PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 118, Number 2, June 1993

UNDECIDABILITY OF PARAMETRIC SOLUTIONS OF POLYNOMIAL EQUATIONS

K. H. KIM AND F. W. ROUSH

(Communicated by Andreas R. Blass)

ABSTRACT. We prove that, for any field $\mathbf{F}$ of characteristic 0 satisfying a hypothesis related to not being algebraically closed, the problem of finding nonconstant parametric solutions in $\mathbf{F}(t)$ to a polynomial system with coefficients in $\mathbf{F}$ is algorithmically unsolvable.

Solutions of Diophantine equations over rings and fields are often expressible in terms of polynomials or rational functions. That is, given an equation system over a ring $\mathscr{R}$ we find nonconstant elements of $\mathscr{R}[t]$ that satisfy the equation. Note that this is not obviously equivalent to the Diophantine problem in $\mathscr{R}[t]$ since, in the latter case, we can have coefficients in $\mathscr{R}[t]$. Two reasons for interest in the parametric problem are that it relates to the case of Diophantine equations over $\mathbf{Q}$ since many systems over $\mathbf{Q}$ have parametric solutions and that it corresponds to nonconstant maps of affine varieties.

After the Matijasevitch-Davis-Putnam-Robinson proof that the Diophantine problem is unsolvable over $\mathbf{Z}$, Denef and coworkers extended this result to various rings of algebraic integers and to $\mathscr{R}[t]$ for $\mathscr{R}$ of characteristic zero (but did not treat the parametric problem) [D1]. In [D2] he dealt with $\mathscr{R}[t]$ for $\mathscr{R}$ of positive characteristic. See [C, BDL] for related work on these questions. Recently, Pheidas, in unpublished work using methods of [P], proved Diophantine undecidability of $\mathscr{R}[t]$ for $\mathscr{R}$, a finite field, and we dealt with $\mathbf{C}(t_1, t_2)$, see [KR]. Pheidas also more recently proved unsolvability of a parametric problem for general rings $\mathscr{R}[t]$ but his problem is not the same as ours, in that he proves undecidability of nonconstancy in a chosen variable and thus does not establish undecidability of nonconstant maps of affine varieties. Neither his proof nor ours extends to settle our parametric problem for $\mathbf{C}[t]$, and we feel this probably lies deeper within algebraic geometry.

Definition. The *polynomial parametric problem* for the given ring $\mathscr{R}$ is given a finite system of polynomial equations over $\mathscr{R}$

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

Received by the editors March 5, 1990 and, in revised form, September 27, 1991.
1991 *Mathematics Subject Classification.* Primary 11U05, 12L05; Secondary 13L05.
Key words and phrases. Diophantine problem in polynomial equation, parametric solution.
This work was partly supported by NSF-DMS 8820801, 9024813.

0002-9939/93 $1.00 + $.25 per page

to find elements x_i in $\mathscr{R}[t]$, not all in $\mathscr{R}$, satisfying these equations.

(H) HYPOTHESIS. Over the given field $\mathscr{R}$ of characteristic 0, for any finite set S of elements there is a polynomial p such that p never assumes a value in S.

All the nonalgebraically closed fields of characteristic 0 which we have been able to construct have this property, but we do not know whether every nonalgebraically closed field has it.

Theorem 1. *The polynomial parametric problem is unsolvable over any field $\mathscr{R}$ of characteristic 0 that satisfies* (H).

Proof. We use an extension of the method of Denef [D1]. We take a Pell equation in which a variable u is a parameter and describe a subset of its solutions in terms of units in a ring, given u is nonconstant. Then we characterize the integers in terms of the coefficients of u in solutions of these equations. Finally, we add equations guaranteeing that u cannot be constant unless every variable is constant. It is the last step that requires the field not be algebraically closed in our proof.

Take as Pell equation

$$y^2 - (u^4 - 1)x^2 = 1 \tag{1}$$

over $\mathscr{R}[t]$. We first prove that if u is nonconstant, and if

$$\begin{cases} x = a_0 + a_1u^2 + a_2u^4, \\ y = a_{00} + a_{10}u^2 + a_{20}u^4, \end{cases} \tag{2}$$

where a_0, a_1, a_{10}, a_{00} are constant and $a_2, a_{20} \in \mathscr{R}[t]$, then

$$y + (\sqrt{u^4 - 1})x = \pm(u^2 - \sqrt{u^4 - 1})^n$$

for some $n \in \mathbf{Z}$. We can specify that a variable $a_i \in \mathscr{R}[t]$ is constant by

$$b_{i1}b_{i2} = 1, \qquad b_{i3}b_{i4} = 1, \qquad a_i = b_{i1} + b_{i3}, \tag{3}$$

i.e., it is a sum of two units in $\mathscr{R}$.

If u is nonconstant then $(u^4 - 1)$ is not square, as otherwise we have a parametric solution of $y^2 = x^4 - 1$ and that gives a nonconstant rational map from a rational curve to a curve of genus 1. Such maps cannot exist.

Therefore, $\mathbf{F}_1 = \mathscr{R}(t, \sqrt{u^4 - 1})$ is a quadratic function field. Therefore, its group of units modulo $\mathscr{R}^*$ has rank at most 1 by consideration of valuations as follows. Let v be the valuation in additive notation of $\mathscr{R}[t]$ that gives the asymptotic degree of a rational function. It has two extensions v_1, v_2 to $\mathbf{F}_1$, according to whether we choose positive or negative signs for the square root.

For any units u_0,

$$v_1(u_0) + v_2(u_0) = v(u_0u_0^*) = 0,$$

and all other valuations, which arise from prime ideals, are trivial on u_0. Suppose that v_1 is trivial on some unit

$$u_0 = f_1 + (\sqrt{u^4 - 1})g_1$$

where f_1 and g_1 are polynomials. Then

$$v_1(2f_1) = v_1(u_0 + u_0^*) \leq \max\{v_1(u_0), v_1(u_0^*)\} = 0.$$

Therefore, f_1 is constant. Moreover

$$v_1(2g_1\sqrt{u^4-1}) = v_1(u_0 - u_0^*) \leq \max\{v_1(u_0), v_1(u_0^*)\} = 0.$$

Therefore, $g_1 = 0$. Therefore, v_1 detects all units modulo constants, and the group of units modulo constants has rank at most 1.

It has rank exactly 1 by consideration of powers of

$$\Omega = u^2 - \sqrt{u^4-1}.$$

Since Ω generates a full rank subgroup, any unit v of norm 1 is a rational power of $\pm\Omega$.

If $v^r = \pm\Omega^s$ and $(r, s) = 1$, then for some $a, b \in \mathbf{Z}$ minimizing $a+sb/r > 0$, the element $\theta = \Omega^a v^b$ will be a common root of $\pm\Omega$ and $\pm v$. If v satisfies (1) and (2) so will θ.

It remains to consider the possible roots of $\pm\Omega$. Suppose $\pm\Omega$ is an n power of

$$\Omega_1 = a + b\sqrt{u^4-1}.$$

First consider n odd. Expanding $\Omega_1^n = \Omega$ as

$$a^n + \cdots + nab^{n-1}(u^4-1)^k + (nba^{n-1} + \cdots + b^n(u^4-1)^k)\sqrt{u^4-1}$$
$$= u^2 - \sqrt{u^4-1}, \qquad k = \frac{n-1}{2},$$

we find b divides 1 and a divides u^2. Since $(a, b) = 1$, if p^s is the highest power of a prime p in a, $s > 0$, then it is also the highest power of p in

$$a^n + \cdots + nab^{n-1}(u^4-1)^k = u^2.$$

Therefore $(u^2/a, a) = 1$ and a is a constant times a perfect square dividing u^2.

Compare with (2). If $a_{00} \neq 0$ then $\gcd(a, u^2) = 1$ so a is constant since it divides u^2. If $a_{00} = 0$, then $a|u^2$ and $u^2|a$, so a is a constant times u^2. But from (1) this gives only solutions 1, -1, Ω, $-\Omega$, and conjugates.

Next consider $n = 2$. Then $2ab = \pm 1$ so a and b are constants. The norm equation implies $b = 0$. But then $\Omega_1^2 = \pm u$ cannot happen.

We have shown that any solution (x, y) of (1) and (2) is of the form

$$y + (\sqrt{u^4-1})x = \pm\Omega^n.$$

The property that n is odd is characterized among those by

$$a_{00} = 0. \tag{4}$$

By binomial expansion, the y term for Ω^n is congruent modulo u^4 to $n(u^2)(-1)^\tau$, $\tau = (n-1)/2$. Therefore, a_{10} ranges over the odd integers, so we may specify that n is an integer by

$$(n - a_{10})(n - a_{10} - 1) = 0. \tag{5}$$

Conversely, given any integer n and u, we may solve (1)–(5) using

$$y + (\sqrt{u^4-1})x^2 = \pm\Omega^m, \qquad m = 2[n/2] \pm 1.$$

Given a Diophantine equation

$$\mathbf{F}(n_1, \ldots, n_k) = 0 \tag{6}$$

over $\mathbf{Z}$, we take variables x_i and y_i and a_i and b_i satisfying k copies of the above equations for respective n. These copies of the equations have disjoint sets of variables except that the same u is used in all equations and the n's of the different copies are the same as the variables in (6). For brevity, we still refer to the copies as equations (1)–(5). Then we have shown the system (1)–(6) has a solution where u is nonconstant over $\mathscr{R}[t]$ if and only if $\mathbf{F}$ has a solution over $\mathbf{Z}$.

Now we study the case when u is constant. We will add one more equation that will still be solvable if (1)–(6) are for nonconstant u and that also ensures that if u is constant then so is every other variable. By the assumption (H), we may assume

$$u = f(v) \tag{7}$$

where v is a nonconstant polynomial that never assumes the values $0, 1, -1, i, -i$. Now suppose u is constant, so by (7) it is not $0, 1, -1, i, -i$. By (7) v is constant. By (1), factoring $y^2 - (u^4 - 1)x^2$ over an extension of the coefficient field, we find that x and y are constant. By (2) a_2, a_{20} are constant. Equation (3) can only be solved with all variables constant. By (4), (5) the n_i are constant also.

Hence if (6) has a solution over $\mathbf{Z}$ then (1)–(7) have a parametric solution over $\mathbf{Z}$; then u must be constant and we have shown that all variables are constant. □

Corollary. *Over a field satisfying hypothesis* (H) *it is undecidable whether there exists a nonconstant morphism from the affine line to a given other affine algebraic variety.*

Acknowledgment

The authors would like to express sincere thanks to an unknown referee and the communicator for very constructive comments on the original and the revisions of this paper.

References

[BDL] J. Becker, J. Denef, and L. Lipshitz, *Further remarks on the elementary theory of formal power series rings*, Model Theory of Algebra and Arithmetic (Proc. Karpacz, Poland 1979), Lectures Notes in Math., vol. 834, Springer-Verlag, Berlin, 1980.

[C] G. L. Cherlin, *Definability in power series rings of nonzero characteristic*, Models and Sets, Lecture Notes in Math., vol. 1103, Springer-Verlag, Berlin, 1984, pp. 102–112.

[D1] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

[D2] ——, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloq., vol. 82, North-Holland, Amsterdam, 1979.

[Ha] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, Berlin, 1977.

[KR] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbf{C}(t_1, t_2)$, J. Algebra (to appear).

[P] T. Pheidas, *An undecidability result for power series rings of positive characteristic*. II, Proc. Amer. Math. Soc. **100** (1987), 526–530.

Mathematics Research Group, Alabama State University, Montgomery, Alabama 36101