Zeitschr. f. math. Logik und Grundlagen d. Math.
Bd. 38, S. 209–212 (1992)

A NEW RELATION-COMBINING THEOREM AND ITS APPLICATION

by ZHI-WEI SUN in Nanjing (P. R. China)

Abstract

Let $\exists^n$ denote the set of all formulas $\exists x_1 \ldots \exists x_n [P(x_1, \ldots, x_n) = 0]$, where P is a polynomial with integer coefficients. We prove a new relation-combining theorem from which it follows that if $\exists^n$ is undecidable over N, then $\exists^{2n+2}$ is undecidable over Z.
MSC: 03D35, 03F30.
Key words: Hilbert's tenth problem, relation-combining, decidability, undecidability.

In 1970 JU. V. MATIJASEVIČ [3] took the last step to solve HILBERT's tenth problem negatively. Consequently it follows that $\exists^n$, the set of formulas of the form $\exists x_1 \exists x_2 \ldots \exists x_n [P(x_1, \ldots, x_n) = 0]$, where P is a polynomial with integer coefficients, is undecidable over $\mathrm{N} = \{0, 1, 2, \ldots\}$ for sufficiently large n. In 1975 MATIJASEVIČ and J. ROBINSON [6] proved that every Diophantine equation with natural number unknowns is reducible to one in 13 unknowns, therefore $\exists^{13}$ is undecidable over N. In this reduction a relation-combining theorem plays an important role. In [5] MATIJASEVIČ announced further that $\exists^9$ is undecidable over N, a complete proof can be found in J. P. JONES [2]. In the proof of the 9-unknowns theorem the relation-combining theorem is again an important tool. Can we replace 9 by a smaller number? It is believed so. In fact, A. BAKER, MATIJASEVIČ and J. ROBINSON even conjectured that $\exists^3$ is undecidable over N (cf. [1], [6]).

Concerning integer unknowns, S. P. TUNG [11] conjectured the decidability of $\exists^2$ over Z, and he showed in [10] that $\exists^{27}$ is undecidable over Z. (From MATIJASEVIČ [4] we know that $x \in \mathrm{N} \Leftrightarrow \exists a, b, c \in \mathrm{Z} (x = a^2 + b^2 + c^2 + c)$, and hence the undecidability of $\exists^n$ over N implies the undecidability of $\exists^{3n}$ over Z.)

In this paper we will present a new relation-combining theorem, from which it follows that if $\exists^n$ is undecidable over N, then $\exists^{2n+2}$ is undecidable over Z.

By $\square$ we denote the set of all squares. Let us first recall the famous

Matijasevič-Robinson Relation-Combining Theorem. *For each k there is a polynomial M_k with integer coefficients such that for all integers $A_1, \ldots, A_k, B, C, D$ with $B \neq 0$ the conditions*

$$A_1 \in \square, \quad \ldots, \quad A_k \in \square, \quad B \mid C, \quad D > 0$$

all hold if and only if

$$M_k(A_1, \ldots, A_k, B, C, D, n) = 0$$

for some natural number n.

This relation-combining theorem is about Diophantine representations with natural number unknowns. In the following we will present a new one concerned with integer unknowns.

For this purpose in the following all variables range over Z. As auxiliary we need

Lemma 1. $m \neq 0 \Leftrightarrow \exists x \exists y[m = (2x-1)(3y-1)]$.

This is a simple fact due to S. P. TUNG [10].

Lemma 2. $m \geqq 0 \Leftrightarrow \exists y \neq 0[(4m+2)y^2 + 1 \in \square]$.

Proof. ($\Rightarrow$) Let $m \geqq 0$. Since $4m+2 \not\equiv 0, 1 \pmod 4$ we have $4m+2 \in \mathrm{N} - \square$. By a well-known theorem in number theory, there are infinitely many x and y such that $x^2 - (4m+2)y^2 = 1$, and hence $(4m+2)y^2 + 1 \in \square$ for some $y \neq 0$.

($\Leftarrow$) Suppose that $y \neq 0$ satisfies $(4m+2)y^2 + 1 \in \square$. If $m < 0$, then $0 \leqq (4m+2)y^2 + 1 \leqq -2y^2 + 1 \leqq -2 + 1 < 0$. This contradiction shows that m is nonnegative.

Our Lemma 2 is much simpler than the following result due to R. M. ROBINSON [7]:

$$m \geqq 0 \Leftrightarrow \exists x \exists y[m = x^2 \vee (x^3 = x + mxy^2 \wedge x^3 \neq x)].$$

Below we will see the key role of Lemma 2.

Lemma 3. *Let*

$$\prod (x \pm \sqrt{A_1} \pm \sqrt{A_2}\, W \pm \ldots \pm \sqrt{A_k}\, W^{k-1}) = x^{2^k} + F_1 x^{2^k - 1} + \ldots + F_{2^k - 1} x + F_{2^k},$$

where $W = 1 + \sum_{i=1}^{k} A_i^2$ *and the product extends over all combinations of signs. Then whenever* $S \neq 0$ *we have*

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

where the polynomial H_k *(with integer coefficients) is given by*

$$H_k(A_1, \ldots, A_k, S, T, x) = (Sx+T)^{2^k} + F_1 S(Sx+T)^{2^k-1} + \ldots + F_{2^k-1} S^{2^k-1}(Sx+T) + F_{2^k} S^{2^k}.$$

This lemma can be easily seen from Section 1 of [6]. A direct proof was given in SUN [8].

Now we are ready to present

New Relation-Combining Theorem. *Whenever* $D \neq 0$ *we have*

$$A_1, \ldots, A_k \in \square \wedge B_1, \ldots, B_m \neq 0 \wedge C_1, \ldots, C_n \geqq 0 \wedge D \mid E$$
$$\Leftrightarrow \exists x_0 \exists x_1 \ldots \exists x_{n+1}[P(A_1, \ldots, A_k; B_1, \ldots, B_m; C_1, \ldots, C_n; D, E, x_0, x_1, \ldots, x_{n+1}) = 0],$$

where

$$P(A_1, \ldots, A_k; B_1, \ldots, B_m; C_1, \ldots, C_n; D, E, x_0, x_1, \ldots, x_{n+1})$$
$$= H_{k+n}(A_1, \ldots, A_k, (4C_1+2)x_1^2 + 1, \ldots, (4C_{n-1}+2)x_{n-1}^2 + 1,$$
$$(4(C_n+1)B_1^2 \cdots B_m^2 x_1^2 \cdots x_{n-1}^2 - 2) \times (2x_n - 1)^2 (3x_{n+1} - 1)^2 + 1, D, E, x_0).$$

Proof.

$$A_1, \ldots, A_k \in \square \wedge B_1, \ldots, B_m \neq 0 \wedge C_1, \ldots, C_n \geqq 0 \wedge D \mid E$$
$$\Leftrightarrow A_1, \ldots, A_k \in \square \wedge C_1, \ldots, C_{n-1} \geqq 0 \wedge B_1^2 \cdots B_m^2 (C_n + 1) > 0 \wedge D \mid E$$
$$\Leftrightarrow A_1, \ldots, A_k \in \square \wedge \exists x_1 \exists x_2 \ldots \exists x_{n-1}[(4C_1+2)x_1^2 + 1 \in \square \wedge \ldots \wedge (4C_{n-1}+2)x_{n-1}^2 + 1 \in \square$$
$$\wedge B_1^2 \cdots B_m^2 (C_n + 1) x_1^2 \cdots x_{n-1}^2 - 1 \geqq 0 \wedge D \mid E]$$

$$\Leftrightarrow \exists x_1 \ldots \exists x_{n-1} \exists y \neq 0[A_1, \ldots, A_k, (4C_1+2)x_1^2+1, \ldots, (4C_{n-1}+2)x_{n-1}^2+1 \in \square \wedge (4B_1^2 \cdots B_m^2(C_n+1)x_1^2 \cdots x_{n-1}^2-2)y^2+1 \in \square \wedge D \mid E]$$

$$\Leftrightarrow \exists x_1 \ldots \exists x_{n-1} \exists x_n \exists x_{n+1} \exists x_0 [H_{k+n}(A_1, \ldots, A_k, (4C_1+2)x_1^2+1, \ldots, (4C_{n-1}+2)x_{n-1}^2+1, (4(C_n+1)B_1^2 \cdots B_m^2 x_1^2 \cdots x_{n-1}^2-2)(2x_n-1)^2(3x_{n+1}-1)^2+1, D, E, x_0)=0].$$

This concludes the proof.

From the theorem we see that

$$\exists x_1 \geqq 0 \ldots \exists x_n \geqq 0[Q(x_1, \ldots, x_n)=0]$$
$$\Leftrightarrow \exists x_1 \ldots \exists x_n \exists y_0 \ldots \exists y_{n+1}[Q^2(x_1, \ldots, x_n)+H_n^2((4x_1+2)y_1^2+1, \ldots, (4x_{n-1}+2)y_{n-1}^2+1, (4(x_n+1)y_1^2 \cdots y_{n-1}^2-2)(2y_n-1)^2(3y_{n+1}-1)^2+1, 1, 0, y_0)=0].$$

This observation yields the following application:

Corollary. *If $\exists^n$ is undecidable over* N, *then $\exists^{2n+2}$ is undecidable over* Z.
Hence we have

(i) *If $\exists^6$ is decidable over* Z, *then $\exists^2$ is decidable over* N.

(ii) *The Baker-Matijasevič-Robinson conjecture implies the undecidability of $\exists^8$ over* Z.

(iii) *$\exists^{20}$ is undecidable over* Z (by the 9-unknowns theorem).

By A. BAKER [1] we can effectively determine whether the Diophantine equation $F(x, y)=m$ is solvable or not, where m is a positive integer and F is a homogeneous polynomial with degree at least 3 and with integer coefficients, irreducible over the rational field. So, perhaps $\exists^2$ is decidable over N.

As for (iii) we mention that it is better than the current result that $\exists^{27}$ is undecidable over Z. The number 20 is certainly not the best, it was announced in [8], [9] that $\exists^{11}$ is undecidable over Z, however the proof is much more complicated and still unpublished.

Acknowledgement. The author is indebted to Prof. SHAWKWEI MOH and J. P. JONES for their encouragement.

References

[1] BAKER, A., On the representation of integers by binary forms. Philos. Trans. Royal Soc. London **263** (1968), 173–191.

[2] JONES, J. P., Universal diophantine equation. J. Symbolic Logic **47** (1982), 549–571.

[3] MATIJASEVIČ, JU. V., Enumerable sets are diophantine. Dokl. Akad. Nauk SSSR **191** (1970), 279–282.

[4] MATIJASEVIČ, JU. V., A Diophantine representation of the set of prime numbers. Dokl. Akad. Nauk SSSR **196** (1971), 770–773.

[5] MATIJASEVIČ, JU. V., Some purely mathematical results inspired by mathematical logic. In: Logic, foundations of mathematics and computability theory (BUTTS and HINTIKKA, eds.), D. Reidel Publ. Co., Dordrecht 1977, pp. 121–127.

[6] MATIJASEVIČ, JU. V., and J. ROBINSON, Reduction of an arbitrary diophantine equation to one in 13 unknowns. Acta Arith. **27** (1975), 521–553.

[7] ROBINSON, R. M., Arithmetical definitions in the ring of integers. Proc. Amer. Math. Soc. **2** (1951), 279–284.

[8] SUN, ZHI-WEI, Reduction of unknowns in Diophantine representations. Science in China (Ser. A), **35** (1992), 257–269.

[9] SUN, ZHI-WEI, Jones' work on Hilbert's tenth problem and related topics—Dedicated to Prof. Jones for his visiting China. Adv. in Math. (China), to appear.
[10] TUNG, S. P., On weak number theories. Japan. J. Math. 11 (1985), 203–232.
[10] TUNG, S. P., Computational complexities of Diophantine equations with parameters. J. Algorithms 8 (1987), 324–336.

Zhi-Wei Sun
Department of Mathematics
Nanjing University
Nanjing 210008
China

(Eingegangen am 23. Juli 1990)