AUTOMORPHISMS MAPPING A POINT INTO A SUBVARIETY

BJORN POONEN

(with an appendix by Matthias Aschenbrenner)

Abstract. The problem of deciding, given a complex variety X, a point $x \in X$, and a subvariety $Z \subseteq X$, whether there is an automorphism of X mapping x into Z is proved undecidable. Along the way, we prove the undecidability of a version of Hilbert's tenth problem for systems of polynomials over $\mathbb{Z}$ defining an affine $\mathbb{Q}$-variety whose projective closure is smooth.

1. Introduction

Theorem 1.1. *There is no algorithm that, given a nice complex variety X, a closed point $x \in X$, and a nice subvariety $Z \subseteq X$, decides whether or not there is an automorphism of X mapping x into Z.*

Variety means separated scheme of finite type over a field. Nice means smooth, projective, and geometrically integral (we will eventually apply this adjective also to varieties over fields that are not algebraically closed). Algorithm means Turing machine. So that the input admits a finite description, we assume that the input includes a description of a finitely generated subfield K of $\mathbb{C}$ and that the coefficients of the equations defining X, x, Z are elements of K. More precisely, we assume that we are given $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $\mathbb{Z}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ is a domain with fraction field K, and that elements of K are presented as rational expressions in the generators.

Actually, we show that the problem is undecidable even if X, x, Z are base extensions of $\mathbb{Q}$-varieties. In fact, we prove a strong form of Theorem 1.1:

Theorem 1.2. *There is a* fixed *nice $\mathbb{Q}$-variety X and a fixed rational point x on X such that it is impossible to decide which nice $\mathbb{Q}$-subvarieties Z of X meet $\{\sigma x : \sigma \in \operatorname{Aut} X\}$.*

That is, there is no algorithm that takes Z as input and decides whether there exists an automorphism of X mapping x into Z.

Finally, our X in Theorem 1.2 will have $\operatorname{Aut} X = \operatorname{Aut} X_{\mathbb{C}}$, where $X_{\mathbb{C}}$ is the base extension $X \underset{\operatorname{Spec} \mathbb{Q}}{\times} \operatorname{Spec} \mathbb{C}$, so it does not matter whether we consider only automorphisms defined over $\mathbb{Q}$ or also automorphisms over $\mathbb{C}$.

These problems are proved undecidable by relating them to Hilbert's tenth problem. Hilbert asked for an algorithm to decide, given a multivariable polynomial equation with

Date: July 14, 2009.

2000 *Mathematics Subject Classification.* Primary 14Q20; Secondary 11U05.

Key words and phrases. automorphism, Hilbert's tenth problem, undecidability.

This research was supported by NSF grant DMS-0841321. This article has been published in *J. Alg. Geom.* **20** (2011), 785–794.

integer coefficients, whether or not it was solvable in integers. Matiyasevich [Mat70], building on earlier work of Davis, Putnam, and Robinson [DPR61], proved that no such algorithm exists.

Remark 1.3. If X is a nice variety of general type, the problems above are *decidable* because $\operatorname{Aut} X$ is finite and computable as a subgroup of some PGL_n acting on some pluricanonical image of X.

Remark 1.4. This is not the first time that a problem in algebraic geometry has been proved undecidable. The problem of deciding whether a rational map of complex varieties $X \dashrightarrow \mathbb{P}^2$ admits a rational section is undecidable [KR92] (this is equivalent to the analogue of Hilbert's tenth problem for $\mathbb{C}(T_1, T_2)$). The generalization with $\mathbb{P}^2$ replaced by any fixed complex variety of dimension at least 2 is undecidable too [Eis04]. (But the analogue for $\mathbb{P}^1$ is still open, as is the analogue for any other fixed curve.)

Remark 1.5. Burt Totaro asked the author in 2007 whether the problem of deciding whether two varieties are isomorphic is undecidable.

2. Lattice automorphisms preserving a finite subset

The group of affine linear automorphisms of $\mathbb{Z}^n$ is the semidirect product $\mathrm{GL}_n(\mathbb{Z}) \ltimes \mathbb{Z}^n$, with $(A, \vec{b})$ acting as $\vec{x} \mapsto A\vec{x} + \vec{b}$.

Lemma 2.1. *For each $n \geq 3$, there exists a finite subset S of $\mathbb{Z}^n$ containing $\vec{0} := (0, 0, \ldots, 0)$ such that the subgroup of $\mathrm{GL}_n(\mathbb{Z}) \ltimes \mathbb{Z}^n$ mapping S to S equals the subgroup G of linear maps given by matrices*

$$\begin{pmatrix} 1 & & & & a_1 \\ & 1 & & & a_2 \\ & & \ddots & & \vdots \\ & & & 1 & a_{n-1} \\ & & & & a_n \end{pmatrix}$$

with $a_i \in \mathbb{Z}$ for all i and $a_n = \pm 1$.

Proof. Let p_i be the i^{th} prime. For $1 \leq i \leq n-1$, let $v_i \in \mathbb{Z}^n$ be the vector with p_i in the i^{th} coordinate and 0 elsewhere. Let $S = \{\vec{0}, v_1, \ldots, v_{n-1}\}$. Let G' be the subgroup of $\mathrm{GL}_n(\mathbb{Z}) \ltimes \mathbb{Z}^n$ mapping S to itself. Suppose that $g \in G'$. Then g fixes $\vec{0}$ since each other vector in S differs from some other vector by a primitive vector. Also g fixes v_i for each i, since v_i is distinguished from the other v_j by being divisible by p_i. So g fixes S pointwise. It hence acts trivially on the real affine linear span of S, so it acts trivially on $\mathbb{Z}^{n-1} \times 0$. Thus $G' \subseteq G$. Conversely, elements of G map S to S. So $G' = G$. □

Remark 2.2. In fact, Lemma 2.1 holds for all $n \geq 1$.

3. Blow-ups of powers of an elliptic curve

In this section, we prove a weak version of Theorem 1.1 in which Z is not required to be smooth or integral.

Fix an elliptic curve E over $\mathbb{Q}$ such that $\operatorname{End} E \simeq \mathbb{Z}$ and such that $E(\mathbb{Q})$ contains a point P of infinite order. For instance, E could be the curve labelled 37A1 in [Cre97], with equation $y^2 + y = x^3 - x$, and P could be $(0, 0)$. Let $n \geq 3$. Let X be the blow-up of E^n at the subset

$S' \subset (\mathbb{Z} \cdot P)^n$ corresponding to the subset $S \subset \mathbb{Z}^n$ given by Lemma 2.1. For a variety V, we write $\operatorname{Aut} V$ for the group of automorphisms of V *as a variety without extra structure*, even if V is an abelian variety. The birational morphism $X \to E^n$ is the map from X to its Albanese torsor, so there is an injective homomorphism $\operatorname{Aut} X \to \operatorname{Aut} E^n$ whose image equals the subgroup of $\operatorname{Aut} E^n$ mapping S' to itself. Any such automorphism of E^n must be of the form $\vec{x} \mapsto A\vec{x}+\vec{b}$ for some $A \in \mathrm{GL}_n(\mathbb{Z})$ and $\vec{b} \in E^n$, but $S' \subset (\mathbb{Z}\cdot P)^n$ so $\vec{b} \in (\mathbb{Z}\cdot P)^n$. It follows that $\operatorname{Aut} X$ is isomorphic to the group G in Lemma 2.1. Identify the exceptional divisor D above $\vec{0} \in E^n$ with $\mathbb{P}^{n-1}$ in the natural way. Let $x = (0 : \cdots : 0 : 1) \in \mathbb{P}^{n-1} = D \subseteq X$. If $\sigma \in \operatorname{Aut} X$ corresponds to

$$\begin{pmatrix} 1 & & & & a_1 \\ & 1 & & & a_2 \\ & & \ddots & & \vdots \\ & & & 1 & a_{n-1} \\ & & & & a_n \end{pmatrix} \in G,$$

then $\sigma x = (a_1 : \cdots : a_n) \in \mathbb{P}^{n-1}$.

Given a polynomial $f(t_1, \ldots, t_{n-1}) \in \mathbb{Z}[t_1, \ldots, t_{n-1}]$, let $F(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$ be its homogenization, and let Z be the zero locus of F in $\mathbb{P}^{n-1} = D \subseteq X$. Then f has a zero in $\mathbb{Z}^{n-1}$ if and only if F has a zero in $\mathbb{Z}^{n-1} \times \{\pm 1\}$, which holds if and only if $\sigma x \in Z$ for some $\sigma \in \operatorname{Aut} X$.

Since the general problem of deciding whether a polynomial in $\mathbb{Z}[t_1, \ldots, t_{n-1}]$ has an zero in $\mathbb{Z}^{n-1}$ is undecidable, the general problem of deciding whether $\sigma x \in Z$ for some $\sigma \in \operatorname{Aut} X$ is undecidable too.

4. Making the subvariety smooth

Lemma 4.1. *There is an algorithm that, given a nonconstant $f \in \mathbb{Z}[x_1, \ldots, x_n]$, constructs a polynomial $F \in \mathbb{Z}[x_1, \ldots, x_{n+1}]$ such that*

(i) *The equation $f(\vec{a}) = 0$ has a solution $\vec{a} \in \mathbb{Z}^n$ if and only if $F(\vec{b}) = 0$ has a solution $\vec{b} \in \mathbb{Z}^{n+1}$.*

(ii) *The affine variety $X := \operatorname{Spec} \mathbb{Q}[x_1, \ldots, x_{n+1}]/(F)$ is smooth and geometrically integral.*

(iii) *We have $\deg F = 2 \deg f$. (Here $\deg$ denotes total degree.)*

Proof. Consider $F(x_1, \ldots, x_n, y) = c(y^2 - y) + f(x_1, \ldots, x_n)^2$ for some $c \in \mathbb{Z}_{>0}$. The values of $y^2 - y$ and $f(x_1, \ldots, x_n)^2$ on integer inputs are nonnegative, so (i) is satisfied. The singular locus S of X is contained in the locus where $\partial F/\partial y = 0$, which is $2y - 1 = 0$ in $\mathbb{A}^N$. On the other hand, Bertini's theorem ([Har77, Remark III.10.9.2]) shows that S is contained in $y^2 - y = 0$ for all but finitely many c. In this case $S = \emptyset$, so X is smooth over $\mathbb{Q}$. By testing $c = 1, 2, \ldots$ in turn, we can effectively find the first c for which X is smooth over $\mathbb{Q}$.

This X is also geometrically integral: since X is isomorphic to a variety of the form $z^2 - g = 0$ for some nonconstant $g \in \mathbb{Z}[x_1, \ldots, x_n]$, if it were not geometrically integral, $z^2 - g$ would factor as $(z + h)(z - h)$ for some nonconstant $h \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$, but then X would have to be singular at the common zeros of z and h, a contradiction. □

Lemma 4.2. *There is an algorithm that, given an affine scheme U of finite type over $\mathbb{Z}$ whose generic fiber $U_{\mathbb{Q}}$ is smooth over $\mathbb{Q}$, constructs $N \in \mathbb{Z}_{>0}$ and a closed immersion $U \hookrightarrow \mathbb{A}^N_{\mathbb{Z}}$*

such that the projective closure of the generic fiber $U_{\mathbb{Q}}$ in $\mathbb{P}^N_{\mathbb{Q}}$ is smooth. Moreover, N can be bounded in terms of the degree and number of variables of the equations defining U.

Proof. Embed U as a closed subscheme of some $\mathbb{A}^m_{\mathbb{Z}}$. Identify $\mathbb{A}^m_{\mathbb{Z}}$ with the locus in $\mathbb{P}^m_{\mathbb{Z}} = \operatorname{Proj} \mathbb{Z}[x_0, \dots, x_m]$ where $x_0 \neq 0$. Let X be the closure of U in $\mathbb{P}^m_{\mathbb{Z}}$. Let $H = X - U$.

Effective resolution of singularities [Vil89, Vil92, BM91, BM97, BS00] lets us construct a coherent sheaf of ideals $\mathcal{I}_{\mathbb{Q}}$ on $X_{\mathbb{Q}}$ with support contained in $H_{\mathbb{Q}}$ such that blowing up $X_{\mathbb{Q}}$ along $\mathcal{I}_{\mathbb{Q}}$ yields a smooth $\mathbb{Q}$-scheme. Moreover, resolution of singularities has computably bounded complexity as one varies the variety in an algebraic family, by noetherian induction: namely, reduce to the case of an irreducible base B, compute the blow-ups needed to resolve the generic fiber, examine the denominators in the rational functions on B that arise in the coefficients, define the open subscheme V of B on which these denominators are invertible so that the same sequence of blow-ups specializes to give a resolution for any fiber above a point of V, and finally apply the inductive hypothesis to the family over $B - V$, which has lower dimension. Therefore the degrees of the homogeneous polynomials that locally generate $\mathcal{I}_{\mathbb{Q}}$ can be bounded (in terms of the degree and number of variables of the equations defining U). Let $I_{\mathbb{Q}}$ be the homogeneous ideal of $\mathbb{Q}[x_0, \dots, x_m]$ generated by these polynomials. Since the support of $\mathcal{I}_{\mathbb{Q}}$ is contained in $H_{\mathbb{Q}}$, the Nullstellensatz shows that there is a positive integer r such that $x_0^r \in I_{\mathbb{Q}}$. By noetherian induction again, r is bounded. We have $x_0^r \in I$.

By the appendix to this article, we can compute $I := I_{\mathbb{Q}} \cap \mathbb{Z}[x_0, \dots, x_m]$. Moreover, the degrees of the generators of I can be bounded in terms of those of $I_{\mathbb{Q}}$, as explained in the remarks at the end of the appendix. Choose d larger than all these degrees and larger than r. Blowing up the coherent sheaf of ideals on X defined by I yields $X' \xrightarrow{\pi} X$ with $X'_{\mathbb{Q}}$ smooth over $\mathbb{Q}$. Let E be the exceptional divisor on X'.

A basis for the degree-d part I_d of I determines a projective embedding of X' in some $\mathbb{P}^N_{\mathbb{Z}}$ (cf. the proofs of [Har77, II.7.10(b) and II.7.16(c)]), and N is bounded. We have $x_0^d \in I_d$, and the corresponding hyperplane section of X' is the Cartier divisor $d\pi^*H - E$, which has the same support as π^*H, since $d > r$. Let $\mathbb{A}^N_{\mathbb{Z}}$ be the complement in $\mathbb{P}^N_{\mathbb{Z}}$ of the hyperplane defined by the coordinate corresponding to $x_0^d \in I_d$. Then $X' \cap \mathbb{A}^N_{\mathbb{Z}} = X' - \pi^{-1}(H) = \pi^{-1}(U) \simeq U$. In other words, U is isomorphic to a closed subscheme of $\mathbb{A}^N_{\mathbb{Z}}$ whose projective closure is X', and the generic fiber $X'_{\mathbb{Q}}$ of X' is smooth. □

Combining the previous two lemmas with the negative solution to Hilbert's tenth problem yields:

Corollary 4.3. *There is no algorithm that, given $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ such that the projective closure of* $\operatorname{Spec} \mathbb{Q}[x_1, \dots, x_n]/(f_1, \dots, f_m)$ *in $\mathbb{P}^n_{\mathbb{Q}}$ is smooth and geometrically integral over $\mathbb{Q}$, decides whether $f_1(\vec{a}) = \cdots = f_m(\vec{a}) = 0$ has a solution $\vec{a} \in \mathbb{Z}^n$.*

Applying the construction of Section 3 to the smooth projective geometrically integral $\mathbb{Q}$-variety Z arising as the projective closure in Corollary 4.3 proves Theorem 1.1.

5. Uniformity

In this section we prove Theorem 1.2. In our proof of Theorem 1.1, the variety X and the point x depend only on the integer n chosen at the beginning of Section 3.

The negative solution of Hilbert's tenth problem shows that there are fixed m and d such that the problem of deciding whether an m-variable polynomial of total degree d is solvable in natural numbers is undecidable [Mat70]. Replacing each variable by a sum of squares of four new variables and applying Lagrange's theorem that every nonnegative integer is a sum of four squares shows that the same uniform undecidability holds for solvability in integers, provided that we replace (m, d) by $(4m, 2d)$. Combining this with Lemma 4.1 yields undecidability even if we restrict to polynomials defining a smooth affine hypersurface over $\mathbb{Q}$, provided that we replace (m, d) by $(m + 1, 2d)$. Lemma 4.2 re-embeds these hypersurfaces in a projective space of bounded dimension, which can then be embedded in a larger projective space of *fixed* dimension D. Finally we may take $n = D + 1$ in Section 3. This completes the proof of Theorem 1.2.

Acknowledgements

It was a discussion with Burt Totaro that inspired the research leading to this article. I thank Andrew Kresch, Florian Pop, and Yuri Tschinkel for a teatime discussion at the Hausdorff Institute for Mathematics that led to an outline of the proof of Lemma 4.2. I thank Matthias Aschenbrenner for permission to include his appendix. Finally, I thank Steven Dale Cutkosky, David Eisenbud, Herwig Hauser, and Laurent Moret-Bailly for suggestions regarding references.

References

[BM91] Edward Bierstone and Pierre D. Milman, *A simple constructive proof of canonical resolution of singularities*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 11–30. MR1106412 (92h:32053) ↑4

[BM97] ———, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Invent. Math. **128** (1997), no. 2, 207–302. MR1440306 (98e:14010) ↑4

[BS00] Gábor Bodnár and Josef Schicho, *Automated resolution of singularities for hypersurfaces*, J. Symbolic Comput. **30** (2000), no. 4, 401–428. MR1784750 (2001i:14083) ↑4

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068) ↑3

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR0133227 (24 #A3061) ↑1

[Eis04] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over* $\mathbb{C}$, Int. Math. Res. Not. **59** (2004), 3191–3205. MR2097039 (2005h:11273) ↑1.4

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116) ↑4, 4

[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. MR1174886 (93h:03062) ↑1.4

[Mat70] Yu. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR0258744 (41 #3390) ↑1, 5

[Vil89] Orlando Villamayor, *Constructiveness of Hironaka's resolution*, Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 1, 1–32. MR985852 (90b:14014) ↑4

[Vil92] O. E. Villamayor U., *Patching local uniformizations*, Ann. Sci. École Norm. Sup. (4) **25** (1992), no. 6, 629–677. MR1198092 (93m:14012) ↑4

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