UNDECIDABILITY OF POLYNOMIAL EQUATIONS OVER $\mathbb{C}(t_1, t_2)$ (WORK OF KIM AND ROUSH)

BJORN POONEN

These are notes for an expository lecture given on June 2, 2009 at a conference at Columbia University. I have no plan currently to publish them.

1. Introduction

Given a rational map of $\mathbb{C}$-varieties $X \dashrightarrow \mathbb{P}^2$, can one decide whether there is a rational section? This question, to be made precise below, is equivalent to a question about polynomial equations over $\mathbb{C}(t_1, t_2)$. As background, consider

Hilbert's tenth problem (1900): Find an algorithm[1] that takes as input an arbitrary polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and outputs YES or NO according to whether $f(\vec{x}) = 0$ has a solution in $\mathbb{Z}^n$.

Theorem 1.1 ([DPR61, Mat70])**.** *No such algorithm exists.*

Our goal is to outline a proof of the corresponding statement with $\mathbb{C}(t_1, t_2)$ in place of $\mathbb{Z}$. The proof we present is the original 1992 proof of Kim and Roush (with some minor modifications by Eisenträger, Demeyer, and myself).

Theorem 1.2. [KR92] *There is no algorithm that takes as input an arbitrary polynomial $f \in \mathbb{Q}(t_1, t_2)[x_1, \ldots, x_n]$ and outputs YES or NO according to whether $f(\vec{x}) = 0$ is solvable over $\mathbb{C}(t_1, t_2)$.*

Remark 1.3. The reason for restricting the coefficients of the input to lie in $\mathbb{Q}(t_1, t_2)$ is so that the input admits a finite description suitable for a Turing machine.

We can restate Theorem 1.2 in logical terms. A positive existential formula in the language $\langle +, \cdot, 0, 1, t_1, t_2 \rangle$ is a first order formula such as

$$(\exists x)(\exists y)\ (x + t_1 \cdot y = 1 + 1) \wedge (t_2 \cdot x + 1 = y \cdot z)$$

built using any of the symbols of the language, $=$, the logical symbols $\wedge, \vee$, and variables, some of which may be bound by existential quantifiers $\exists$, but not negation $\neg$ or universal quantifiers $\forall$. A positive existential formula in which all variables are bound by $\exists$ is called a positive existential sentence. If one then interprets the variables as running over $\mathbb{C}(t_1, t_2)$ with the symbols having their usual meanings, the sentence has a truth value. More generally, given a positive existential formula, the truth depends on the values of the free variables, so it defines a subset of $\mathbb{C}(t_1, t_2)^n$ (namely, the subset of parameter values that make the

Date: June 2, 2009.

[1]A precise notion of algorithm came only later, with the work of Church and Turing in the 1930s. The modern interpretation of "algorithm" is "Turing machine", essentially a computer program.

formula true), where n is the number of free variables; such a subset is called a positive existential subset. The positive existential theory of $\langle \mathbb{C}(t_1,t_2); +, \cdot, 0, 1, t_1, t_2\rangle$ is the set of positive existential sentences that are true for $\mathbb{C}(t_1,t_2)$. The positive existential theory is said to be decidable if there is an algorithm that can decide whether an arbitrary positive existential sentence belongs to the theory. Theorem 1.2 is equivalent to the following:

Theorem 1.4. *The positive existential theory of $\langle \mathbb{C}(t_1,t_2); +, \cdot, 0, 1, t_1, t_2\rangle$ is undecidable.*

The equivalence of Theorem 1.2 and 1.4 is almost trivial: it relies on elementary observations such as:

- Equations with coefficients in $\mathbb{Q}(t_1,t_2)$ are equivalent to equations with coefficients in $\mathbb{Z}[t_1,t_2]$.
- The formula $(f=0)\vee(g=0)$ is equivalent to $fg=0$.
- The formula $(f=0)\wedge(g=0)$ is equivalent to $f^2+t_1g^2=0$.

2. Proof

Lemma 2.1. *If m and n are odd integers, then*

$$T_0^2 - a^m T_1^2 - b^n T_2^2 = 0$$

has no nontrivial solution with $T_0, T_1, T_2 \in \mathbb{C}((a))((b))$.

Proof. Without loss of generality, $m=n=1$, and T_0,T_1,T_2 are b-adically integral, with at least one of them being nonzero modulo b. Since a is not a square in the residue field $\mathbb{C}((a))$, the element b divides T_0 and T_1. Then the equation forces b to divide T_2 as well, a contradiction. □

Let $E\colon y^2=x^3+ax+b$ be an elliptic curve over $\mathbb{C}$ with $a,b\in\mathbb{Q}$ and $\operatorname{End} E\simeq\mathbb{Z}$. Let $O\in E(\mathbb{C})$ be the identity. Let $L=\mathbb{C}(t_1,u_1,t_2,u_2)$ be the function field of $E\times E$, where the i^{th} copy of E uses the variables t_i,u_i in place of x,y. So L is a degree-4 extension of $K:=\mathbb{C}(t_1,t_2)$. Rational maps $E\times E \dashrightarrow E$ are everywhere defined, so $E(L)\simeq \operatorname{Hom}_{\mathbb{C}\text{-varieties}}(E\times E, E)$ (the morphisms here need not be homomorphisms of abelian varieties). Let $P_i\in E(L)$ correspond to the i^{th} projection $E\times E\to E$. Let $G:=\mathbb{Z}P_1\oplus\mathbb{Z}P_2\subset E(L)$. Let $G'=G-\{(O,O)\}$, which may be identified with a subset of L^2, which may be identified with K^8.

Lemma 2.2. *The subset of K^8 corresponding to G' is positive existential.*

Sketch of proof. Multiplication by -1 on $E\times E$ induces an element $\sigma\in\operatorname{Aut}(L/K)$. Let $E(L)^- := \{P\in E(L) : \sigma P = -P\}$. Then $E(L)^- = \mathbb{Z}P_1\oplus\mathbb{Z}P_2\oplus E[2]$. So $G=\mathbb{Z}P_1\oplus\mathbb{Z}P_2 = 2E(L)^- + \{O, P_1, P_2, P_1+P_2\}$, which can be expressed in terms of polynomial equations. □

For two elements (a,b) and (c,d) of $\mathbb{Z}\times\mathbb{Z}$, let $(a,b)\sim(c,d)$ mean that they are $\mathbb{Z}$-dependent.

Proposition 2.3. *We have $(a,b)\sim(c,d)$ if and only if $(a,b)=(0,0)$ or $(c,d)=(0,0)$ or there exist $T_0,T_1,T_2\in L$ not all zero such that*

$$T_0^2 - y(aP_1+bP_2)T_1^2 - y(cP_1+dP_2)T_2^2 = 0. \tag{1}$$

Proof. If (a,b) and (c,d) are nonzero and dependent, then $y(aP_1+bP_2)$ and $y(cP_1+dP_2)$ lie in a subfield $L_0 \subseteq L$ of transcendence degree 1 over $\mathbb{C}$, so the Tsen-Lang theorem (or actually, a special case proved earlier by Max Noether) shows that (1) has a solution in L_0, and hence in L.

Now suppose that (a,b) and (c,d) are independent. The divisor of $y(aP_1+bP_2)$ on $E \times E$ agrees in a neighborhood of (O,O) with $-3D_1$ where $D_1 := \{(Q_1,Q_2) \in E \times E : aQ_1+bQ_2 = O\}$. Define D_2 similarly. Then D_1 and D_2 meet transversely at (O,O). After an analytic change of variable, (1) becomes as in Lemma 2.1 with $m=n=-3$. So (1) has no nontrivial solution. □

Corollary 2.4. *There is a positive existential model of the structure* $\mathcal{L} := \langle \mathbb{Z} \times \mathbb{Z}; +, \sim, (1,0), (0,1) \rangle$ *in* $\langle \mathbb{C}(t_1,t_2); +, \cdot, 0, 1, t_1, t_2 \rangle$.

Corollary 2.4 is saying that there is a bijection between $\mathbb{Z} \times \mathbb{Z}$ and a positive existential subset of $\mathbb{C}(t_1,t_2)^N$ for some N such that the graph of $+$ in $(\mathbb{Z}\times\mathbb{Z})^3$ corresponds to a positive existential subset of $\mathbb{C}(t_1,t_2)^{3N}$, and $\sim$ corresponds to ..., and so on.

Proof. The bijection identifies $\mathbb{Z} \times \mathbb{Z}$ with G' (plus one extra point). The operation $+$ corresponds to a subset defined by polynomial equations expressing the group law on $E(L)$, and $\sim$ corresponds to a positive existential subset defined using Proposition 2.3. □

Proposition 2.5. *There is a positive existential model of* $\langle \mathbb{Z}; +, \cdot, 0, 1 \rangle$ *in* $\langle \mathbb{Z} \times \mathbb{Z}; +, \sim, (1,0), (0,1) \rangle$.

Proof. The subgroup $\mathbb{Z} \times \{0\}$ admits a positive existential definition in $\mathcal{L}$ since it is the set of (r,s) such that $(r,s) \sim (1,0)$. Similarly, $\{0\} \times \mathbb{Z}$ is positive existential. Also, $\{(a,0),(0,a)\} \in (\mathbb{Z}\times\mathbb{Z})^2$ is positive existential since it is the subset of $(\mathbb{Z}\times\{0\}) \times (\{0\}\times\mathbb{Z})$ determined by $(a,0)+(0,b) \sim (1,1)$.

Consider the bijection $\mathbb{Z} \to \mathbb{Z} \times \{0\}$ sending a to $(a,0)$. Addition in $\mathbb{Z}$ corresponds to addition in $\mathbb{Z} \times \mathbb{Z}$ restricted to $\mathbb{Z} \times \{0\}$. Now, given $a,b,c \in \mathbb{Z}$, we have

$$ab = c \qquad \text{if and only if} \qquad (a,0)+(0,1) \sim (c,0)+(0,b).$$ □

Proof of Theorem 1.4. Combining Corollary 2.4 and Proposition 2.5 shows that there is an effective procedure for taking an instance of Hilbert's tenth problem (over $\mathbb{Z}$) and producing a positive existential sentence in $\langle \mathbb{C}(t_1,t_2); +, \cdot, 0, 1, t_1, t_2 \rangle$ with the corresponding truth value. So if there were an algorithm for the positive existential theory of $\langle \mathbb{C}(t_1,t_2); +, \cdot, 0, 1, t_1, t_2 \rangle$, there would be an algorithm for Hilbert's tenth problem. But there is no algorithm for the latter. □

Remark 2.6. The use of elliptic curves in undecidability proofs originated much earlier, in [Den78], which proved undecidability of polynomial equations over fields such as $\mathbb{R}(t)$.

3. Generalization

Theorem 3.1. [Eis04] *Let* K_1 *be a field that is generated over* $\mathbb{C}$ *by a finite subset* S *of* K_1. *Let* $K_0 = \mathbb{Q}(S) \subset K_1$. *If* $\operatorname{trdeg}(K_1/\mathbb{C}) \geq 2$, *then there is no algorithm that takes as input an arbitrary polynomial* $f \in K_0[x_1,\dots,x_n]$ *and outputs YES or NO according to whether* $f(\vec{x}) = 0$ *is solvable over* K_1.

The proof chooses an embedding $K := \mathbb{C}(t_1, t_2) \hookrightarrow K_1$ and considers $E(L_1)$ where L_1 is a compositum of K_1 and the L used before, but much more work, involving a theorem of Moret-Bailly, is required to ensure that $E(L_1)$ is no larger than $E(L)$. Some care is required also in the proof of Proposition 2.3.

Remark 3.2. The question is open for every finitely generated extension of $\mathbb{C}$ of transcendence degree 1. See [Kol08] for some work related to this question.

References

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR 0133227 (24 #A3061) ↑1.1

[Den78] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399. MR 0491583 (58 #10809) ↑2.6

[Eis04] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over* $\mathbb{C}$, Int. Math. Res. Not. (2004), no. 59, 3191–3205. MR **2097039 (2005h:**11273) ↑3.1

[KR92] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44. MR **1174886 (93h:**03062) ↑1.2

[Kol08] János Kollár, *Diophantine subsets of function fields of curves*, Algebra Number Theory **2** (2008), no. 3, 299–311. MR 2407117 ↑3.2

[Mat70] Yu. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR 0258744 (41 #3390) ↑1.1

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen