, arXiv:1704.03504). Let p be a prime, and let $b \in p\uparrow$ and $g \in \mathbb{Z}^+$. Let P, Q, X, Y be integers with $P > Q > 0$ and $X, Y \geqslant b$. Suppose that $Y \mid \binom{PX}{QX}$. Then there are integers $h, k, l, w, x, y \geqslant b$ for which

$$DFI \in \square,\ (U^{2P}V^2-4)K^2+4 \in \square,\ pA-p^2-1 \mid (p^2-1)WC-p(W^2-1),$$

$$bw = p^B \ \text{ and } \ 16g^2(C-KL)^2 < K^2,$$

where

$$L := IY,\ U := PLX,\ V := 4gwY,$$
$$W := bw,\ K := QX+1+k(U^PV-2),$$
$$A := U^Q(V+1),\ B := PX+1,\ C := B+(A-2)h,$$

and D, F, I are as before.

Remark. We actually take $C = u_B(A,1)$, $K = u_{QX+1}(U^PV,1)$, $L = \lfloor (V+1)^{PX}/V^{QX} \rfloor \equiv \binom{PX}{QX} \pmod V$.

The third auxiliary theorem

Theorem 3 (Sun, arXiv:1704.03504). Let p be a prime, and let $b \in \mathbb{N}$ and $g \in \mathbb{Z}^+$. Let P, Q, X, Y be integers with

$$P > Q > 0,\ X \geqslant 3b,\ \text{and}\ Y \geqslant \max\{b, p^{4P}\}.$$

Suppose that there are integers h, k, l, w, x, y with $lx \neq 0$ such that

$$DFI \in \square,\ (U^{2P}V^2-4)K^2+4 \in \square,\ pA-p^2-1 \mid (p^2-1)WC-p(W^2-1),$$

and

$$4(C - KL)^2 < K^2,$$

where we adopt previous notations. Then

$$b \in p\uparrow \quad \text{and} \quad Y \mid \binom{PX}{QX}.$$

Remark. This theorem involving integer variables plays a central role in our proof of the undecidability of $\exists^{11}$ over $\mathbb{Z}$.

Main Theorem

Theorem (Sun, arXiv:1704.03504). Let $\mathcal{A} \subseteq \mathbb{N}$ be an r.e. set.

(i) There is a polynomial $P_{\mathcal{A}}(z_0, z_1, \ldots, z_9)$ with integer coefficients such that for any $a \in \mathbb{N}$ we have

$$\exists z_1 \ldots \exists z_8 \exists z_9 \geqslant 0[P_{\mathcal{A}}(a, z_1, \ldots, z_9) = 0] \Longrightarrow a \in \mathcal{A},$$

and

$$a \in \mathcal{A} \Longrightarrow \forall Z > 0 \exists z_1 \geqslant Z \ldots \exists z_9 \geqslant Z[P_{\mathcal{A}}(a, z_1, \ldots, z_9) = 0].$$

(ii) There is a polynomial $Q_{\mathcal{A}}(z_0, z_1, \ldots, z_{10})$ with integer coefficients such that for any $a \in \mathbb{N}$ we have

$$a \in \mathcal{A} \iff \exists z_1 \ldots \exists z_9 \exists z_{10} \neq 0[Q_{\mathcal{A}}(a, z_1, \ldots, z_{10}) = 0].$$

Two Lemmas

Lemma 1. For any $A_1, \ldots, A_k, S, T \in \mathbb{Z}$ with $S \neq 0$, we have

$$A_1 \in \square \wedge \cdots \wedge A_k \in \square \wedge S \mid T \iff \exists z[H_k(A_1, \ldots, A_k, S, T, z) = 0],$$

where

$$H_k(x_1, \ldots, x_k, x, y, z) := x^{2^k} J_k\left(x_1, \ldots, x_k, z - \frac{y}{x}\right).$$

Remark. This is motivated by Matiyasevich-Robinson's Relation-Combining Theorem. Note that z is an integer variable.

Lemma 2 (Sun, arXiv:1704.03504). Let $m \in \mathbb{Z}$. Then

$$m \geqslant 0 \iff \exists x \neq 0[(3m-1)x^2 + 1 \in \square].$$

Remark. This is easy since if $m \in \mathbb{Z}^+$ then $3m - 1 \notin \square$ and hence the Pell equation

$$y^2 - (3m-1)x^2 = 1$$

has infinitely many integral solutions.

Corollary 1

As some r.e. sets are not Diophantine, the Main Theorem has the following consequence.

Corollary 1. (i) There is no algorithm to determine for any $P(z_1, \ldots, z_9) \in \mathbb{Z}[z_1, \ldots, z_9]$ whether the equation

$$P(z_0, \ldots, z_9) = 0$$

has integral solutions with $z_9 \geqslant 0$ (or $z_1 + \ldots + z_9 \geqslant 0$).

(ii) There is no algorithm to determine for any $Q(z_1, \ldots, z_{10}) \in \mathbb{Z}[z_1, \ldots, z_9]$ whether the equation

$$Q(z_0, \ldots, z_{10}) = 0$$

has integral solutions with $z_{10} \neq 0$ (or $z_1 + \ldots + z_{10} \neq 0$).

Remark. Let $z_9' = z_9 - z_1 - \ldots - z_8$. Then

$$P(z_1, \ldots, z_8, z_9') = 0 \text{ with } z_1 + \ldots + z_8 + z_9' \geqslant 0$$
$$\iff P(z_1, \ldots, z_8, z_9) = 0 \text{ with } z_9 \geqslant 0.$$

$\exists^{11}$ over $\mathbb{Z}$ is undecidable

Recall that

$$m \geqslant 0 \iff \exists x \exists y \exists z [m = x^2 + y^2 + z^2 + z].$$

So,

$$\begin{aligned} &\exists z_1 \ldots \exists z_8 \exists z_9 \geqslant 0 [P(z_1, \ldots, z_8, z_9) = 0] \\ \iff &\exists z_1 \ldots \exists z_{11} [P(z_1, \ldots, z_8, z_9^2 + z_{10}^2 + z_{11}^2 + z_{11}) = 0]. \end{aligned}$$

Similarly, in view of S.P. Tung's observation (1985)

$$m \neq 0 \iff \exists x \exists y [m = (2x + 1)(2y + 1)],$$

we have

$$\begin{aligned} &\exists z_1 \ldots \exists z_9 \exists z_{10} \neq 0 [Q(z_1, \ldots, z_9, z_{10}) = 0] \\ \iff &\exists z_1 \ldots \exists z_{11} [Q(z_1, \ldots, z_9, (2z_{10} + 1)(3z_{11} + 1)) = 0]. \end{aligned}$$

Therefore, both parts of the Main Theorem implies the undecidability of $\exists^{11}$ over $\mathbb{Z}$.

Corollary 2

By taking negations of the formulas

$$\exists z_1 \ldots \exists z_8 \exists z_9 \geqslant 0[P(z_1, \ldots, z_9) = 0]$$

and

$$\exists z_1 \ldots \exists z_9 \exists z_{10} \neq 0[Q(z_1, \ldots, z_{10}) = 0]$$

in the Main Theorem, we get the following result.

Corollary 2 (Sun, arXiv:1704.03504) (i) $\forall^9\exists^3$ over $\mathbb{Z}$ is undecidable, i.e., there is no algorithm to test whether

$$\forall z_1 \ldots \forall z_9 \exists x \exists y \exists z[P(z_1, \ldots, z_9, x, y, z) = 0],$$

where P is an arbitrary polynomial of 12 variables with integer coefficients.

(ii) $\forall^{10}\exists^2$ over $\mathbb{Z}$ is undecidable, i.e., there is no algorithm to test whether

$$\forall z_1 \ldots \forall z_{10} \exists x \exists y[Q(z_1, \ldots, z_{10}, x, y) = 0],$$

where Q is an arbitrary polynomial of 12 variables with integer coefficients.

Quantifier prefixes over Diophantine equations

In 1987 S.P. Tung proved for each $n \in \mathbb{Z}^+$ that $\forall^n\exists$ over $\mathbb{Z}$ is co-NP-complete. He also showed that $\forall^{27}\exists^2$ over $\mathbb{Z}$ is undecidable, and asked whether 27 here can be replaced by a smaller number. Corollary 2 of us tells that $\forall^{10}\exists^2$ over $\mathbb{Z}$ and $\forall^9\exists^3$ over $\mathbb{Z}$ are undecidable.

In 1975 Matiyasevich and Robinson showed that $\exists^2\forall\exists$ with $\forall$ bounded is undecidable over $\mathbb{N}$. In 1981 Jones obtained the decidability of $\forall\exists$ over $\mathbb{N}$ as well as some other undecidable results over $\mathbb{N}$.

In my PhD thesis in 1992, I also proved that

$$\forall\exists^6,\ \forall^2\exists^4,\ \forall\exists\forall\exists^3,\ \forall\exists\forall^3\exists^2,\ \forall^2\exists\forall^2\exists^2,\ \forall\exists^2\forall^2\exists^2,$$
$$\exists^2\forall\exists^3,\ \exists^2\forall^3\exists^2,\ \exists\forall\exists\forall^2\exists^2,\ \exists\forall\exists^4,\ \exists\forall^2\exists^3,\ \exists\forall^5\exists^2$$

over $\mathbb{Z}$ are undecidable, and that

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

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

References

For main sources of my work mentioned here, you may look at:

1. Z.-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Math. 35(1992), 257–269.

2. Z.-W. Sun, *A new relation-combining theorem and its application*, Z. Math. Logik Grundlag. Math. 38(1992), 209-212.

3. Z.-W. Sun, *Further results on Hilbert's tenth problem*, arXiv:1704.03504, http://arxiv.org/abs/1704.03504.

Thank you!