PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 77, Number 3, December 1979

SOME DECIDABLE DIOPHANTINE PROBLEMS: POSITIVE SOLUTION TO A PROBLEM OF DAVIS, MATIJASEVIČ AND ROBINSON[1]

MOSHE KOPPEL

ABSTRACT. An algorithm is given for determining whether or not a finite system of conditions of the types $a|B$, $a < B$, a is a square, possess a simultaneous solution in positive integers. Various generalizations are also obtained.

In 1970, Matijasevič proved that there is no algorithm to determine if a general polynomial Diophantine equation has a solution in positive integers (see, for example, Davis, Matijasevič and Robinson [1]). A particularly neat formulation of this theorem can be obtained from the observation made by Skolem [6] that any Diophantine equation can be reduced to a system of conditions of types $\alpha + \beta = \gamma$, $\alpha \cdot \beta = \gamma$. The theorem then reads: There is no algorithm to determine whether a system of conditions of types: $\alpha + \beta = \gamma$, $\alpha \cdot \beta = \gamma$ has a solution in positive integers.

There are other relations such that certain systems of conditions using those relations are equivalent to $\alpha + \beta = \gamma$ and $\alpha \cdot \beta = \gamma$. For example, consider the relations $\alpha + 1 = \beta$, $\alpha \cdot \beta = \gamma$. Then, $x + y = z$ is equivalent to the system $x + 1 = \alpha_1$, $z + 1 = \alpha_2$, $\alpha_1 \cdot \alpha_2 = \alpha_3$, $\alpha_3 + 1 = \alpha_4$, $\alpha_2 \cdot y = \alpha_5$, $\alpha_5 + 1 = \alpha_6$, $\alpha_6 \cdot \alpha_4 = \alpha_7$, $\alpha_1 \cdot y = \alpha_8$, $\alpha_8 + 1 = \alpha_9$, $\alpha_9 \cdot \alpha_2 = \alpha_{10}$, $\alpha_{10} \cdot \alpha_2 = \alpha_{11}$, $\alpha_{11} + 1 = \alpha_7$. (This is simply an expansion of $s(sx \cdot sz) \cdot s(y \cdot sz) = s(sz \cdot sz \cdot s(sx \cdot y))$ where $s\alpha = \alpha + 1$.) Consequently, there is no algorithm to determine if a system of conditions of types: $\alpha + 1 = \beta$, $\alpha \cdot \beta = \gamma$ has a solution in positive integers.

Similar methods have been used to extend the theorem to various classes of relations (see, for example, Robinson [4] and Schwartz [5]). In particular, Kosovskii [3] showed that there is no algorithm to determine if a system of conditions of types: $\alpha + \beta = \gamma$, $\alpha | \beta$, $\alpha = \square$ has a solution in positive integers. ($\alpha = \square$ means that α is a perfect square.)

This result motivated the problem posed by Davis, Matijasevič and Robinson [1]:

(*) Does there exist an algorithm to determine if a sequence of formulas of types: $\alpha < \beta$, $\alpha | \beta$, $\alpha = \square$ has a solution in positive integers?

Received by the editors June 8, 1978 and, in revised form, July 10, 1978.
AMS (*MOS*) *subject classifications* (1970). Primary 10N05, 10B99.
Key words and phrases. Diophantine problems, decidability.
[1]The author gratefully acknowledges the invaluable assistance of Professor M. Davis. Thanks are also due to David Bassain for his numerous helpful suggestions.

This paper includes a general theorem concerning binary relations which has as a corollary an affirmative solution to (*).

In this paper α, β are either variables or positive integers and N is the set of positive integers. $\alpha\ R\ \beta$ means "α is related to β in relation R",

$$R(\alpha) = \{\beta \mid \alpha\ R\ \beta\}, \quad R(S) = \bigcup_{\alpha \in S} R(\alpha).$$

Below, contexts will be encountered in which specific variables have their range restricted by stipulations already made. In such contexts, $\langle\alpha\rangle$ represents the set of possible values of the variable α.

DEFINITION. The family of computable functions $\{g^{(l)}: l \in N\}$ is called a *generalized common multiple in the relation* R if for any $\alpha_1, \ldots, \alpha_l$,

$$g^{(l)}(\alpha_1, \ldots, \alpha_l) \in \bigcap_{i=1}^{l} R(\alpha_i).$$

Consider computable relations $R_1, \ldots, R_m$ and computable sets $S_1, \ldots, S_n$. Let

$$R_U = \bigcup_{i=1}^{m} R_i, \qquad R_I = \bigcap_{i=1}^{m} R_i, \qquad S_I = \bigcap_{i=1}^{n} S_i,$$

$P_I(\alpha) = R_I(\alpha) \cap S_I$. Then we have:

MAIN THEOREM. *If* (i) *for all* $i = 1, \ldots, m$, $\alpha\ R_i\ \beta \Rightarrow \alpha < f(\beta)$ *for some strictly increasing computable function* f,

(ii) *there is a family* $\{g^{(l)}: l \in N\}$ *which is a generalized common multiple in the relation* P_I.

For all $i = 1, 2, \ldots, m$ *there exists* c_0 *such that*

(iii) *either for all* $\alpha > c_0$ $\alpha\ R_i\ \alpha$, *in which case* R_i *is called* c_0*-reflexive, or for all* $\alpha > c_0 \sim \alpha\ R_i\ \alpha$ *in which case* R_i *is called* c_0*-antireflexive, and*

(iv) *for all* $\alpha > c_0$, $R_U(R_U(\alpha) - \{\alpha\}) \subseteq R_U(\alpha) - \{\alpha\}$,

then there exists an algorithm to determine whether or not a given system of conditions of the types $\alpha\ R_i\ \beta$, $\alpha \in S_i$, *has a solution in positive integers.*

Let P be some given system consisting of p_0 conditions. The proof of the Main Theorem will use the following definitions, of which the second is inductive.

DEFINITION. L_P is the set of (numbers or variables) α such that P contains a sequence of conditions of the form:

$$\alpha\ R_{i_1}\ \alpha_1, \quad \alpha_1\ R_{i_2}\ \alpha_2, \quad \cdots, \quad \alpha_{w-1}\ R_{i_w}\ \alpha \tag{1}$$

where some R_{i_j} is c_0-antireflexive.

DEFINITION.

$$B_P = \{c \in N: (\alpha\ R\ c) \in P\} \cup \{\alpha: (\alpha\ R\ \beta) \in P \wedge \beta \in (L_P \cup B_P)\}.$$

Thus, $L_P \subseteq B_P$.

Let $c_1 = \max_{c \in B_P} c$, $c_2 = f^{(2p_0)}(c_0) + f^{(p_0)}(c_1)$ where f and c_0 are from the statement of the theorem, and $f^{(p_0)}$ is the function obtained by p_0 iterations of f:

DEFINITION. $\bar{P} = \{\alpha\ R\ \beta\colon\ (\alpha\ R\ \beta) \in P \wedge \alpha, \beta \in B_P\} \cup \{\alpha \in S_i\colon\ (\alpha \in S_i) \in P \wedge \alpha \in B_P\}$.

The proof of the Main Theorem follows from the following.

LEMMA. *P has a solution in positive integers if and only if $\bar{P}$ has a solution in positive integers $< c_2$.*

PROOF. Suppose P has a solution. Let $\alpha \in L_P$. Then there is the sequence of conditions (1) where R_{i_j} is c_0-antireflexive. Now, suppose that P had a solution in which α_{j-1} had a value $x > c_0$. Then $x \notin \langle \alpha_j \rangle$. Therefore, $\langle \alpha_j \rangle \subseteq R_u(x) - \{x\}$, and

$$x \in R^{(w-1)}(\langle \alpha_j \rangle) \subseteq R_u(x) - \{x\},$$

using (1) and (iv). This contradiction shows that for any solution, $\alpha_{j-1} \leqslant c_0$ and $\alpha_i \leqslant f^{(p_0)}(c_0)$ for $i = 1, 2, \ldots, w$. Hence any solution of P is such that all variables in L_P have values $\leqslant f^{(p_0)}(c_0)$.

Next let $\alpha \in B_P$. Then P contains a sequence of the form

$$\alpha\ R_{i_0}\,\alpha_1, \quad \alpha_1\ R_{i_1}\,\alpha_2, \quad \ldots, \quad \alpha_w\ R_{i_w}\ \beta$$

where $w < p_0$ and β is either a constant $\leqslant c_1$ or a variable in L_P and hence with value $< f^{(p_0)}(c_0)$ in any solution. Then, in any solution of P,

$$\begin{aligned} \alpha &\leqslant f^{(w)}\big(\max\big(c_1, f^{(p_0)}(c_0)\big)\big) \\ &= \max\big(f^{(w)}(c_1), f^{(w+p_0)}(c_0)\big) < c_2. \end{aligned}$$

Since all variables in B_P have values $< c_2$ in any solution of P, $\bar{P}$ has such a solution.

Conversely, suppose $\bar{P}$ has such a solution. Then any "loop" of the form (1) in which no R_{i_j} is c_0-antireflexive can be satisfied by

$$\alpha = \alpha_1 = \alpha_2 = \cdots = \alpha_w > c_0.$$

Consequently all such "loops" in P can be eliminated by replacing each occurrence of α_i ($i = 1, 2, \ldots, w$) by α. (But the value to be assigned α must be $> c_0$.)

For the purpose of this proof α is called a *parent* of β if the condition $\alpha\ R_i\ \beta$ is in P for some i, and the *generation* of α, for $\alpha \notin B_P$, is the largest w such that P contains a sequence

$$\alpha_1\ R_{i_1}\,\alpha_2, \quad \alpha_2\ R_{i_2}\,\alpha_3, \quad \ldots, \quad \alpha_w\ R_{i_w}\ \alpha$$

where $\alpha_2 \notin B_P$. Since $\bar{P}$ has a solution we can assign values to all $\alpha \in B_P$. Also assign all parentless α's the value s_0 where $s_0 = \min(S_l)$. At this point any variable of the first generation, say α, has parents which are either constants or have already been assigned values. Suppose these parents have values $a_1, \ldots, a_l$. Then fix the value of α as $g^{(l+1)}(a_1, \ldots, a_l, f(c_0))$. ($f(c_0)$ is included as an argument in order to guarantee, by (i) that variables arising from collapsed "loops" are given values $> c_0$.) In this way the whole first generation is assigned values. Now any variable of the second generation has parents with definite values. Continue this process until all variables have been assigned values. These values constitute a solution of P in positive integers.

Using the same notation as above and sacrificing some generality a much simpler statement of the Main Theorem can be obtained.

COROLLARY. *If* (i) *there is a family* $\{g^{(l)}: l \in N\}$ *which is a generalized common multiple in the relation* P_l,

(ii) R_i *is reflexive or antireflexive, and*

(iii) $\alpha\ R_i\ \beta$ *implies* $\alpha \leqslant \beta$,

then there is an algorithm to determine whether or not a system of conditions of types $\alpha\ R_i\ \beta$, $\alpha \in S_i$, *has a solution in positive integers.*

There are two interesting applications of this corollary.

The first gives a positive solution to the problem posed in [1].

COROLLARY. *There is an algorithm to determine whether or not a system of conditions of types* $\alpha < \beta$, $\alpha \mid \beta$, $\alpha = \square$ *has a solution in positive integers.*

The second finds a fine boundary line between decidable and undecidable problems.

THEOREM. *There is an algorithm to determine whether or not a system of conditions of type* $f_i(\beta) < \alpha$, *where the* f_i *are any recursive, strictly increasing functions, has a solution in positive integers. However for general nondecreasing functions* f_i *there is no such algorithm.*

PROOF. The first assertion is an immediate consequence of the first corollary above where the R_i of the corollary are $f_i(\beta) < \alpha$. To prove the second assertion, suppose there were such an algorithm. Then in particular there is an algorithm to determine whether or not there is a solution in positive integers to the system:

$$f_1(\beta) - 1 < \alpha, \quad f_1^{-1}(\alpha) - 1 < \beta, \qquad f_2(\gamma) - 1 < \alpha, \quad f_2^{-1}(\alpha) - 1 < \gamma$$

where $f_i^{-1}(\alpha) = \min_x(f_i(x) \geqslant \alpha)$. (If the minimum does not exist let $f_i^{-1}(\alpha)$ be "infinite".) This sequence of formulas is equivalent to $f_1(\beta) = \alpha = f_2(\gamma)$. Consequently, if there were an algorithm to determine whether or not this system has a solution then there would be an algorithm to determine whether or not $\mathrm{Range}(f_1) \cap \mathrm{Range}(f_2) = \varnothing$. But since every computable set–and, in particular, every context-free set–is expressible as $\mathrm{Range}(f)$ for some increasing computable function f, we would then have an algorithm to determine whether $L(\Gamma_1) \cap L(\Gamma_2) = \varnothing$ where Γ_1 and Γ_2 are context-free grammars and where $L(\Gamma)$ is the language accepted by Γ. No such algorithm exists (cf., e.g., [2, p. 583]).

REFERENCES

1. Martin Davis, Yuri Matijasevič and Julia Robinson, *Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution*, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R. I., 1976, pp. 323–378.

2. ______, *Unsolvable problems*, Handbook of Mathematical Logic, North-Holland, Amsterdam, 1977, pp. 567–594.

3. N. K. Kosovskii, *On solutions of systems consisting of both word equations and word length inequalities*, Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **40** (1974), 24–29. (Russian)

4. Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

5. Edward Schwartz, *Existential definability in terms of some quadratic functions*, Doctoral Dissertation, Yeshiva University, 1974.

6. Th. Skolem, *Diophantische Gleichungen*, Ergebnisse der Math. und ihrer Grenzgebiete, Band 5, Springer, Berlin, 1938.

COURANT INSTITUTE OF MATHEMATICAL SCIENCES, NEW YORK UNIVERSITY, NEW YORK, NEW YORK 10012