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 $\{\alpha x : \alpha \in \operatorname{Aut} X\}$.

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 $X \times_{\operatorname{Spec} \mathbb{Q}} \operatorname{Spec} \mathbb{C}$, 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: February 22, 2011.

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

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

M. A. and B. P. were partially supported by NSF grants DMS-0556197 and DMS-0841321, respectively.

This article has been published in J. Alg. Geom. 20 (2011), 785–794.

Remarks. Algorithm 1 seems better suited for practical computations. However, unlike in the case of fields, the precise worst-case behavior of the analogue of Buchberger's algorithm for computing Gröbner bases over $\mathsf{Z}[X]$ is as of yet still unclear. (For very weak bounds see [GM94], and for further discussion the forthcoming [Asc09].) Algorithm 2 has the advantage of coming with explicit (doubly-exponential) complexity bounds: for example, suppose $d \in \mathsf{N}$ is an upper bound on the (total) degree of f_i for $i = 1, \ldots, n$; then $I\mathsf{Q}[X] \cap \mathsf{Z}[X] = (g_1, \ldots, g_m)$ where $\deg(g_j) \leq (2d)^{2^{N \log(N+1)}}$ for $j = 1, \ldots, m$, cf. [Asc04, Theorem B]. (Note that this bound only depends on the bound d on the degrees and not on the particular coefficients of the f_i.)

In connection with (P1), we remark that the *smallest* positive integer δ such that $(I : \delta) = I\mathsf{Q}[X] \cap \mathsf{Z}[X]$ agrees with the exponent of the torsion subgroup of the additive group of $\mathsf{Z}[X]/I$. (The torsion subgroup of the additive group of a Noetherian ring always has finite exponent.) The algorithms indicated above, together with a procedure for deciding equality of ideals in $\mathsf{Z}[X]$ (found in [GTZ88, Asc04]), give rise to a procedure for computing this exponent in an obvious way; another algorithm was given by Clivio [Cli90] (based on earlier work of Ayoub [Ayo83]).

References

[AL94] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994. MR1287608 (95g:13025) ↑5, 1, 2, 5

[Asc04] Matthias Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. (2004), no. 2, 407–441 (electronic). MR2051617 (2005c:13032) ↑5, 5

[Asc09] ———, *Uniform degree bounds for Gröbner bases*, 2009. In preparation. ↑5

[Ayo83] Christine W. Ayoub, *On constructing bases for ideals in polynomial rings over the integers*, J. Number Theory (1983), no. 2, 204–225, DOI 10.1016/0022-314X(83)90021-5. MR716943 (85m:13017) ↑5

[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. (1997), no. 2, 207–302. MR1440306 (98e:14010) ↑4

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

[Cli90] A. Clivio, *Algorithmic aspects of* $[x_1, \cdots, x_n]$ *with applications to tiling problems*, Z. Math. Logik Grundlag. Math. (1990), no. 6, 493–515. MR1114102 (92j:13024) ↑5

[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) (1961), 425–436. MR0133227 (24 #A3061) ↑1

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

[GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. (1988), no. 2-3, 149–167. Computational aspects of commutative algebra. MR988410 (90f:68091) ↑5, 5, 5

[GM94] Giovanni Gallo and Bhubaneswar Mishra, *A solution to Kronecker's problem*, Appl. Algebra Engrg. Comm. Comput. (1994), no. 6, 343–370, DOI 10.1007/BF01188747. MR1302282 (95i:13026) ↑5

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

[Her26] Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. (1926), no. 1, 736–788, DOI 10.1007/BF01206635 (German). MR1512302 ↑5

[KR92] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathsf{C}(t_1, t_2)$, J. Algebra (1992), no. 1, 35–44. MR1174886 (93h:03062) ↑1.4

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

[Vas97] Wolmer V. Vasconcelos, *Flatness testing and torsionfree morphisms*, J. Pure Appl. Algebra (1997), no. 3, 313–321, DOI 10.1016/S0022-4049(97)00062-5. MR1481094 (98i:13013) ↑1

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

[Vil92] O. E. Villamayor U., *Patching local uniformizations*, Ann. Sci. École Norm. Sup. (4) (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`