Laboratoire de l'Informatique du Parallélisme

École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON n° 5668

The Limit Theory of Generic Polynomials

Pascal Koiran

September 2001

Research Report N° 2001-35

École Normale Supérieure de Lyon
46 Allée d'Italie, 69364 Lyon Cedex 07, France
Téléphone : +33(0)4.72.72.80.37
Télécopieur : +33(0)4.72.72.80.80
Adresse électronique : `lip@ens-lyon.fr`

The Limit Theory of Generic Polynomials

Pascal Koiran

September 2001

Abstract

We show that the set T of first-order sentences satisfied by all generic polynomials of sufficiently high degree forms a complete theory. As a consequence, complex polynomials of even degree cannot be distinguished from complex polynomials of odd degree by a first-order formula. We ask whether T has an analytic model.

Keywords: model theory, definability, intersection.

Résumé

On montre que l'ensemble T des énoncés du premier ordre satisfaits par tous les polynômes génériques de degré suffisament grand forme une théorie complète. Il en résulte que les polynômes complexes de degré pair ne peuvent pas être distingués de ceux de degré impair par une formule du premier ordre. Nous demandons si T admet un modèle analytique.

Mots-clés: théorie des modèles, définissabilité, intersection.

The Limit Theory of Generic Polynomials

Pascal Koiran

28th September 2001

Abstract

We show that the set T of first-order sentences satisfied by all generic polynomials of sufficiently high degree forms a complete theory. As a consequence, complex polynomials of even degree cannot be distinguished from complex polynomials of odd degree by a first-order formula. We ask whether T has an analytic model.

Keywords: model theory, definability, intersection.

1 Introduction

A generic polynomial is a polynomial $f : \mathbb{C} \rightarrow \mathbb{C}$ of the form

$$f(x) = c_1 x + \cdots + c_d x^d$$

where the coefficients $c_1, \ldots, c_d$ are algebraically independent over $\mathbb{Q}$. One could work in the language of fields expanded with a unary function symbol f. Here we prefer to work in the language of "curved fields": the language of fields expanded with a binary predicate C (which stands for $y = f(x)$). This choice emphasizes the connection with generic curves [2, 4] and turns out to be more convenient for the explicit construction of a model by an amalgamation method à la Hrushovski (see [7] for a survey on this topic).

In this paper we show that the parity of the degree of complex polynomials is not definable. This means that there does not exist a first-order sentence F of the language of curved fields such that:

(i) F is true in $\mathbb{C}$ whenever C is interpreted by the graph of a polynomial of even degree.

(ii) F is false in $\mathbb{C}$ whenever C is interpreted by the graph of a polynomial of odd degree.

Note that the parity of the degree of *real* polynomials is definable. This follows from the fact that a real polynomial is of odd degree if and only if it has different limits at $\pm\infty$ (more on this in section 2).

Our undefinability result follows immediately from the following main result: a sentence of the language of curved fields is either true for all generic polynomials of sufficiently high degree or false for all generic polynomials of sufficiently high degree. The set T of sentences which are true for all generic polynomials of sufficiently high degree therefore forms a consistent and complete theory: the "limit theory of generic polynomials".

Starting from somewhat different motivations, Zilber has independently constructed a related theory [11]. He works in a richer language with countably many binary predicates, which are to be thought of as the graphs of the higher order derivatives of the original function.

In section 3 we give an axiomatization of a theory which is shown to be consistent and (more crucially) complete. It will turn out in section 4 that this theory really is the limit theory of generic polynomials.

By elementary equivalence the above results apply not only to the field of complex numbers but to any algebraically closed field of characteristic 0. They seem quite likely to hold also in positive characteristic (this is definitely true for the consistence and completeness results of section 3).

One could naively imagine that generic polynomials are easier to understand than generic curves. Even though the results and the general proof strategy are similar, the opposite is true: the axiomatization is slightly more complicated for generic polynomials, and it is significantly more difficult to show that the axioms are satisfied when the degree is sufficiently high. The proof given in section 4 relies on the intersection theorems of section 5 and of [5].

An intriguing open question is whether the limit theory of generic polynomials admits an analytic model (more on this in section 6). Wilkie's Liouville functions [10] are plausible candidates. Some partial results in this direction are already contained in [10].

2 Case of the Real Field

We have just seen that the set of real polynomials of even degree is definable. Given $p \geq 3$, is it also possible to define the set of real polynomials whose degree is a multiple of p ? It turns out that the answer to this question is negative.

Proposition 1 *Let $p \geq 3$ be an integer. There exists no sentence F of the language of curved fields such that when the curve C is interpreted by the graph of a degree d polynomial, $(\mathbb{R}, C) \models F$ if and only if d is a multiple of p.*

Proof. Assume by contradiction that such a sentence exists for some even integer $p \geq 4$. Write $p = 2q$. When we interpret C by the graph of the polynomial $y = x^{2n}$, $(\mathbb{R}, C) \models F$ if and only if n is a multiple of q. Let $G(n, x, y)$ be the following formula of language of the real exponential field:

$$(x = 0 \wedge y = 0) \vee \exists z\ (\exp(z) = x^2 \wedge y = \exp(nz)).$$

When n is an integer, $G(n, ., .)$ defines the graph of the polynomial $y = x^{2n}$. Let $H(n)$ be the formula of the real exponential field obtained from F by replacing each instance $C(x, y)$ of C by $G(n, x, y)$. This formula should be true whenever the integer n is a multiple of q, and false otherwise. This is impossible for $q \geq 2$ since the real exponential field is o-minimal [9].

Assume now that $p \geq 3$ is an odd integer, and that it is possible to define the set of real polynomials of degree multiple of p. Since the set of real polynomials of even degree is definable, one could also define the set of real polynomials of degree multiple of $2p$. We have just shown that this is impossible. □

Several other undefinability results can be obtained by the same o-minimality argument [3, 8]. Unfortunately, for algebraically closed fields we do not know any theory which could play the same "universal" role. More ad-hoc constructions are therefore necessary. The limit theory of generic curves is a tool which makes it possible to obtain several undefinability results for algebraic curves [2]. The theory constructed and studied in the rest of this paper plays a similar role for definability problems involving polynomials over an algebraically closed field of characteristic 0.

3 Construction of the Limit Theory

In this section we work in an algebraically closed field K of arbitrary characteristic. We denote by Q the prime field of K. Given n elements $x_1, \ldots, x_n$ of a model, we denote the tuple $(x_1, \ldots, x_n)$ by x. When there is a risk of confusion between tuples and elements we may also write $\overline{x}$ instead of x.

We consider the theory T defined by the following axioms.

1. The axioms of algebraically closed fields of a fixed characteristic.

2. The functional axiom
$$\forall x, y_1, y_2 \; C(x, y_1) \wedge C(x, y_2) \rightarrow y_1 = y_2.$$

3. The function is everywhere defined: $\forall x \exists y C(x, y)$.

4. $C(0, 0)$.

5. The universal axioms. Let $\phi(x_1, y_1, \ldots, x_n, y_n)$ be a conjunction of polynomial equations with coefficients in the prime field. If the subset of K^{2n} defined by ϕ is of dimension $< n$, we add the axiom
$$\forall x_1, y_1, \ldots, x_n, y_n \; A(x_1, y_1, \ldots, x_n, y_n) \rightarrow \neg\phi(\overline{x}, \overline{y}) \tag{1}$$
where $A(x_1, y_1, \ldots, x_n, y_n)$ stands for
$$\bigwedge_{i \neq j} (x_i, y_i) \neq (x_j, y_j) \wedge \bigwedge_{i=1}^{n} x_i \neq 0 \wedge \bigwedge_{i=1}^{n} C(x_i, y_i)$$
Instead of these axioms, one could also use an equivalent set of universal axioms in the style of [2].

6. The inductive axioms. Let $\phi(x_1, y_1, \ldots, x_n, y_n, \overline{z})$ be a conjunction of polynomial equations with coefficients in the prime field. For any fixed value of the parameter $\overline{z}$, ϕ defines an algebraic subset $V_{\overline{z}}$ of K^{2n}. Let $\xi(\overline{z})$ be a formula of the language of fields which states that $V_{\overline{z}}$ is irreducible

and is not contained in a subspace of the form $x_i = x_j$ for some $i \neq j$, or of the form $x_i = c$ for some element c in the model.

Let ϵ be a function which chooses one variable $u_i^\epsilon \in \{x_i, y_i\}$ for every $i \in \{1, \ldots, n\}$. For each value of the parameter $\overline{z}$, the formula $\exists u_1^\epsilon, \ldots, u_n^\epsilon \phi(\overline{x}, \overline{y}, \overline{z})$ defines a constructible set $C_{\overline{z}}^\epsilon \subseteq K^n$. As pointed out in [2], there is a formula $\psi_\epsilon(\overline{z})$ of the language of fields which states that $C_{\overline{z}}^\epsilon$ is dense in K^n. Let $\psi(\overline{z})$ be the disjunction of the 2^n formulas $\psi_\epsilon(\overline{z})$. Let θ be the conjunction of ξ and ψ. We add the following axiom:

$$\forall \overline{z}\ \exists x_1, y_1, \ldots, x_n, y_n\ \theta(\overline{z}) \rightarrow \bigwedge_{i=1}^{n} C(x_i, y_i) \wedge \phi(\overline{x}, \overline{y}, \overline{z}). \tag{2}$$

3.1 Consistence

The consistence of T follows from the results of section 4. In this subsection we give a simpler and more direct proof. We shall construct a model K of T which is the union of an increasing sequence of "curved fields" K_i. Each K_i is an algebraically closed field of finite transcendence degree endowed with a "curve" C_i made up of finitely many points. We start from $K_0 = \overline{Q}$ with the curve $C_0 = \{(0, 0)\}$. One goes from K_i to K_{i+1} by application of one of the two following steps:

(i) We choose some $a \in K_i$ such that $K_i \models \forall y\ \neg C(a, y)$. K_{i+1} is the algebraic closure of $K_i \cup \{(a, b)\}$ where b is transcendent over K_i, and $C_{i+1} = C_i \cup \{(a, b)\}$.

(ii) We choose a conjunction of polynomial equations $\phi(\overline{x}, \overline{y}, \overline{z})$ and a tuple $\overline{z}$ of parameters from K_i which satisfies formula θ in (2). K_{i+1} is the algebraic closure of $K_i \cup \{(a_1, b_1), \ldots, (a_n, b_n)\}$ where $(a_1, b_1, \ldots, a_n, b_n)$ is a generic point over K_i of the irreducible variety $V_{\overline{z}}$, and $C_{n+1} = C_n \cup \{(a_1, b_1), \ldots, (a_n, b_n)\}$. Note that the $a_1, \ldots, a_n$ all lie outside K_i and are distinct from each other due to condition $\xi(\overline{z})$ in the inductive axioms. Moreover, for any subset Γ of $\{(a_1, b_1), \ldots, (a_n, b_n)\}$ the transcendence degree of Γ over K_i is at least equal to the cardinality of Γ due to condition $\psi(\overline{z})$.

A straightforward induction on i shows that n points on C_i with nonzero first coordinates must have transcendence degree at least n over the prime field. Hence all the K_i (and K itself) satisfy the universal axioms. It is also true that the K_i, and therefore K, satisfy the functional axiom. This follows from the fact that in step (i) we only consider a point a whose image is not already defined, and that in step (ii) $a_1, \ldots, a_n$ are distinct elements of $K_{i+1} \setminus K_i$. Finally, it follows from a standard diagonal argument that we can alternate steps (i) and (ii) in order to obtain a function which is defined everywhere and satisfies the inductive axioms.

3.2 Completeness

We start with a strengthening of the inductive axioms.

Lemma 1 *Let M be a model of T and $\phi(x_1, y_1, \ldots, x_n, y_n, \overline{z})$ a conjunction of polynomial equations where the tuple $\overline{z}$ of parameters satisfies the formula θ in the inductive axioms. Let S be a finite subset of M^2. There exist n distinct points in $C \setminus S$ whose $2n$ coordinates satisfy ϕ.*

Proof. Let $S = \{(a_1, b_1), \ldots, (a_s, b_s)\}$. We add a pair (x_0, y_0) of new variables and consider the formula ϕ' in $2n+2$ free variables (and the parameters $\overline{z}' = \overline{z}\hat{\ }(a_1, b_1, \ldots, a_s, b_s)$) which is the conjunction of ϕ and of the formula

$$y_0 \prod_{0<i<j} (x_i - x_j) \times \prod_{i,j>0} (x_i - a_j) = 1.$$

Note that x_0 does not appear in ϕ'. We just have to check that $\overline{z}'$ satisfies the condition $\theta' = \xi' \wedge \psi'$ which is associated to ϕ' in the inductive axioms.

The variety V' defined by ϕ' is irreducible since the same is true of ϕ. Let $(\alpha_0, \beta_0, \ldots, \alpha_n, \beta_n)$ be a point of V' which is generic over $k' = Q(\overline{z}')$. By the hypothesis on ϕ each α_i is transcendent over k', and these $n+1$ coordinates are distinct from each other. Moreover there exist n coordinates $u_1 \in \{\alpha_1, \beta_1\}, \ldots, u_n \in \{\alpha_n, \beta_n\}$ such that $(\alpha_0, u_1, \ldots, u_n)$ is of transcendence degree $n+1$ over k'. Hence we can indeed apply the inductive axiom associated to ϕ'. $\square$

Let M be a model of T and k an algebraically closed subfield of M of finite transcendence degree. We define $\delta(k) = \mathrm{tr.deg}(k) + 1 - |C \cap k^2|$. The universal axioms imply that $\delta(k) \geq 0$ for all k. We say that k is self-sufficient if for all algebraically closed subfields $l \subseteq M$ of finite transcendence degree, $k \subseteq l$ implies $\delta(k) \leq \delta(l)$. Any algebraically closed subfield of M of finite transcendence degree has a self-sufficient extension (consider an extension of δ as small as possible).

An extension $k \subset l$ with k and l self-sufficient is said to be minimal if there exists no self-sufficient structure k' with $k \subset k' \subset l$. Any extension $k \subset l$ with k and l self-sufficient can be broken down into a tower of minimal extensions.

Lemma 2 *Let M be an ω-saturated model of T and k a self-sufficient substructure of M. There exists $\alpha \in M \setminus k$ such that the algebraic closure l of $k \cup \{\alpha\}$ is self-sufficient and there is no point on the curve in $l^2 \setminus k^2$.*

Proof. Let $(x_1, y_1), \ldots, (x_n, y_n)$ be the (finitely many) points on the curve in k^2, and $(a_1, \ldots, a_r)$ a transcendence basis of k. We define three families $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of first-order formulas in one free variable c. The first family is made of all formulas of the form $P(a_1, \ldots, a_r, c) \neq 0$ where P is a nonzero polynomial with integer coefficients. Obviously, any point α which satisfies this family lies outside k. The second family is made of all formulas of the form

$$\begin{aligned}\neg\exists x, y \quad & [\phi(c) \wedge P(x, a_1, \ldots, a_r, c) = 0 \wedge Q(y, a_1, \ldots, a_r, c) = 0 \\ & \wedge C(x, y) \wedge \textstyle\bigwedge_{i=1}^n (x, y) \neq (x_i, y_i)]\end{aligned}$$

where P and Q are nonzero polynomials with integer coefficients, and ϕ states that none of the two univariate polynomials $x \mapsto P(x, a_1, \ldots, a_r, c)$ and $y \mapsto Q(y, a_1, \ldots, a_r, c)$ are identically zero. If α satisfies this family, any point on the curve with both coordinates in the algebraic closure of $k \cup \{\alpha\}$ is in fact in k^2. Moreover, this family is satisfied by all $\alpha \in k$ since $(x_1, y_1), \ldots, (x_r, y_r)$ are the only points on the curve with both coordinates in this algebraically closed field.

The third family is made of all formulas of the form

$$\neg \exists \overline{u}, \overline{v} \ \bigwedge_{i=1}^{m} C(u_i, v_i) \wedge \psi(\overline{u}, \overline{v}, \overline{a}, c) \wedge \theta(c) \wedge \bigwedge_{i,j} (u_i, v_i) \neq (x_j, y_j)$$

where $\overline{u} = (u_1, \ldots, u_m)$, $\overline{v} = (v_1, \ldots, v_m)$, $\overline{a} = (a_1, \ldots, a_r)$, ψ is a conjunction of polynomial equations with integer coefficients, and θ states that the subset of all $(u_1, \ldots, u_m, v_1, \ldots, v_m) \in M^{2m}$ which satisfy $\psi(\overline{u}, \overline{v}, \overline{a}, c)$ has dimension at most $m - 1$. If α satisfies this family, the algebraic closure of $k \cup \{\alpha\}$ is self-sufficient. Moreover, all $\alpha \in k$ satisfy this family since k is self-sufficient.

By ω-saturation we just need to check that $\mathcal{F} \cup \mathcal{G} \cup \mathcal{H}$ is finitely satisfiable. This is clear since any finite subset of $\mathcal{F}$ is satisfiable by an element of k, and any element of k satisfies all of $\mathcal{G}$ and $\mathcal{H}$. $\square$

We also need the "independent marriage lemma" from [2].

Lemma 3 *Let K be a field. Fix an arbitrary set $\{(x_1, y_1), \ldots, (x_n, y_n)\}$ of n points of K^2, and a subfield $k \subseteq K$. The two following properties are equivalent:*

(i) There exist n coordinates $t_1 \in \{x_1, y_1\}, \ldots, t_n \in \{x_n, y_n\}$ which are algebraically independent over k.

(ii) For any integer $m \leq n$ and any subset $\{(x_{i_1}, y_{i_1}), \ldots, (x_{i_m}, y_{i_m})\}$ of our set of n points, the transcendence degree of $(x_{i_1}, y_{i_1}, \ldots, x_{i_m}, y_{i_m})$ over k is at least m.

The completeness of T follows immediately from the next proposition.

Proposition 2 *Let M and M' be ω-saturated models of T. The family of partial isomorphisms between self-sufficient substructures of M and M' has the back-and-forth property.*

Proof. Let $\sigma : k \to k'$ be such an isomorphism. By symmetry it suffices to show that for every $\alpha \in M \setminus k$ there exists a partial isomorphism τ between self-sufficient substructures which extends σ and is defined in α. Two cases can be distinguished:

(i) There exists an extension l of $k \cup \{\alpha\}$ such that $\delta(l) = \delta(k)$.

(ii) There is no such extension.

In the first case l is self-sufficient since k is self-sufficient. Without loss of generality we may assume that the extension $k \subset l$ is minimal. This leaves only two possibilities:

(a) There exists a point (a, b) on the curve with $a \in k$ and $b \in l \setminus k$.

By minimality of l, (a, b) is unique and l is the algebraic closure of $k \cup \{b\}$. There is a unique $b' \in M'$ such that $M' \models C(\sigma(a), b')$. Let l' be the algebraic closure of $k' \cup \{b'\}$. Since b is transcendent over k and b' over k', there exists an isomorphism of fields $\tau : l \to l'$ which extends σ and maps b to b'. By self-sufficiency (a, b) is the only point on the curve of M in $l^2 \setminus k^2$, and $(\sigma(a), b')$ is the only point on the curve of M' in $l'^2 \setminus k'^2$. This isomorphism of fields is therefore an isomorphism of curved fields.

(b) The points $(a_1, b_1), \dots, (a_n, b_n)$ on the curve in $l^2 \setminus k^2$ all have their first coordinates outside k.

We can view $(a_1, b_1, \dots, a_n, b_n)$ as a generic point over k of an irreducible variety $V_{\overline{z}}$ defined by a conjunction $\phi(x_1, y_1, \dots, x_n, y_n, \overline{z})$ of polynomial equations. Here $\overline{z}$ is a tuple of parameters from k. This variety has dimension n since $\delta(l) = \delta(k)$. Our tuple of parameters $\overline{z}$ satisfies the formula ξ which is associated to ϕ in the inductive axioms since $a_1, \dots, a_n$ are pairwise distinct (by the functional axiom) and transcendent over k. Since k is self-sufficient, by Lemma 3 this tuple satisfies formula ψ as well. The tuple $\sigma(\overline{z})$ must therefore satisfy $\xi \wedge \psi$. By application of an inductive axiom there exist n points $(a'_1, b'_1), \dots, (a'_n, b'_n)$ on the curve of M' whose $2n$ coordinates satisfy $\phi(\overline{x}, \overline{y}, \sigma(\overline{z}))$. In fact, by Lemma 1 we can choose these points so that they are all distinct from the (finitely many) points of the curve in k'^2, and distinct from each other. This choice implies that $(a'_1, b'_1, \dots, a'_n, b'_n)$ is a generic point of the algebraic subset of M'^{2n} defined by ϕ since this variety has dimension n and the transcendence degree over k' of $(a'_1, b'_1, \dots, a'_n, b'_n)$ must be at least n by the self-sufficiency of k'. It follows that exists an isomorphism of fields $\tau : l \to l'$ which extends σ and maps $a_1, b_1, \dots, a_n, b_n$ to $a'_1, b'_1, \dots, a'_n, b'_n$. Here l' is the algebraic closure of $k' \cup \{a'_1, b'_1, \dots, a'_n, b'_n\}$. This isomorphism of fields is an isomorphism of curved fields since $(a'_1, b'_1), \dots, (a'_n, b'_n)$ are the only points on the curve in $l'^2 \setminus k'^2$ by self-sufficiency of k'. The analysis of case (i) is now completed.

In case (ii) we set $l = \overline{k(\alpha)}$. Since we are not in case (i), l is self-sufficient and there is no point on the curve in $l^2 \setminus k^2$. Hence we just need to find $\alpha' \in M' \setminus k'$ such that $l' = \overline{k'(\alpha')}$ is self sufficient, and there is no point on the curve in $l'^2 \setminus k'^2$. Any isomorphism of fields $\tau : l \to l'$ will then be good for our purposes. The existence of α' is given by Lemma 2 (applied to M'). $\square$

4 Convergence to the limit theory

In this section we show that any axiom of T is satisfied by all generic polynomials of sufficiently high degree. This implies immediately that any sentence F in the language of curved fields is satisfied by all generic polynomials of sufficiently high degree if $T \vdash F$. Conversely, if F is not a sentence of T then $T \vdash \neg F$ by completeness of T, so that F is false for all generic polynomials of sufficiently high degree.

4.1 Satisfaction of Universal Axioms

Given two sequences $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ of elements of K, we denote by $W(x, y)$ the affine subspace of all $(\alpha_1, \ldots, \alpha_d) \in K^d$ such that $\sum_{j=1}^{d} x_i^j \alpha_j = y_i$ for $i = 1, \ldots, n$. This set can be interpreted as the the set of degree d polynomials without constant term which go through the n points $(x_1, y_1), \ldots, (x_n, y_n)$.

Lemma 4 *If $d \geq n$ and $x_1, \ldots, x_n$ are distinct and nonzero then $W(x, y)$ has dimension $d - n$.*

Proof. If the x_i's are pairwise distinct and nonzero the matrix of the system defining $W(x, y)$ has rank n by the well-known property of Vandermonde determinants. The solution space is thus of dimension $d - n$. □

Proposition 3 *If $d \geq n$ and a generic polynomial of degree d goes through n distinct points $(x_1, y_1), \ldots, (x_n, y_n)$ with $x_i \neq 0$ for all i, their $2n$ coordinates have transcendence degree at least n.*

Proof. Since these $2n$ points are distinct and lie on the same polynomial curve, their first coordinates are also distinct. It then follows from Lemma 4 that the coefficients of the generic polynomial, which are of transcendence degree d over the prime field, have transcendence degree at most $d-n$ over $\{x_1, y_1, \ldots, x_n, y_n\}$. These $2n$ coordinates must therefore be of transcendence degree at least n over the prime field. □

It follows that a generic polynomial of degree d satisfies axiom (1) as soon as $d \geq n$.

4.2 Satisfaction of Inductive Axioms

From now on we assume that $K = \mathbb{C}$. Let $\varphi(r, n) = n(nr + n + r)$. We first state two intersection theorems.

Theorem 1 *Let V be an algebraic subset of $\mathbb{C}^d$ of codimension r, defined over an algebraically closed subfield $k \subseteq \mathbb{C}$. Then $V \cap W(x, y) \neq \emptyset$ if x and y satisfy the following two conditions and if $d \geq \varphi(r, n)$:*

(i) The x_i's are pairwise distinct and all lie outside k.

(ii) There exists $u_1 \in \{x_1, y_1\}, \ldots, u_n \in \{x_n, y_n\}$ such that $(u_1, \ldots, u_n)$ is of transcendence degree n over k.

It is clear that the theorem fails if condition (i) is removed. We have shown in [5] that condition (ii) is also necessary. We do not known whether the bound $n(nr+n+r)$ in this theorem is optimal. A precise analysis [5] of the case where V is an affine subspace yields the lower bound $n(r + 1)$. The consideration of more general algebraic sets could perhaps yield better lower bounds.

The second main ingredient is the following result.

Theorem 2 *Let V be an irreducible algebraic subset of $\mathbb{C}^d$ of codimension r, defined over an algebraically closed subfield $k \subseteq \mathbb{C}$.*

Assume that $d \geq n(2n+r+1)$ and that condition (ii) is satisfied as well as:

(i') The x_i's are pairwise distinct and are all nonzero.

If $V \cap W(x,y) \neq \emptyset$ then this intersection contains a generic point of V (i.e., a point of transcendence degree over k equal to the dimension V).

The proof of these two theorems is postponed to the next section. Our immediate goal is to show that any inductive axiom is satisfied by all generic polynomials of sufficiently high degree.

Given $r \in \mathbb{N}$, consider any inductive axiom such that the tuple $\overline{z}$ of parameters in (2) is of length at most r. Let C be the graph of a generic polynomial of degree d. We claim that C satisfies the inductive axiom as soon as $d \geq \varphi'(r,n)$, where $\varphi'(r,n) = n(nr+n+r+1)$. Indeed, fix any $\overline{z}$ such that $\mathbb{C} \models \theta(\overline{z})$. The tuple $\alpha = (\alpha_1, \ldots, \alpha_d)$ of coefficients of C can be viewed as a generic point over $\mathbb{Q}(\overline{z})$ of some irreducible algebraic set V of $\mathbb{C}^d$. Since $\overline{z}$ is of length at most r, V is of codimension at most r.

Let $V_{\overline{z}}$ be the subset of $\mathbb{C}^{2n}$ defined by $\phi(.,.,\overline{z})$. Let $(x_1, y_1, \ldots, x_n, y_n)$ be a point of $V_{\overline{z}}$ which is generic over $\mathbb{Q}(\overline{z})$. Conditions (i) and (ii) of Theorem 1 are satisfied by $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ since $\mathbb{C} \models \theta(\overline{z})$. The intersection $V \cap W(x,y)$ is therefore nonempty since $d \geq \varphi'(r,n) \geq \varphi(r,n)$. By Theorem 2 this intersection contains a generic point β of V since $\varphi'(r,n) \geq n(2n+r+1)$. We conclude that the graph of the generic polynomial of coefficient vector β contains n points whose $2n$ coordinates lie on $V_{\overline{z}}$ (and the same is true of C since α and β have same type over $\overline{z}$). We have thus proved that the inductive axiom is satisfied as soon as $d \geq \varphi'(r,n)$.

5 The intersection theorems

In this section we give the proofs of Theorems 1 and 2. We start with Theorem 2 since it is needed for the proof of Theorem 1.

5.1 Proof of Theorem 2

It is almost identical to the proof of the corresponding result in [2]. In particular, the proof of Lemma 5 below differs from the proof of Lemma 7 from [2] only by minor details. Here the main difference with that previous paper does not lie in the proof of the theorem but in its hypotheses: we need to assume that $V \cap W(x,y)$ is nonempty whereas that condition was automatically satisfied in [2] due to the projective nature of the problem.

Let k' be the algebraic closure of $k(x,y)$. We denote the transcendence degree of k' over k by $n+m$. Note that $m \geq 0$ by condition (ii) and that $W(x,y)$ is of codimension n by condition (i'). Let us assume that $W(x,y)$ intersects V and let β be a point of $V \cap W(x,y)$ which is generic over k'. "Generic" again means that the transcendence degree of β over k' is equal to the dimension of $V \cap W(x,y)$, which is at least $d-(n+r)$.

Lemma 5 *If $d \geq n(2n+r+1)$, $x\hat{}y$ is of transcendence degree at most m over $k(\beta)$.*

Proof. Let n_1 be the cardinality of the set P_1 of the points (x_i, y_i) which are algebraic over $k(\beta)$. We denote by P_2 the set of the remaining $n_2 = n - n_1$ points. Note that x_i is transcendent over $k(\beta)$ for every point (x_y, y_i). Indeed, if x_i was algebraic over $k(\beta)$ the same would be true of y_i since $\beta \in W(x, y)$.

Let θ be the transcendence degree of P_2 over $k(\beta)$. We need to show that $\theta \leq m$ if d is large enough. Note that $\text{tr.deg}k(P_1)/k \geq n_1$ by condition (ii). Since $\text{tr.deg}k(P_1, P_2)/k = n_1 + n_2 + m$ by definition of m, this implies that $\text{tr.deg}k(P_1, P_2)/k(P_1) \leq n_2 + m$. Now we consider $l = \lfloor (d - n_1)/n_2 \rfloor$ independent copies $P_{2,1}, \ldots, P_{2,l}$ of P_2. More precisely, these new points should satisfy the two following conditions:

1. Each set $P_{2,i}$ has same type over $k(\beta)$ as P_2.
2. The transcendence degree over $k(\beta)$ of their union is equal to $l\theta$.

Let Q be the union of P_1 and of the set of new points. The first coordinates of the new points are all transcendent over $k(\beta)$ and distinct from each other. It follows that the first coordinates of the points of Q are all nonzero and distinct from each other. In particular, these points are all distinct so that $|Q| = n_1 + ln_2 \in]d - n_2, d]$. We can now apply Lemma 4 since the polynomial curve of coefficient vector β goes through all the points of Q. It follows that that β is of transcendence degree at most n_2 over $k(Q)$. We can now compute the transcendence degree of $\beta\hat{}Q$ over k in two different ways.

On the one hand, $\text{tr.deg}k(\beta\hat{}Q)/k = \text{tr.deg}k(\beta)/k + \text{tr.deg}k(\beta\hat{}Q)/k(\beta) \geq d - (n+r) + l\theta$.

On the other hand, $\text{tr.deg}k(\beta\hat{}Q)/k = \text{tr.deg}k(Q)/k + \text{tr.deg}k(\beta\hat{}Q)/k(Q) < \text{tr.deg}k(P_1)/k + l(n_2 + m) + n_2$. Comparing these two expressions, we obtain the inequality

$$d - (n+r) + l\theta < l(n_2 + m) + 2n_1 + n_2. \tag{3}$$

Letting d (and consequently l) go to infinity in this inequality then shows that $\theta > m$ is impossible. The specific bound $d \geq n(2n+r+1)$ can be derived from a straightforward calculation which we do not detail completely. The first step is to assume that $\theta \geq m+1$. We obtain from (3) that $l < 2n + r$, which implies in turn $d < n_1 + n_2(2n+r)$. We finally conclude that the (probably rough) bound $d < n(2n+r+1)$ holds if $\theta > m$. □

In order to complete the proof of Theorem 2 we compute the transcendence degree of $k(\beta, x, y)$ over k in two different ways. On the one hand, it is upper bounded by $\text{tr.deg}k(\beta)/k + \text{tr.deg}k(\beta, x, y)/k(\beta)$. By the above lemma this is at most $\text{tr.deg}k(\beta)/k + m$ if $d \geq n(2n+r+1)$. On the other hand, this transcendence degree is equal to $\text{tr.deg}k(x, y)/k + \text{tr.deg}k(x, y, \beta)/k(x, y) = n + m + \dim(V \cap W(x, y))$ which is at least $n + m + d - (n+r) = m + d - r$. A comparison of these two expressions shows that $\text{tr.deg}k(\beta)/k \geq d - r = \dim V$. Since $\beta \in V$ this inequality must be an equality, and β is indeed a generic point of V.

5.2 Pseudocylinders

Before moving on to the proof of Theorem 1 we need some geometric preliminaries. In this subsection we work with the Euclidean topology on $\mathbb{C}^p$. We denote by $Z(f_1, \ldots, f_s)$ the zero set of s polynomials $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_p]$. We denote by $\mathcal{P}(d_1, \ldots, d_s)$ the space of all tuples $(f_1, \ldots, f_s)$ of polynomials such that $\deg(f_i) \leq d_i$ for $i = 1, \ldots, s$. This space can be identified to $\mathbb{C}^N$ for $N = \prod_{i=1}^{s} \binom{p+d_i}{p}$, and it is also endowed with the Euclidean topology.

Lemma 6 (continuity of roots) *Assume that $s \leq p$ and that a point α of $\mathbb{C}^p$ lies on an irreducible component of $Z(f_1, \ldots, f_s)$ of codimension s. For any neighbourhood O of α, there exists a neighbourhood O' of $f_1, \ldots, f_s$ in $\mathcal{P}(\deg(f_1), \ldots, \deg(f_s))$ such that $Z(f'_1, \ldots, f'_s) \cap O \neq \emptyset$ for any $(f'_1, \ldots, f'_s)$ in O'.*

Proof. There exist $n - s$ affine functions $l_1, \ldots, l_{n-s}$ such that $Z(f_1, \ldots, f_s, l_1, \ldots, l_{n-s}) = \{\alpha\}$. We can now apply the "extended geometric version" of Bézout's Theorem from [1] since we have as many equations as unknowns. We conclude that there exists a neighbourhood O' of $(f_1, \ldots, s_s)$ in $\mathcal{P}(\deg(f_1), \ldots, \deg(f_s))$ and a neighbourhood O'' of $l_1, \ldots, l_{n-s}$ in $\mathcal{P}(1, \ldots, 1)$ such that $Z(f'_1, \ldots, f'_s, l'_1, \ldots, l'_{n-s}) \cap O \neq \emptyset$ whenever $(f'_1, \ldots, f'_s) \in O'$ and $(l'_1, \ldots, l'_s) \in O''$. $\square$

Let V be an irreducible algebraic subset of $\mathbb{C}^p$ of codimension r. Recall that V is said to be a complete intersection if it can be defined by exactly r polynomial equations. This is not always possible, but it is always possible to find a a variety V' defined by r equations such that V is an irreducible component of V' (see for instance Proposition 2.7 of [6]).

Corollary 1 *Let V be an irreducible algebraic subset of $\mathbb{C}^p$ of codimension r and W an affine subspace of codimension n where $r+n \leq p$. Let α be a point of V which does not lie on any other component of V', where V' is as above. If α lies on an irreducible component of $V \cap W$ of codimension $r+n$ then $V \cap W' \neq \emptyset$ for any affine subspace W' of codimension n which is sufficiently close to W.*

Proof. By choice of α, there is a neighbourhood O of this point such that $V' \cap O \subseteq V$. Let us apply Lemma 6 to the system of $s = r + n$ equations defining $V' \cap W$. We conclude that $V' \cap W' \cap O \neq \emptyset$ if W' is sufficiently close to W, but $V' \cap W' \cap O \subseteq V \cap W'$ by choice of O. $\square$

Proposition 4 *Let V be an algebraic subset of $\mathbb{C}^p$ of codimension r. For any $n \leq p - r$, let I_n be the set of points $\alpha \in \mathbb{C}^p$ such that there exists an affine subspace of codimension n containing α which does not intersect V. If I_n is dense in $\mathbb{C}^p$, there exists an affine subspace of codimension n in which V is of codimension $< r$ (i.e., $V \cap W$ has codimension at most $n + r - 1$).*

Proof. Assume first that V is irreducible. Let α be a point of V which does not lie on any other component of V', where V' is as in Corollary 1. If I_n is dense we can find a sequence of points α_k which converges to α and a sequence W_k

of affine subspaces of codimension n containing α_k such that $V \cap W_k = \emptyset$. By compactness of the set of directions of affine subspaces of codimension n, we may assume (extracting a subsequence if necessary) that W_k converges to some affine subspace W of codimension n. We claim that $V \cap W$ has codimension at most $n+r-1$. Indeed, assume by contradiction that $V \cap W$ has codimension at least $n+r$. Since $V \cap W \neq \emptyset$ (α is in the intersection) the codimension should be exactly $n+r$. This is in contradiction with Corollary 1 (take $W' = W_k$ for a large enough k). This completes the proof of Proposition 4 for irreducible varieties. If V is not irreducible, we can apply the result to an irreducible component. □

For instance, in the case $r = 1$ the conclusion of this proposition is that V contains an affine subspace of codimension n. As an example of this situation, take for V a cylinder in $\mathbb{C}^3$ (in this case $p = 3$, $r = 1$ and $n = 2$).

5.3 Proof of Theorem 1

This theorem was obtained in [5] in the special case where V is an affine subspace. More precisely, we proved the following result.

Theorem 3 *Let V be an affine subspace of $\mathbb{C}^d$ of codimension r, defined over an algebraically closed subfield $k \subseteq \mathbb{C}$.*

If x satisfies condition (i) then $V \cap W(x,y) \neq \emptyset$ as soon as $d \geq n(r+1)$, and this intersection is of codimension $r+n$ in $\mathbb{C}^d$.

The proof of Theorem 1 relies on Theorem 3 as well as on an inductive argument which is contained in the next lemma.

Lemma 7 *Let V be an algebraic subset of $\mathbb{C}^d$ defined over an algebraically closed subfield $k \subseteq \mathbb{C}$. Assume that there exists an affine subspace A of $\mathbb{C}^d$ of codimension s in which V is of codimension $r \geq 1$. Assume also that x and y satisfy conditions (i) and (ii) and that $V \cap W(x,y) = \emptyset$. There exists an affine subspace A' of $\mathbb{C}^d$ of codimension $s+n$ in which V if of codimension $r-1$ as soon as:*

$$d \geq \max(n(s+1), n(2n+s+1), n+r+s).$$

Proof. We shall assume that A is defined over k (there must exist such an A since V is defined over k). If $d \geq n(s+1)$ the intersection $A \cap W(x,y)$ is nonempty by Theorem 3, and it is of codimension n in A. If additionally $d \geq n(2n+s+1)$ this intersection contains a generic point of A by Theorem 2. Obviously, $A \cap W(x,y)$ does not intersect $A \cap V$ since $W(x,y)$ does not intersect V. We can therefore apply Proposition 4 with $p = d-s$ and A in place of $\mathbb{C}^p$. This is legitimate as soon as $n+r \leq \dim(A) = d-s$. We conclude that there exists an affine subspace $A' \subseteq A$ of codimension n in A such that $V \cap A'$ is of codimension at most $r-1$ in A'. □

Theorem 1 follows almost immediately from the above lemma. Indeed, assume by contradiction that $d \geq \varphi(r,n)$ but $V \cap W(x,y) = \emptyset$. We can apply the lemma iteratively for $s = 0, n, 2n, \ldots$ up to $s = (r-1)n$. This is legitimate due the inequalities $\varphi(r,n) \geq n((r-1)n+1)$, $\varphi(r,n) \geq n(2n+(r-1)n+1)$ and $\varphi(r,n) \geq n+r+(r-1)n$. We conclude that V contains an affine subspace of codimension nr. Without loss of generality we can assume again that this subspace is defined over k. Since $\varphi(r,n) \geq n(nr+1)$ we can apply Theorem 3 one more time. This yields the contradiction $V \cap W(x,y) \neq \emptyset$.

6 Remarks on Liouville Functions

In [10] Wilkie calls "Liouville function" a function $H : \mathbb{C} \to \mathbb{C}$ with a Talyor series of the form

$$H(z) = \sum_{i=1}^{\infty} z^i / a_i$$

where the a_i are non-zero integers satisfying the condition: for every $l \geq 1$, $|a_{i+1}| > |a_i|^{i^l}$ for all sufficiently large i. It seems plausible to conjecture that the first-order theory of the complex field expanded with H is the limit theory of generic polynomials. As of now it is not even known whether all Liouville functions have the same first-order theory. Some partial results towards this conjecture can be found in [10]. Indeed, it is shown that any Liouville function satisfies the universal axioms. Other results in the same paper imply that some of the inductive axioms are also satisfied: those for which the tuple $\overline{z}$ of parameters is of length 0. It follows from the results in the present paper that any inductive axiom is satisfied by the partial sums $H_d(z) = \sum_{i=1}^{d} z^i / a_i$ for all sufficiently large d.

References

[1] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation.* Springer-Verlag, 1998.

[2] O. Chapuis, E. Hrushovski, P. Koiran, and B. Poizat. La limite des théories de courbes génériques. To appear in *Journal of Symbolic Logic*, 1999.

[3] P. Koiran. On defining irreducibility. *Comptes Rendus de l'Académie des Sciences*, 330:529–532, 2000.

[4] P. Koiran and N. Portier. Back-and-forth systems for generic curves and a decision algorithm for the limit theory. *Annals of Pure and Applied Logic*, 111:257–275, 2001.

[5] P. Koiran, N. Portier, and G. Villard. A rank theorem for Vandermonde matrices. preprint, 2001.

[6] D. Perrin. *Géométrie Algébrique: une Introduction.* Interéditions / CNRS Editions, 1995.

[7] B. Poizat. Amalgames de Hrushovski: une tentative de classification. preprint, 2000.

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

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

[10] A. J. Wilkie. Liouville functions. preprint, 2000.

[11] B. Zilber. A theory of generic functions with derivatives. preprint.