The Work of Kim and Roush on Questions of Decidability in Algebra and Number Theory

Kirsten Eisenträger

Received: 30 November 2012 / Accepted: 30 November 2012 / Published online: 8 March 2013
© Springer Science+Business Media Dordrecht 2013

Abstract This article describes the work of Ki Hang Kim and Fred Roush on questions of decidability in algebra and number theory.

Keywords Hilbert's Tenth Problem · Undecidability

Mathematics Subject Classification (2010) 11U05 · 03B25

1 Introduction

Ki Hang Kim wrote many papers with Fred Roush about questions of decidability in algebra and number theory. They made important contributions to several areas, in particular to questions related to generalizations of Hilbert's Tenth Problem. This paper reviews those contributions.

2 Hilbert's Tenth Problem

Hilbert's Tenth Problem in its original form was to find an algorithm to decide, given a polynomial equation $f(x_1, \dots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether it has a solution with $x_1, \dots, x_n \in \mathbb{Z}$. In 1969 Matiyasevich [18], using work by Davis, Putnam and Robinson (see [13]), proved that no such algorithm exists, *i.e.* Hilbert's Tenth Problem is undecidable. Since then, analogues of this problem have been studied by asking the same question for polynomial equations with coefficients and solutions in other recursive commutative rings R . This is referred to either as Hilbert's Tenth Problem over R or the Diophantine Problem over R . Perhaps the most important unsolved problem in this area is the case of $R = \mathbb{Q}$. More background on Hilbert's Tenth Problem can be found in [23].

The author was partially supported by National Science Foundation grant DMS-1056703.

K. Eisenträger (✉)

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA
e-mail: eisentra@math.psu.edu

2.1 An Approach to Rational Diophantine Undecidability

One strategy for proving that Hilbert's Tenth Problem over $\mathbb{Q}$ is undecidable is to try and construct a Diophantine model of the integers in $\mathbb{Q}$. A *Diophantine model of the integers* $\mathbb{Z}$ in $\mathbb{Q}$ is a Diophantine set $S \subseteq \mathbb{Q}^k$ for some $k \geq 1$, equipped with a bijection $\phi : \mathbb{Z} \rightarrow S$ such that under ϕ the graphs of addition and multiplication on $\mathbb{Z}$ correspond to subsets of S^3 that are Diophantine over $\mathbb{Q}$.

By using a reduction argument it is not hard to show that if $\mathbb{Q}$ admits a Diophantine model of the integers, then Hilbert's Tenth Problem for $\mathbb{Q}$ is undecidable.

At present nobody knows how to construct such a model. By using rational points on a rank-one elliptic curve over $\mathbb{Q}$ and the fact that the group law on the elliptic curve is given by equations in terms of the coordinates of the points it is possible to construct a Diophantine set S with a bijection to the integers such that the graph of addition is Diophantine over $\mathbb{Q}$. It is not known, however, how to obtain a set S , for which the graph of multiplication is Diophantine as well. In [4] Kim and Roush consider the problem of constructing a Diophantine model of $\mathbb{Z}$ in $\mathbb{Q}$. They show that it is possible to give a Diophantine definition of a limited form of divisibility, namely specifying that the denominator of a rational number is not divisible by a certain set of primes.

2.2 Diophantine Undecidability of $\mathbb{C}(t_1, t_2)$

While Hilbert's Tenth Problem over the rationals remains open, the function field analogue has been much more tractable. Undecidability of Hilbert's Tenth Problem is known for function fields of curves over finite fields [14, 20–22, 24], and also for several rational function fields of characteristic zero: In 1978 Denef proved the undecidability of Hilbert's Tenth Problem for rational function fields $K(T)$ over formally real fields K [12], and he was the first to use rank-one elliptic curves to prove undecidability. Kim and Roush [5] showed that the problem is undecidable for the purely transcendental function field $\mathbb{C}(t_1, t_2)$ (and for $\overline{\mathbb{F}}_p(t_1, t_2)$ when $p \neq 2$). Their approach also used rank-one elliptic curves. They proved the undecidability of Hilbert's Tenth Problem by constructing a model of $\mathbb{Z} \times \mathbb{Z}$ inside the field. To obtain such a model they used the $\mathbb{C}(t_1, t_2)$ -rational points on two elliptic curves which have rank one over $\mathbb{C}(t_1, t_2)$ and showed that a certain divisibility relations on pairs of points on the curve is Diophantine. Their result was the first result for function fields over algebraically closed fields. In [15, 17] this was generalized to finite extensions of $\mathbb{C}(t_1, \dots, t_n)$ and $\overline{\mathbb{F}}_p(t_1, \dots, t_n)$ (for p odd) and $n \geq 2$.

2.3 Diophantine Undecidability over p -adic Function Fields

In [9] Kim and Roush address Hilbert's Tenth Problem over p -adic function fields. They prove the following theorem: Let F be a subfield of a nonarchimedean local field of odd residue characteristic. Then Hilbert's Tenth Problem for $F(t)$ is undecidable. In particular, this proves that Hilbert's Tenth Problem for $\mathbb{Q}_p(t)$ is undecidable for $p > 2$ and that Hilbert's Tenth Problem is undecidable for $K(t)$ when K is a number field. The proof for $F(t)$ proceeds by using an elliptic curve of rank one over $F(t)$ to construct a Diophantine model of the integers. To construct the model the authors also give a local-global principle for determining whether certain quadratic forms are isotropic over $F(t)$. In [16, 19] the techniques of Kim and Roush were generalized to finite extensions of $F(t)$ for F as above.

2.4 Diophantine Unsolvability for Function Fields over Certain Infinite Fields of Characteristic p

In 1991 Pheidas proved that Hilbert's Tenth Problem for $F(t)$ is undecidable when F is a finite field of odd characteristic. In 1992 Kim and Roush [6] generalized this result to rational function fields over some infinite fields. They proved the following theorem:

Let p be an odd prime and F any field of characteristic p not containing the algebraic closure of a finite field. Then Hilbert's Tenth Problem for $F(t)$ is undecidable.

For the proof the authors use equations related to norm forms and division algebras and give a Diophantine definition of a predicate $P(g)$ such that if g has negative order in t then $P(g)$ is false and if g has nonnegative order in t and coefficients that are algebraic over a finite field, then $P(g)$ is true. In [22] the result was generalized to global function fields and some function fields over infinite fields.

2.5 Problems Equivalent to Rational Diophantine Solvability

Hilbert's Tenth Problem over $\mathbb{Q}$ is one of the biggest open problems in the area of Diophantine unsolvability. Assuming that Hilbert's Tenth Problem over $\mathbb{Q}$ is undecidable, Kim and Roush prove the unsolvability of a number of decision problems in algebra [3]. These include the following: Find an algorithm to decide, given algebraic groups G and H over $\mathbb{Q}$ and subspaces V and W , whether there are $g \in G$ and $h \in H$ with $gV \subset hW$. The problem of determining whether a linear space of matrices contains a singular matrix is also shown to be unsolvable. Moreover, the authors also show that the problem of determining the existence of monomorphisms or epimorphisms between finitely generated modules over additively finitely generated $\mathbb{Q}$ -algebras is undecidable.

2.6 Undecidability of Parametric Solutions of Polynomial Equations

A problem related to Hilbert's Tenth Problem is a problem to which Kim and Roush refer as the polynomial parametric problem. They define the polynomial parametric problem for a field F as follows:

Given a finite system of polynomial equations over F ,

$$f_i(x_1, \dots, x_n) = 0 \quad (i = 1, \dots, k),$$

find elements $x_1, \dots, x_n \in F[t]$, not all in F , satisfying these equations.

In [7] Kim and Roush prove that the polynomial parametric problem is unsolvable for any field F of characteristic 0 that satisfies a certain hypothesis.

The hypothesis (for a field F of characteristic zero) that the field has to satisfy is that for any finite set S of elements of F there is a polynomial g such that g never assumes a value in S . The authors point out that any field of characteristic zero that they have considered and which is not algebraically closed seems to satisfy this hypothesis, but they do not know if the hypothesis is equivalent to not being algebraically closed.

A related result was proved by Denef [12] who proved that for any integral domain R , Hilbert's Tenth Problem for $R[t]$ is undecidable.

3 Decidability Questions for Modules

3.1 Undecidability of Module Homomorphisms

In [1] Kim and Roush consider two algorithmic problems for modules over a ring R . The first is to decide, given two R -modules M_1 and M_2 , whether there exists a monomorphism from M_1 to M_2 . The second problem is to decide whether there exists an epimorphism from M_1 to M_2 . It is shown that for additively finitely generated modules and rings the first problem is algorithmically decidable, and the second is undecidable.

3.2 Decidability of Epimorphisms of Dimension Groups and Certain Modules

In [2] Kim and Roush address some arithmetic decision problems. The paper contains two main results, which are motivated by certain problems about shift equivalence.

The first is an algorithm for deciding the existence of epimorphisms of finitely generated $\mathbb{Z}[t]$ -modules. The second is that for integer matrices the epimorphism problem for their dimension modules is decidable.

4 Other Results

4.1 A Decision Procedure for Certain Abelian Varieties over Function Fields

The algorithms that are given in [8] were motivated by a study of the twists of elliptic curves that were relevant for the undecidability proofs for Hilbert's Tenth Problem over $\mathbb{R}(t)$ [12] and over $\mathbb{C}(t_1, t_2)$ [5]. In [8] Kim and Roush prove that there is a finite decision procedure for computing the rank and generators of the additive group of isogenies between two Abelian varieties over $K(t)$, where K denotes either a number field or the algebraic closure of the rational numbers $\mathbb{Q}$. The decision procedure uses Faltings' isogeny theorem and a calculation of Galois actions on the division points modulo m for increasing m .

4.2 Double Coset Decompositions for Algebraic Groups over $K[t]$

In [10] the authors state that their ultimate goal was to prove that the following problem is decidable: For any algebraic group G over a polynomial ring $K[t]$ and an algebraic representation ρ of this group and vectors v, w decide whether there is an element g in G with $v\rho(g) = w$. This motivated their investigation of analogues of some fundamental decidability results of Grunewald and Segal related to decidability of isomorphism of forms over the polynomial ring $K[t]$. They obtain a description of the set of double cosets for an algebraic group over the power series fields $K((t))$ and also a description for double cosets of the adèle group of G . They do not specify which fields K are under consideration.

4.3 Results on Undecidability of Isomorphism of Forms over Polynomial Rings

In [11] Kim and Roush prove a conditional undecidability result for the isomorphism of forms over certain polynomial rings. This is applied to related decision problems. All of the results depend on a hypothesis which concerns the structure of the units in certain associated quaternion algebras. The method of proof is via encoding of a variant of the word problem of group theory into this commutative ring theoretic context. It follows that the problem of isomorphism for algebraic varieties over fields of characteristic 0 which satisfy the hypothesis is undecidable.

References to Work of Kim and Roush

1. Kim, K.H., Roush, F.W.: Undecidability of module homomorphisms. *Proc. Am. Math. Soc.* **104**(2), 374–377 (1988)
2. Kim, K.H., Roush, F.W.: Decidability of epimorphisms of dimension groups and certain modules. *Ergod. Theory Dyn. Syst.* **9**(3), 479–493 (1989)
3. Kim, K.H., Roush, F.W.: Problems equivalent to rational Diophantine solvability. *J. Algebra* **124**(2), 493–505 (1989)
4. Kim, K.H., Roush, F.W.: An approach to rational Diophantine undecidability. In: *Proceedings of Asian Mathematical Conference 1990, Hong Kong, 1990*, pp. 242–248. World Scientific Publishing, River Edge (1992)
5. Kim, K.H., Roush, F.W.: Diophantine undecidability of $\mathbf{C}(t_1, t_2)$. *J. Algebra* **150**(1), 35–44 (1992)
6. Kim, K.H., Roush, F.W.: Diophantine unsolvability for function fields over certain infinite fields of characteristic p . *J. Algebra* **152**(1), 230–239 (1992)
7. Kim, K.H., Roush, F.W.: Undecidability of parametric solutions of polynomial equations. *Proc. Am. Math. Soc.* **118**(2), 345–348 (1993)
8. Kim, K.H., Roush, F.W.: A decision procedure for certain Abelian varieties over function fields. *J. Algebra* **163**(2), 424–446 (1994)
9. Kim, K.H., Roush, F.W.: Diophantine unsolvability over p -adic function fields. *J. Algebra* **176**(1), 83–110 (1995)
10. Kim, K.H., Roush, F.W.: Double coset decompositions for algebraic groups over $K[t]$. In: *Hilbert’s Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, Ghent, 1999. *Contemp. Math.*, vol. 270, pp. 339–356. Math. Assoc. of America, Providence (2000)
11. Kim, K.H., Roush, F.W.: Results on undecidability of isomorphism of forms over polynomial rings. *Algebra Univers.* **49**(2), 179–189 (2003). Dedicated to the memory of Gian-Carlo Rota

Supplementary References

12. Denef, J.: The Diophantine problem for polynomial rings and fields of rational functions. *Trans. Am. Math. Soc.* **242**, 391–399 (1978)
13. Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential Diophantine equations. *Ann. Math. (2)* **74**, 425–436 (1961)
14. Eisenträger, K.: Hilbert’s Tenth Problem for algebraic function fields of characteristic 2. *Pac. J. Math.* **210**(2), 261–281 (2003)
15. Eisenträger, K.: Hilbert’s tenth problem for function fields of varieties over $\mathbb{C}$. *Int. Math. Res. Not.* **59**, 3191–3205 (2004)
16. Eisenträger, K.: Hilbert’s tenth problem for function fields of varieties over number fields and p -adic fields. *J. Algebra* **310**(2), 775–792 (2007)
17. Eisenträger, K.: Hilbert’s Tenth Problem for function fields of varieties over algebraically closed fields of positive characteristic. *Monatshefte Math.* **168**(1), 1–16 (2012)
18. Matijasevič, Yu.V.: The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR* **191**, 279–282 (1970)
19. Moret-Bailly, L.: Elliptic curves and Hilbert’s tenth problem for algebraic function fields over real and p -adic fields. *J. Reine Angew. Math.* **587**, 77–143 (2005)
20. Pheidas, T.: Hilbert’s tenth problem for fields of rational functions over finite fields. *Invent. Math.* **103**(1), 1–8 (1991)
21. Shlapentokh, A.: Diophantine undecidability over algebraic function fields over finite fields of constants. *J. Number Theory* **58**(2), 317–342 (1996)
22. Shlapentokh, A.: Hilbert’s tenth problem for algebraic function fields over infinite fields of constants of positive characteristic. *Pac. J. Math.* **193**(2), 463–500 (2000)
23. Shlapentokh, A.: *Hilbert’s Tenth Problem*. New Mathematical Monographs, vol. 7. Cambridge University Press, Cambridge (2007). Diophantine classes and extensions to global fields
24. Videla, C.R.: Hilbert’s tenth problem for rational function fields in characteristic 2. *Proc. Am. Math. Soc.* **120**(1), 249–253 (1994)