On Defining Irreducibility

Pascal Koiran
Laboratoire de l'Informatique du Parallélisme
Ecole Normale Supérieure de Lyon – CNRS
46, allée d'Italie
69364 Lyon Cedex 07, France
Pascal.Koiran@ens-lyon.fr
http://www.ens-lyon.fr/~koiran

February 8, 2000

Abstract

We show that for real algebraic varieties, irreducibility is not a first-order definable property. This result holds in any real closed field; its proof is based on the o-minimality of the real exponential field.

1 Irreducibility of Real Algebraic Varieties

Let us recall that for any field F, an algebraic variety of F^p is the intersection of the zero sets of a finite family of polynomials of $F[x_1, \ldots, x_p]$. If $P_1, \ldots, P_k$ is such a family, we denote by $V_F(P_1, \ldots, P_k)$ the corresponding variety. Of course, if F is real closed any variety can be defined by a single polynomial.

An algebraic variety V of F^p is said to be irreducible if it cannot be written as the union of two algebraic varieties V_1 and V_2 of F^p where V_1 and V_2 are strict subsets of V. In this paper we prove the following result.

Theorem 1 *For any $p \geq 2$, irreducibility is not a definable property of algebraic varieties of $\mathbb{R}^p$.*

This means that for all $p \geq 2$, there exists no first-order sentence F_p in the language $\mathcal{L}_p = (+, -, \times, =, 0, 1, I_p)$ satisfying the following property: for any algebraic variety V of $\mathbb{R}^p$, if we interpret the p-ary predicate I_p by membership to V then $\mathbb{R} \models F_p$ if and only if V is irreducible. Our proof will imply that irreducibility remains undefinable even if we add the exponential function to $\mathcal{L}_p$. It was inspired by Wilkie's proof that C^∞ functions are not definable [10].

There is a growing body of work on definability in o-minimal and stable structures (mostly concerned with properties of "finite embedded models", see for instance [1, 2, 3, 4, 5, 8]). A study of definability in algebraically closed fields was initiated in [7]: in that paper we gave some examples of definable properties (for instance, dimension is definable), showed that connectivity of algebraic varieties is not definable, and conjectured that algebraic varieties are not definable among constructible sets (note however that for the Euclidean topology, closed subsets of $\mathbb{R}^p$ are definable by an obvious formula of $\mathcal{L}_p$). This conjecture was very recently proved in [6] (its counterpart for the field of real numbers is also true: see Theorem 2 at the end of this section). It is shown in the same paper that the counterpart of Theorem 1 for algebraically closed fields is also true (i.e., irreducible varieties are not definable). More generally, one can ask whether there exists an infinite field F such that irreducible varieties of F^p are definable, for some $p \geq 2$.

Like the proof of Theorem 1, the proofs of these two results from [6] rely heavily on the properties of a suitable complete theory. They are much more involved, however, because we had to construct a theory tailored to our needs: the limit of the theories of generic curves. In the present paper we use an "off the rack" theory: the theory of the reals with exponentiation.

Let V_n be the real variety $\{(x, y) \in \mathbb{R}^2;\ P_n(x, y) = 0\}$ where

$$P_n(x, y) = x^{2n} - (1 + y^2)^2.$$

Note that $P_n = Q_n R_n$ with $Q_n(x, y) = x^n - 1 - y^2$ and $R_n(x, y) = x^n + 1 + y^2$. Note also that there is a formula $F(n, x, y)$ of the language

$$\mathcal{L}_{\exp} = \{+, -, \times, =, \exp, 0, 1\}$$

such that whenever n is a positive integer, $F(n, ., .)$ defines V_n: take for F the formula

$$\exists z[e^z = x^2 \wedge e^{nz} = (1 + y^2)^2].$$

Here is another useful remark.

Lemma 1 *For any integer $n \geq 0$, the real variety $V_{\mathbb{R}}(Q_n)$ defined by Q_n is irreducible.*

Proof. For $n = 0$, $V_{\mathbb{R}}(Q_n)$ is the line $\{y = 0\}$ and is therefore irreducible. For $n \geq 1$, $V_{\mathbb{R}}(Q_n)$ also has dimension 1 and it is not hard to check that Q_n is irreducible over $\mathbb{C}$. It therefore follows from Lemma 2 below that $V_{\mathbb{R}}(Q_n)$ is irreducible. □

Lemma 2 *Let $Q \in \mathbb{R}[x, y]$ be a polynomial defining a real variety $V_{\mathbb{R}}(Q)$ of dimension 1. If Q is irreducible over $\mathbb{C}$ then $V_{\mathbb{R}}(Q)$ is irreducible.*

Proof. Let V_1 and V_2 be two real varieties such that $V_{\mathbb{R}}(Q) = V_1 \cup V_2$. We shall see that $V_1 = V_{\mathbb{R}}(Q)$ or $V_2 = V_{\mathbb{R}}(Q)$. At least one of the V_i must be of dimension 1. Assume for instance that this is true of V_1, and let $P_1 \in \mathbb{R}[x, y]$ be a polynomial such that $V_1 = V_{\mathbb{R}}(P_1)$. Since $V_{\mathbb{R}}(P_1, Q)$ has dimension 1, the complex variety $V_{\mathbb{C}}(P_1, Q)$ also has dimension 1. By irreducibility of Q, $V_{\mathbb{C}}(Q)$ is irreducible. It follows that $V_{\mathbb{C}}(Q) \subseteq V_{\mathbb{C}}(P_1)$ and therefore $V_{\mathbb{R}}(Q) \subseteq V_{\mathbb{R}}(P_1)$, i.e., $V_{\mathbb{R}}(P_1) = V_{\mathbb{R}}(Q)$. □

A generalization of this lemma is given in Lemma 4.

Proposition 1 *V_n is irreducible if and only if n is even.*

Proof. If n is an odd number, the real varieties defined by Q_n and R_n are distinct (they are in fact disjoint). Hence V_n is not irreducible in this case.

If n is even, R_n has no real zeros. V_n is therefore irreducible by Lemma 1. $\square$

Proof of Theorem 1. We shall prove that irreducibility is not definable in dimension 2. The result for higher dimensions follows immediately from this special case.

Assume by contradiction that there exists a formula F of $\mathcal{L}_2$ such that for any real variety V of $\mathbb{R}^2$, if we interpret I_2 by membership to V then $\mathbb{R} \models F$ if and only if V is irreducible. Let $G(n)$ be the formula obtained from F by replacing each instance $I_2(x, y)$ of I_2 in F by $F(n, x, y)$. By Proposition 1, $G(n)$ is true whenever n is an even integer, and is false whenever $G(n)$ is an odd integer. This is in contradiction with the o-minimality of the real exponential field (see [11] and the references there). $\square$

A similar argument yields the following result.

Theorem 2 *For any $p \geq 2$, algebraic varieties of $\mathbb{R}^p$ are not characterized among semi-algebraic sets by a formula of $\mathcal{L}_p$.*

The proof is even simpler than the proof of Theorem 1. Instead of V_n we consider the family of semi-algebraic sets S_n of $\mathbb{R}^2$ defined by the equation $y = |x|^n$ (this is very similar to Wilkie's example [10]). For any integer n, S_n is an algebraic variety if and only if n is even.

2 Irreducibility in Real Closed Fields

The proof of Theorem 1 clearly shows that irreducibility remains undefinable even if we allow arbitrary real parameters in F_p. This is in fact true for any real closed field R. More precisely, denote by $\mathcal{L}_p^R$ the expansion of $\mathcal{L}_p$ obtained by adding one constant symbol for each element of R. We then have the following generalization of Theorem 1.

Theorem 3 *Let R be a real-closed field and $p \geq 2$ an integer. Irreducibility of algebraic varieties of R^p cannot be defined by a sentence of $\mathcal{L}_p^R$.*

Before proving Theorem 3, we point out in Proposition 2 that irreducibility *is* definable if we restrict our attention to polynomials of fixed degree (in the terminology of [7], one would say that "irreducibility is locally definable without parameters").

Lemma 3 *Let P and Q be two nonconstant polynomials of $F[x, y]$ where F is an arbitrary field. If P and Q are relatively prime then $V_F(P, Q)$ is finite.*

Proof. Let K be the algebraic closure of F. If P and Q are relatively prime in $F[x, y]$ then they are also relatively prime in $K[x, y]$ (this follows from the fact that for any two polynomials in $F[x, y]$, their greatest common divisor in $K[x, y]$ is an element of $F[x, y]$, up to a constant multiplicative factor). Let us therefore assume that P and Q are relatively prime in $K[x,y]$. Let $P_1,\ldots,P_k$ be the prime factors of P in $K[x,y]$. We claim that $V_K(P_i,Q)$ is finite for any $i\in\{1,\ldots,k\}$. Assume by contradiction that $V_K(P_i,Q)$ is infinite. Since $V_K(P_i)$ is irreducible this implies that $V_K(P_i)=V_K(P_i,Q)$, i.e., that Q vanishes on $V_K(P_i)$. This implies that P_i divides a power of Q, and therefore that P_i divides Q since P_i is irreducible. This is in contradiction with the hypothesis that P and Q are relatively prime, and completes the proof of the claim. We conclude that $V_K(P,Q)$, and therefore $V_F(P,Q)$, is finite. □

Lemma 4 *Let F be an arbitrary field and $V_F(P)\subseteq F^2$ an algebraic variety of infinite cardinality. If P is irreducible in $F[x,y]$ then $V_F(P)$ is irreducible.*

Proof. Let $W=V_F(P_1,\ldots,P_k)$ and $W'=V_F(P'_1,\ldots,P'_l)$ be two varieties whose union is equal to V. We shall see that $V=W$ or $V=W'$. Assume for instance that W is infinite. Since $W=\bigcap_{1\leq i\leq k}V_F(P,P_i)$ the varieties $V_F(P,P_i)$ are all infinite. Since P is irreducible, this implies by Lemma 3 that all the P_i's are multiples of P. Therefore $V\subseteq W$, and in fact $V=W$. If W' is infinite the same reasoning shows that $V=W'$. □

Proposition 2 *Let F be an arbitrary field.*

(i) If a polynomial $P\in F[x,y]$ of degree d defines a reducible variety $V_F(P)$ of infinite cardinality, there exist two polynomials $P_1,P_2\in F[x,y]$ of degree at most d such that $V_F(P_1)$ and $V_F(P_2)$ are strict subsets of $V_F(P)$ whose union is equal to $V_F(P)$.

Moreover, the following proposition holds if F is real closed.

(ii) The set X_d of coefficients of a polynomial $Q\in F[x,y]$ of degree $\leq d$ such that $V_F(Q)$ is irreducible is a semi-algebraic subset of $F^{(d+1)(d+2)/2}$. This set can be defined by the same parameter-free formula of the language of ordered rings in all real closed fields.

Proof. The proof of assertion (i) is by induction on d. There is nothing to prove for $d\leq 1$ since $V_F(P)$ is always irreducible in this case. Assume now that $d\geq 2$ and that the result is true for all polynomials of degree at most $d-1$. If $V_F(P)$ is infinite and reducible, P can be written as the product of two nonconstant polynomials P_1 and P_2 of $F[x,y]$ by Lemma 4. If $V_F(P)\neq V_F(P_1)$ and $V_F(P)\neq V_F(P_2)$ we are done since these polynomials are of degree $<d$. If $V_F(P)=V_F(P_1)$, the result follows from the induction hypothesis applied to P_1. The case $V_F(P)=V_F(P_2)$ is identical.

Assertion (ii) follows from (i) and quantifier elimination: $V_F(Q)$ is reducible iff this variety is finite of cardinality at least two, or if there exist two polynomials $Q_1,Q_2\in F[x,y]$ of degree at most d such that $V_F(Q_1)$ and $V_F(Q_2)$ are strict subsets of $V_F(Q)$ whose union is equal to $V_F(Q)$. Finiteness of $V_F(Q)$ is easily expressed by a first-order formula: state for instance that all points of $V_F(Q)$ are isolated. □

It is in fact known [9, 2.10.v] that there exists a (presumably very fast growing) function $B(p,d)$ such that for any field F and any variety V of F^p defined by polynomial equations of degree at most d, the irreducible components of V can be defined by polynomial equations of degree at most $B(p,d)$.

Corollary 1 *Let R be a real closed field. If irreducibility of algebraic varieties of R^2 was definable by a formula of $\mathcal{L}_2^R$, this formula would define irreducibility of algebraic varieties of R'^2 for any real closed field R' containing R.*

Proof. This follows from Proposition 2.(ii) and the fact that R' is an elementary extension of R. □

Proof of Theorem 3. As in the proof of Theorem 1, it is sufficient to prove the theorem for $p = 2$. The proof of that theorem clearly applies to any model of theory of the reals with exponentiation. Corollary 1 then yields a contradiction, if we take for R' any model of this theory containing R. □

One can also avoid Proposition 2 in the proof of this theorem by recycling the proof of Theorem 1: assume that irreducibility of algebraic varieties of R^2 is defined by a sentence F of $\mathcal{L}_2^R$. Replacing each instance of $I_2(x,y)$ in F by $P_n(x,y) = 0$, we obtain a sentence G_n of the language of rings (with parameters in R) which is true if and only if the integer n is even. In R', these sentences must also be true for the same values of n. However, G_n is equivalent in R' to a formula $G(n)$ of $\mathcal{L}_{exp}$ (with parameters in R). We therefore obtain the same contradiction as in the proof of Theorem 1.

References

[1] J. T. Baldwin and M. Benedikt. Embedded finite models, stability theory, and the impact of order. In *Proc. 13th IEEE Symposium on Logic in Computer Science*, pages 490–500, 1998.

[2] O. V. Belegradek, A. Stolboushkin, and M. A. Taitslin. Extended order-generic queries. *Annals of Pure and Applied Logic*, 97:85–125, 1999.

[3] M. Benedikt, G. Dong, L. Libkin, and L. Wong. Relational expressive power of constraint query languages. *Journal of the ACM*, pages 1–34, 1998.

[4] M. Benedikt and L. Libkin. On the structure of queries in constraint query languages. In *Proc. 11th IEEE Symposium on Logic in Computer Science*, pages 25–34, 1996.

[5] M. Benedikt and L. Libkin. Languages for relational databases over interpreted structures. In *Proc. 16th ACM Symposium on Principles of Database Systems*, pages 87–98, 1997.

[6] O. Chapuis, E. Hrushovski, P. Koiran, et B. Poizat. La limite des théories de courbes génériques. To appear in *Journal of Symbolic Logic*.

[7] O. Chapuis and P. Koiran. Definability of geometric properties in algebraically closed fields. *Mathematical Logic Quarterly*, 45(4):533-550, 1999.

[8] S. Grumbach and J. Su. Queries with arithmetical constraints. *Theoretical Computer Science*, 173:151–181, 1997.

[9] L. van den Dries and K. Schmidt. Bounds in the theory of polynomials rings over fields. A nonstandard approach. *Inventiones Mathematicae*, 76:77–91, 1984.

[10] A. J. Wilkie. On defining C^∞. *Journal of Symbolic Logic*, 59(1):344, 1994.

[11] A. J. Wilkie. O-minimality. *Documenta Mathematica*, I:633–636, 1998. http://www.mathematik.uni-bielefeld.de/documenta, Extra Volume ICM 1998.