BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 3, Number 2, September 1980

UNDECIDABLE DIOPHANTINE EQUATIONS

BY JAMES P. JONES

In 1900 Hilbert asked for an algorithm to decide the solvability of all diophantine equations, $P(x_1, \ldots, x_v) = 0$, where P is a polynomial with integer coefficients. In special cases of Hilbert's tenth problem, such algorithms are known. Siegel [7] gives an algorithm for all polynomials $P(x_1, \ldots, x_v)$ of degree $\leqslant 2$. From the work of A. Baker [1] we know that there is also a decision procedure for the case of homogeneous polynomials in two variables, $P(x, y) = c$.

The first steps toward the eventual negative solution of the entire (unrestricted) form of Hilbert's tenth problem, were taken in 1961 by Julia Robinson, Martin Davis and Hilary Putnam [2]. They proved that every recursively enumerable set, W can be represented in exponential diophantine form

$$x \in W \Leftrightarrow \exists x_1, x_2, \ldots, x_\mu \, P(x, x_1, \ldots, x_\mu, 2^{x_1}, \ldots, 2^{x_\mu}) = 0,$$

where P is a polynomial with integer coefficients and $x_1, \ldots, x_\mu$ range over positive integers.

In 1970 Ju. V. Matijasevič [4] proved that the exponential relation, $y = 2^x$ is diophantine and hence that every r.e. set W can be represented in polynomial (diophantine) form

$$x \in W \Leftrightarrow \exists x_1, x_2, \ldots, x_v \, P(x, x_1, x_2, \ldots, x_v) = 0,$$

where the unknowns $x_1, \ldots, x_v$ range over positive integers.

Since there exist r.e. nonrecursive sets, Matijasevič's Theorem implies the undecidability of Hilbert's tenth problem. There is no algorithm to decide whether an arbitrary diophantine equation has a solution.

Matijasevič's Theorem implies also the existence of particular undecidable diophantine equations. In fact there must exist *universal* diophantine equations, polynomial analogues of the universal Turing machine. This follows from the well-known fact that the r.e. sets, $W_1, W_2, \ldots$, can be listed in such a way that the binary relation, $x \in W_v$, is r.e. Hence by [2], [4] there exists a universal polynomial $U(x, v, x_1, \ldots, x_v)$ with the property

$$x \in W_v \Leftrightarrow \exists x_1, \ldots, x_v \, U(x, v, x_1, \ldots, x_v) = 0.$$

Thus a single polynomial, in a fixed degree and a fixed number of unknowns, can define every r.e. set, by mere change of a parameter v. The existence of such

Received by the editors March 5, 1980.
AMS (MOS) subject classifications (1970). Primary 02F25, 10N05; Secondary 10B15.

0002-9904/80/0000-0406/$02.00

a universal polynomial follows immediately from [2], [4]. However, the construction of an actual example is a different matter. The first example to be specifically written down is given in [3]. More recently the author has constructed further examples. These are given below, without proof. (The proof uses the code idea of [6] together with new methods of Matijasevič based on E. Kummer's Theorem about divisibility of binomial coefficients by prime powers.)

THEOREM 1. *In order that* $x \in W_{\langle z,u,y\rangle}$, *it is necessary and sufficient that the following system of equations has a solution in positive integers.*

$$elg^2 + \alpha = (b - xy)q^2, \quad q = b^{5^{60}}, \quad \lambda + q^4 = 1 + \lambda b^5, \quad \theta + 2z = b^5,$$

$$l = u + t\theta, \quad e = y + m\theta, \quad b = 2^w,$$

$$\binom{g + q^3 - 1 - bl + l}{g} \binom{\theta\lambda + e + lq^2}{\theta\lambda}$$

$$\cdot \binom{b^5q - 2q + 2(e - z\lambda)(1 + xb^5 + g)^4 + b^5\lambda(1 + q^4)}{b^5q - 2q} = 2\eta + 1.$$

Here we consider the r.e. sets to be indexed by three indices, z, u, y instead of the usual one. This is an inessential restriction. If the reader prefers the traditional indexing with a single parameter v, he need only add to our equations a new equation, $v = ((zuy)^2 + u)^2 + y$ and regard z, u and y as unknowns instead of parameters.

As stated above our system of equations has 12 unknowns, specifically b, e, g, l, m, q, t, w, α, η, θ, λ and four parameters, z, u, y and x. An exponential equation, $b = 2^w$ appears, and the last line is a product of three binomial coefficients. In the next system the number of binomial coefficients is reduced to one.

THEOREM 2. *In order that* $x \in W_{\langle z,u,y\rangle}$, *it is necessary and sufficient that the following system of equations has a solution in positive integers.*

$$elg^2 + \alpha = (b - xy)q^2, \quad q = b^{5^{60}}, \quad \lambda + q^4 = 1 + \lambda b^5, \quad \theta + 2z = b^5,$$

$$l = u + t\theta, \quad e = y + m\theta, \quad b = 2^w, \quad n = q^{16},$$

$$r = [g + eq^3 + lq^5 + (2(e - z\lambda) \cdot (1 + xb^5 + g)^4 + \lambda b^5 + \lambda b^5q^4)q^4]$$

$$\cdot [n^2 - n] + [q^3 - bl + l + \theta\lambda q^3 + (b^5 - 2)q^5] \cdot [n^2 - 1], \quad \eta n^2 = \binom{2r}{r}.$$

Here there are fourteen unknowns, b, e, g, l, m, n, q, r, t, w, α, η, θ, λ and the four parameters x, z, u, y. Only one binomial coefficient and one exponential

function appear. Next these are eliminated so that we obtain a system of purely polynomial equations.

THEOREM 3. *In order that* $x \in W_{\langle z,u,y\rangle}$, *it is necessary and sufficient that the following system of equations has a solution in positive integers.*

$$elg^2 + \alpha = (b - xy)q^2, \quad q = b^{5^{60}}, \quad \lambda + q^4 = 1 + \lambda b^5,$$

$$\theta + 2z = b^5, \quad l = u + t\theta, \quad e = y + m\theta, \quad n = q^{16},$$

$$r = [g + eq^3 + lq^5 + (2(e - z\lambda)(1 + xb^5 + g)^4 + \lambda b^5 + \lambda b^5 q^4)q^4][n^2 - n]$$

$$+ [q^3 - bl + l + \theta\lambda q^3 + (b^5 - 2)q^5][n^2 - 1],$$

$$p = 2ws^2r^2n^2, \quad p^2k^2 - k^2 + 1 = \tau^2, \quad 4(c - ksn^2)^2 + \eta = k^2,$$

$$k = r + 1 + hp - h, \quad a = (wn^2 + 1)rsn^2,$$

$$c = 2r + 1 + \varphi, \quad d = bw + ca - 2c + 4\alpha\gamma - 5\gamma, \quad d^2 = (a^2 - 1)c^2 + 1,$$

$$f^2 = (a^2 - 1)i^2c^4 + 1, (d + of)^2 = ((a + f^2(d^2 - a))^2 - 1)(2r + 1 + jc)^2 + 1.$$

The equations of Theorem 3 have twenty eight unknowns, $a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, w, \alpha, \gamma, \eta, \theta, \lambda, \tau, \varphi$. The degree is 5^{60}, however the equation $q = b^{5^{60}}$ can be replaced by certain others of low degree. In fact, by introducing some 30 additional unknowns and new equations one can reduce the degree of the system to 2. Then, by transposing terms to one side and summing squares one can construct a universal diophantine equation in 58 unknowns and degree 4.

Alternatively one may try instead to reduce the total number of unknowns, v. In [6] Julia Robinson and Ju. Matijasevič showed that v can be reduced universally to 13. More recently Matijasevič [5] has improved this to $v = 9$. The corresponding value of the degree, δ is however very large. The following table gives various simultaneous possibilities for δ and v, sufficient for a universal equation.

THEOREM 4. *The following pairs are universal.*

$v = 58$,	$\delta = 4$	$v = 21$,	$\delta = 96$
$v = 38$,	$\delta = 8$	$v = 19$,	$\delta = 2668$
$v = 32$,	$\delta = 12$	$v = 14$,	$\delta = 2.0 \times 10^5$
$v = 29$,	$\delta = 16$	$v = 13$,	$\delta = 6.6 \times 10^{43}$
$v = 28$,	$\delta = 20$	$v = 12$,	$\delta = 1.3 \times 10^{44}$
$v = 26$,	$\delta = 24$	$v = 11$,	$\delta = 4.6 \times 10^{44}$
$v = 25$,	$\delta = 28$	$v = 10$,	$\delta = 8.6 \times 10^{44}$
$v = 24$,	$\delta = 36$	$v = 9$,	$\delta = 1.6 \times 10^{45}$

A different measure of size and complexity of a system of diophantine equations is the total number of indicated arithmetical *operations, o,* i.e. the number of additions, subtractions and multiplications necessary to evaluate or determine the correctness of proposed solution. For the equations of Theorem 3, modified to do away with $q = b^{5^{60}}$, it can be shown that $o = 100$. This number, o, can be given an interesting interpretation as a proof-theoretic complexity bound.

Via Gödel numbering the theorems of an axiomatizable theory T become in effect an r.e. set, and the search for proofs the search for solutions of a diophantine equation. These solutions faithfully reflect the logical complexity of the original proof, for the entire deduction is effectively recoverable from the solution. Hence we have

THEOREM 5. *For any axiomatizable theory T and any proposition P, if P has a proof in T, then P has another proof consisting of* 100 *additions and multiplications of integers.*

For the universal equations in [3] the value of o was 243. At present $o = 100$. As with v and δ it would be interesting to know the minimum value of o.

REFERENCES

1. A. Baker, *Contributions to the theory of diophantine equations.* I, Philos. Trans. Roy. Soc. London Ser. A **263** (1968), 173–191.

2. Martin Davis, Hilary Putnam and Julia Robinson, *The decision problem for exponential diophantine equations,* Ann. of Math. (2) **74** (1961), 425–436.

3. J. P. Jones, *Three universal representations of r.e. sets,* J. Symbolic Logic **43** (1978), 335–351.

4. Ju. V. Matijasevič, *Enumerable sets are diophantine,* Dokl. Akad. Nauk SSSR **191** (1970), 279–282. English transl.: Soviet Math. Doklady **11** (1970), 354–358.

5. ————, *Some purely mathematical results inspired by mathematical logic,* Foundations of Mathematics and Computability Theory (Butts and Hintakka, eds.), Reidel, Dordrecht, Holland, 1977, pp. 121–127.

6. Ju. V. Matijasevič and Julia Robinson, *Reduction of an arbitrary diophantine equation to one in* 13 *unknowns,* Acta Arith. **27** (1975), 521–553.

7. Carl. L. Siegel, *Zur Theorie der quadratischen Formen,* Nachr. Akad. Wiss. Göttingen Math.-Phys. KL II 1972, 21–46.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA, CANADA, T2N 1N4