Laboratoire de l'Informatique du Parallélisme

École Normale Supérieure de Lyon
Unité Mixte de Recherche CNRS-INRIA-ENS LYON n° 8512

Back-and-Forth Systems for Generic Curves and a Decision Algorithm for the Limit Theory

Pascal Koiran and Natacha Portier

September 2000

Research Report N° 2000-29

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`

Back-and-Forth Systems for Generic Curves and a Decision Algorithm for the Limit Theory

Pascal Koiran and Natacha Portier

September 2000

Abstract

It was recently shown that the theories of generic algebraic curves converge to a limit theory as their degrees go to infinity. In this paper we give quantitative versions of this result and other similar results. In particular, we show that generic curves of degree higher than 2^{2r} cannot be distinguished by a first-order formula of quantifier rank r. A decision algorithm for the limit theory then follows easily. We also show that in this theory all formulas are equivalent to boolean combinations of existential formulas, and give a quantitative version of this result.

Keywords: algebraic curves, algebraic algorithms, back-and-forth systems, model theory.

Résumé

On a récemment établi l'existence d'une limite des théories des courbes algébriques génériques de degré croissant. Dans cet article nous donnons des versions quantitatives de ce résultat et d'autres résultats semblables. Par exemple, nous montrons que des courbes génériques de degré au moins 2^{2r} ne peuvent pas être distinguées par une formule du premier ordre de rang de quantification r. On en déduit facilement un algorithme de décision pour la théorie limite. Nous montrons aussi que dans cette théorie toutes les formules sont équivalentes à des combinaisons booléennes de formules existentielles, et nous donnons une version quantitative de ce résultat.

Mots-clés: courbes algébriques, algorithmes algébriques, va-et-vient, théorie des modèles.

Back-and-Forth Systems for Generic Curves and a Decision Algorithm for the Limit Theory

Pascal Koiran and Natacha Portier*

22nd September 2000

Abstract

It was recently shown that the theories of generic algebraic curves converge to a limit theory as their degrees go to infinity. In this paper we give quantitative versions of this result and other similar results. In particular, we show that generic curves of degree higher than 2^{2r} cannot be distinguished by a first-order formula of quantifier rank r. A decision algorithm for the limit theory then follows easily. We also show that in this theory all formulas are equivalent to boolean combinations of existential formulas, and give a quantitative version of this result.

Keywords: algebraic curves, algebraic algorithms, back-and-forth systems, model theory.

1 Introduction

O. Chapuis, E. Hrushovski, P. Koiran and B. Poizat introduced in [2] a new complete theory: the limit theory of generic curves. Strictly speaking there are several limit theories (one for each characteristic). We shall therefore assume that the characteristic is arbitrary, but fixed throughout the paper. The base field of the chosen characteristic will be denoted by Q and $\overline{Q}$ is its algebraic closure.

Let d be an integer, K an algebraically closed field of infinite transcendence degree and $\{a_{i,j} | 0 \leq i, j \leq d \text{ and } i + j \leq d\}$ a set of algebraically independent elements of K. Consider the language of curved fields: the language of fields $(+, -, \times, 0, 1)$ together with an extra binary predicate symbol C. The theory T_d of degree d generic curves is the set of closed formulas of this language that become true when $C(x, y)$ is interpreted in K by:

$$\sum_{i+j \leq d} a_{i,j} x^i y^j = 0.$$

It was shown in [2] that T_d converges to a limit theory as d goes to infinity. This means that for any closed formula F in the language of curved fields, there exists an integer d_F such that F belongs to T_d for all integers $d \geq d_F$

*LIP, École Normale Supérieure, 46 allée d'Italie, 69364 LYON CEDEX 07, France; email: {Pascal.Koiran, Natacha.Portier}@ens-lyon.fr

(in which case F belongs to the limit theory), or such that $\neg F$ belongs to T_d for all integers $d \geq d_F$ (in which case $\neg F$ belongs to the limit theory). The main tool of our decision algorithm is a result of independent interest: we show in Theorem 2 that $d_F \leq 2^{r-1}(2^r + 1) - 1$, where r is the quantifier rank of F. This upper bound makes it possible to reduce the decision problem for the limit theory to a decision problem about algebraically closed fields. As a byproduct we also obtain partially new proofs of the main results of [2]. The main difference is that we work with actual algebraic curves whereas [2] often works with models of the limit theory (we still rely heavily on [2], in particular for the axiomatization presented in section 3).

The remainder of this paper is organized as follows. We present some basic notions from model theory in section 2, and review some material from [2] in section 3. Our limit theorems (quantitative versions of results from [2]) are established in section 5. They rely on technical lemmas from section 4. We show in section 6 that in the limit theory, every formula is equivalent to a boolean combination of existential formulas. Bruno Poizat has pointed out that the argument also applies to other "Hrushovski-style" constructions (see [2] for some references). More precisely, we show that a formula of quantifier rank r with n free variables is equivalent to a boolean combination of existential formulas having at most $2n + 2(n+1)(2^r - 1)$ quantifiers each. We also give an example of a universal formula which is not equivalent to any existential formula. A short section 7 on existential formulas completes the paper.

1.1 Curved Fields

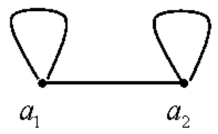
Unless stated otherwise, fields denoted by upper case or lower case letters (K, K', k, ℓ,...) will always be algebraically closed. As the notion of algebraic degree of an extension is irrelevant for our purposes, we will denote by $[l : k]$ the transcendence degree of ℓ over a subfield $k \subseteq l$. The notion of p-sufficient substructure defined below is crucial for applying the method of Ehrenfeucht-Fraïssé games to our problem. It is a kind of finite approximation of the notion of *structure autosuffisante* used in [2].

Definition 1 *A curved field $(K, +, -, \times, 0, 1, C)$ is a field $(K, +, -, \times, 0, 1)$ together with a subset C of k^2. It will be denoted (K, C) for short, or K. A substructure (k, γ) of the curved field (K, C) is a subfield k of K together with the curve $\gamma = \Gamma \cap k^2$. By abuse of notation we will write (k, C) instead of $(k, C \cap k^2)$.*

Let ℓ be an extension field of k in K, of finite transcendence degree over k. Whenever $(C \cap \ell^2) - (C \cap k^2)$ is a finite set, $\delta(l : k)$ is by definition equal to $[l : k]$ minus the cardinality of that set.

Given a positive integer p, k is said to be p-sufficient (in K) if $\delta(l : k) \geq 0$ for any extension field $k \subseteq \ell \subseteq K$ of transcendence degree $[\ell : k] \leq p$.

Here is an example: a_1 and a_2 are algebraically independent over Q and $C = \{(a_1, a_1), (a_1, a_2), (a_2, a_2)\}$. Then $\delta(Q(a_1) : Q) = 0$ and $\delta(Q(a_1, a_2) : Q(a_1)) = -1$.



Natural examples of curves include: algebraic curves; algebraic curves minus a point (see Theorem 5); the limit curve constructed in [2]. More exotic curves are constructed in section 4 to establish the optimality of Lemma 2.

2 Back-and-forth Systems

This section is devoted to some logical background. For more details one may consult the books of B. Poizat [7] or W. Hodges [6].

We first recall the notions of (parameter-free) formula and of quantifier rank. *Atomic formulas* in curved fields are of the form $P_1(\bar{x}) = 0$ or of the form $C(P_1(\bar{x}), P_2(\bar{x}))$, which means $(P_1(\bar{x}), P_2(\bar{x})) \in C$. Here P_1 and P_2 are polynomials with coefficients in the prime field Q.

The quantifier rank of a formula is defined by induction on the set of formulas. By definition, atomic formulas are of quantifier rank 0 and $\neg F(\bar{x})$ has the same quantification rank as $F(\bar{x})$. The quantifier ranks of $F(\bar{x}) \wedge G(\bar{x})$ and $F(\bar{x}) \vee G(\bar{x})$ are equal to the maximum of the quantifier ranks of F and G. Let $H(y, \bar{x})$ be a formula of quantifier rank r. Then $\exists y H(y, \bar{x})$ and $\forall y H(y, \bar{x})$ are formulas of quantifier rank $r + 1$.

Formulas of quantifier rank 0 are said to be "quantifier-free". They are boolean combinations of atomic formulas. A formula is closed if it has no free variable, that is, every variable is bound by a quantifier. One writes $(K, C) \models F(a_1, \ldots, a_n)$ to state that an element $(a_1, \ldots, a_n)$ of K^n satisfies a formula $F(x_1, \ldots, x_n)$.

Let F be a closed formula of quantifier rank r. In section 5 we will show that if C_d and $C_{d'}$ are generic curves of degrees higher than 2^{2r} then $(K, C_d) \models F$ if and only if $(K, C_{d'}) \models F$. This result will be obtained by the method of partial isomorphisms (also known as method of back-and-forth games, or of Ehrenfeucht-Fraïssé games). This method works as follows.

Consider two curved fields K and K' with the same prime field Q. In this case an isomorphism is a field isomorphism that conserves the curve. A *partial isomorphism* between K and K' is an isomorphism from a subfield k of K to a subfield k' of K'. The notion of *r-isomorphism* between K and K' is defined by induction on the integer r. A 0-isomorphism is a partial isomorphism. An isomorphism $\varphi : k \to k'$ is an $(r + 1)$-isomorphism between K and K' if it satisfies the back and forth conditions:

- for every $a' \in K'$ there exists $a \in K$ and an r-isomorphism extending φ which sends a to a'.
- for every $a \in K$ there exists $a' \in K'$ and an r-isomorphism extending φ which sends a to a'.

We claim that if there is an r-isomorphism φ between K and K' sending $\bar{c}$ to $\bar{c'}$ then for every formula $F(\bar{x})$ with quantifier rank at most r we have $(K, C) \models F(\bar{c})$ if and only if $(K', C') \models F(\varphi(\bar{c}))$. As a consequence, K and K' satisfy the same set of closed formulas without parameters of quantifier rank at most r. The proof is by induction on r. The result is clear for $r = 0$. Suppose now φ is an $(r+1)$-isomorphism between K and K' sending $\bar{c}$ to $\bar{c'}$. It suffices to prove the result for formulas $F(\bar{x})$ of the form $\exists y H(y, \bar{x})$ where the quantifier rank of H is r. Suppose for instance that $(K, C) \models F(\bar{c})$ (the case $(K', C') \models F(\bar{c'})$ is similar). Then there exists an element b of K such that $(K, C) \models H(b, \bar{c})$. By the "forth" condition, the $(r+1)$-isomorphism φ can be extended into an r-isomorphism χ defined in b. By induction hypothesis $(K', C') \models H(\chi(b), \bar{c'})$ since H is of quantifier rank r. Hence $(K', C') \models F(\bar{c'})$.

3 Axiomatization of the Limit Theory

Recall from [2] that there are three groups of axioms:

1. The axioms of algebraically closed fields of the chosen characteristic.

2. Universal axioms. For all integers n we consider the list $A(n)$ of all axioms of the form

$$\forall x_1, y_1, \ldots, x_n, y_n \left[\bigwedge_{1 \le i < j \le n} (x_i, y_i) \neq (x_j, y_j) \wedge \bigwedge_{1 \le i \le n} C(x_i, y_i) \right] \rightarrow \bigvee_{t_i \in \{x_i, y_i\}} P(t_1, \ldots, t_n) \neq 0$$

   where P is a non constant polynomial with coefficients in the prime field.

3. Inductive ($\forall\exists$) axioms. For all integers $n, k \ge 1$ we consider the list $AE(n, k)$ of all axioms of the form

$$\forall z_1, \ldots, z_k \exists x_1, y_1, \ldots, x_n, y_n \; \Psi(z) \rightarrow \left[\bigwedge_{i=1}^{n} C(x_i, y_i) \wedge \phi(x, y, z) \right] \qquad (1)$$

   where ϕ is a conjunction of polynomials equations in the variables $x = x_1, \ldots, x_n$, $y = y_1, \ldots, y_n$, $z = z_1, \ldots, z_k$ with coefficients in Q. $\Psi(z)$ is a formula of the language of fields which states that the subset $V_z \subseteq K^{2n}$ of all tuples $(x_1, y_1, \ldots, x_n, y_n)$ satisfying $\phi(x, y, z)$ verifies the following property: there exist n variables $t_1 \in \{x_1, y_1\}, \ldots, t_n \in \{x_n, y_n\}$ such that the projection of V_z on $t_1, \ldots, t_n$ is a dense subset of K^n.

The fact that any axiom is satisfied by generic curves of sufficiently high degree is established in the "deuxième partie" of [2]. In fact, it is shown that generic curves satisfy a strong version of the inductive axioms, which we shall call $AE'(n, \Delta)$.

This property is as follows. Let $\phi(x,y,z)$ be a conjunction of polynomial equations with coefficients in the prime field. Fix a tuple $z_1,\dots,z_k$ of parameters which satisfies the formula Ψ of (1), and assume that $[Q(z):Q] \le \Delta$. Then there exist n points $(x_1,y_1),\dots,(x_n,y_n)$ on the curve whose coordinates satisfy $\phi(x,y,z)$, such that one can choose n coordinates $t_1 \in \{x_1,y_1\},\dots,t_n \in \{x_n,y_n\}$ which are algebraically independent over $Q(z)$. We note for future use in Lemma 4 that this last condition implies in particular that none of these points lies in $\overline{Q(z)}^2$.

It turns out that the generic curve C_d satisfies $AE'(n,\Delta)$ as soon as $d \ge n(2n+\Delta+1)-1$ (see [2], Lemme 7).

As to universal axioms, it is shown in Corollary 6 of [2] that if n distinct points $(x_1,y_1),\dots,(x_n,y_n)$ belong to a generic curve C_d with $d \ge n-1$, then $Q(x_1,y_1,\dots,x_n,y_n)$ has transcendence degree at least n. This implies that $\overline{Q}$ (or even Q) is d-sufficient in (K,C_d). By Lemma 1 below (for a proof see Lemme 2 and Corollaire 3 of [2]), the same property implies that $A(n)$ is satisfied as soon as $d \ge n-1$.

Lemma 1 *Fix an arbitrary set $\{(x_1,y_1),\dots,(x_n,y_n)\}$ of n points of K^2, and a subfield $k \subseteq K$. The two following properties are equivalent:*

- *(i) There exist n coordinates $t_1 \in \{x_1,y_1\},\dots,t_n \in \{x_n,y_n\}$ which are algebraically independent over k.*
- *(ii) For any integer $m \le n$ and any subset $\{(x_{i_1},y_{i_1}),\dots,(x_{i_m},y_{i_m})\}$ of our set of n points, the transcendence degree of $(x_{i_1},y_{i_1},\dots,x_{i_m},y_{i_m})$ over k is at least m.*

For $d \ge n-1$, the property that n points on the curve have transcendence degree at least n is also satisfied *a fortiori* by the "curve" C'_d obtained by removing a point $(a,b) \in C_d$ from C_d. This fact will be useful in section 5. There is a similar statement for AE axioms. We just need to note that for any curve C which satisfies $AE'(n,\Delta+2)$, $C \setminus \{(a,b)\}$ satisfies $AE'(n,\Delta)$ (just add (a,b) to the tuple of parameters in (1)). We conclude that C'_d satisfies $AE'(n,\Delta)$ as soon as $d \ge n(2n+\Delta+3)-1$.

4 Back-and-Forth Lemmas

We begin with a simple but crucial lemma.

Lemma 2 *Let k be a p-sufficient substructure of a curved field (K,C) and a an element of $K \backslash k$. There exists an extension field ℓ of $k(a)$ in K which satisfies one of the following conditions:*

- *(i) ℓ is $\lfloor p/2 \rfloor$-sufficient, $[\ell:k] \le \lceil p/2 \rceil$ and $\delta(\ell:k)=0$.*
- *(ii) ℓ is $(\lceil p/2 \rceil - 1)$-sufficient, $\ell = \overline{k(a)}$ and $\delta(\ell:k)=1$.*

Note that ℓ is $(\lceil p/2 \rceil - 1)$-sufficient in both cases.

Proof:

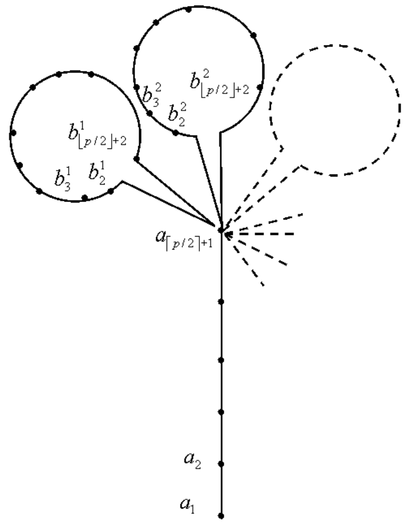
Suppose there is some extension ℓ of $k(a)$ such that $[\ell : k] \leq \lceil p/2 \rceil$ and $\delta(\ell : k) = 0$. Then ℓ is provably $\lfloor p/2 \rfloor$-sufficient. Indeed, let f be an extension of ℓ such that $[f : \ell] \leq \lfloor p/2 \rfloor$. Then $[f : k] \leq p$ and $\delta(f : l) = \delta(f : k) \geq 0$ since k is p-sufficient.

Now suppose that $\delta(f : k) > 0$ for every extension f of $k(a)$ such that $[f : k] \leq \lceil p/2 \rceil$. In particular, $\delta(\overline{k(a)} : k) = 1$. We show that $\ell = \overline{k(a)}$ is $(\lceil p/2 \rceil - 1)$-sufficient. Let f be an extension of ℓ such that $[f : \ell] \leq \lceil p/2 \rceil - 1$. Then $[f : k] \leq \lceil p/2 \rceil$ and $\delta(f : k) > 0$. Thus $\delta(f : \ell) \geq 0$ and ℓ is $(\lceil p/2 \rceil - 1)$-sufficient.

△

Optimality of Lemma 2: First we prove the optimality of case (i) of Lemma 2. We use the following example. Let K be a field of infinite transcendence degree and let $\{a_1, \dots, a_{\lceil p/2 \rceil + 1}\} \cup \{b_2^i, \dots b^i_{\lfloor p/2 \rfloor + 2} | i \in \mathbf{N}\}$ be a set of algebraically independent elements.

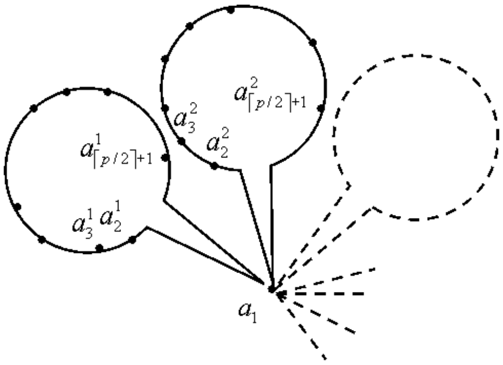
The curve C is a flower made of a stem $\{(a_1, a_2), \dots, (a_{\lceil p/2 \rceil}, a_{\lceil p/2 \rceil + 1})\}$ and infinitely many petals:
$\{(a_{\lceil p/2 \rceil + 1}, b_2^i), (b_2^i, b_3^i), \dots, (b^i_{\lfloor p/2 \rfloor + 1}, b^i_{\lfloor p/2 \rfloor + 2}), (b^i_{\lfloor p/2 \rfloor + 2}, a_{\lceil p/2 \rceil + 1})\}$.



Let $k = \overline{Q(a_1)}$. This field is p-sufficient but not $(p+1)$-sufficient. Indeed, any extension ℓ of k such that $\delta(\ell : k) < 0$ must contain two petals, or the stem and one petal. In the first case at least $p+2$ algebraically independent elements must be added to k, and $p+1$ elements must be added in the second case.

Let a be the element $a_{\lceil p/2 \rceil + 1}$. The field $\overline{k(a)}$ is not $(\lceil p/2 \rceil - 1)$-sufficient because if the $(\lceil p/2 \rceil - 1)$ other elements $a_2, a_3, \dots, a_{\lceil p/2 \rceil}$ on the stem are added then there are $\lceil p/2 \rceil$ more points on the curve. We are therefore in case (i) of Lemma 2, and indeed $\ell = \overline{k(a_2, ..., a_{\lceil p/2 \rceil + 1})}$ satisfies the first condition of the lemma and is thus $\lfloor p/2 \rfloor$-sufficient. Adding a petal shows that this field is not $(\lfloor p/2 \rfloor + 1)$-sufficient. In fact, none of the extensions of $\overline{k(a)}$ of finite transcendence degree is $(\lfloor p/2 \rfloor + 1)$-sufficient because such an extension cannot include all petals.

Now we prove the optimality of case (ii) using the following example. Let $\{a_1, a_2^i, \ldots a^i_{\lceil p/2\rceil+1} | i \in \mathbf{N}\}$ be a set of algebraically independent elements and let C be the curve made of infinitely many petals:
$\{(a_1, a_2^i), (a_2^i, a_3^i), \ldots, (a^i_{\lceil p/2\rceil}, a^i_{\lceil p/2\rceil+1}), (a^i_{\lceil p/2\rceil+1}, a_1)\}$.



Let $k = \overline{Q}$. This field is $2\lceil p/2\rceil$-sufficient but not $(2\lceil p/2\rceil + 1)$-sufficient: it is p-sufficient if p is even and $p+1$-sufficient if p is odd. Indeed, any extension ℓ of k such that $\delta(\ell : k) < 0$ must contain two petals.

Let a be the element a_1. The field $\overline{k(a)}$ is clearly $(\lceil p/2\rceil - 1)$-sufficient but not $\lceil p/2\rceil$-sufficient. Any $\lceil p/2\rceil$-sufficient extension field of k must contain every a_i^j and must therefore be of infinite transcendence degree.

△

The remaining two lemmas of this section can be used to extend a local isomorphism (the first one when we are in the second case of Lemma 2). We have tried to prove these lemmas under fairly general hypotheses. This makes it possible to apply them not only to generic curves, but also to sequences of structures with the same limit theory, such as for instance: generic curves minus a point, generic curves plus a point, unions of generic curves...

Lemma 3 *Let (K, C) and (K', C') be two curved fields such that K' has infinite transcendence degree. Let k be a substructure of K of finite transcendence degree and $f : k \to k'$ an isomorphism of curved fields mapping k to a substructure k' of K'. Assume further that C' is a constructible subset of ${K'}^2$ (i.e., definable in the language of fields), and that $C \cap k^2$ is a finite set.*

Let a be an element of $K \setminus k$ such that $\ell = \overline{k(a)}$ satisfies $\delta(\ell : k) = 1$. There exists $a' \in K'$ and an isomorphism $g : l \to \ell' = \overline{k'(a')}$ which extends f. Moreover, if k' is p-sufficient for some integer $p \geq 1$, ℓ' is p-sufficient as well.

Proof: Let $\phi(x, y, \alpha)$ be the formula of the language of fields defining C', where α is a tuple of parameters. Let a' be an element of K' which is transcendent over $k'(\alpha)$. We show that $l' = \overline{k'(a')}$ satisfies $\delta(l' : k') = 1$, that is, there is no new point of the curve in ${l'}^2$. Assume by contradiction that (u, v) is a point of C' in ${\ell'}^2 \setminus {k'}^2$. There are two nonzero polynomials P and Q of $k'[X_1, X_2]$ such that $P(u, a') = 0$ and $Q(v, a') = 0$. Let $E = \{(a_i, b_i) | i \in I\}$ be the finite set of points of the curve with coordinates in k'. Consider the formula $\varphi(c)$ of the language of fields:

$$\exists x \exists y [P(x,c) = 0 \wedge Q(y,c) = 0 \wedge \phi(x,y,\alpha) \wedge \bigwedge_{i \in I} (x,y) \neq (a_i, b_i)]$$

The set Γ_1 of elements satisfying φ is finite or cofinite and a' belongs to it. Since a' is transcendent over the parameters of φ, we are in the case where Γ_1 is cofinite. Moreover, the set Γ_2 of elements $c \in K'$ such that the polynomials $P(.,c)$ and $Q(.,c)$ are both nonzero is cofinite as well. Thus there is an element of $\Gamma_1 \cap \Gamma_2$ in k'. We conclude that there exists a point $(x,y) \notin E$ on the curve with coordinates in k'. This is impossible by definition of E. Any fields isomorphism $g : \ell \to \ell'$ extending f is therefore an isomorphism of curved fields.

Let us now prove that l' is p-sufficient if k' is p-sufficient. Assume by contradiction that there exist $t \leq p$ points $(u_1, v_1), ..., (u_t, v_t)$ of $C' \setminus l'^2$ such that $(u_1, v_1, \ldots, u_t, v_t)$ has transcendence degree at most $t-1$ over l'. This tuple therefore lies on a variety of K'^{2t} of dimension $\leq t-1$ defined by a conjunction $\Psi(x_1, y_1, ..., x_t, y_t, a', \beta)$ of polynomial equations, where β is a tuple of parameters in k. Now we use a similar argument as in the first part of this proof: consider a formula $\theta(c)$ with parameters in $k'(\alpha)$ which states the existence of points $(x_1, y_1), \ldots, (x_t, y_t)$ on C', distinct from the points of E, with coordinates lying on the variety of K'^{2t} defined by $\Psi(., c, \beta)$. The set Γ_3 of elements of K' satisfying θ must be cofinite since a' is transcendent over the parameters of θ, and satisfies this formula. Moreover, the set Γ_4 of elements $c \in K'$ such that $\Psi(., c, \beta)$ defines a variety of dimension $\leq t-1$ is cofinite as well. Thus there is an element of $\Gamma_3 \cap \Gamma_4$ in k'. We conclude that there exist t points on $C' \setminus k'^2$ whose coordinates have transcendence degree at most $t-1$ over k'. This is impossible since k' is p-sufficient.

$\triangle$

The final lemma of this section will be used when we are in the first case of Lemma 2.

Lemma 4 *Let (K, C) and (K', C') be two curved fields. Let k be a substructure of K of finite transcendence degree and $f : k \to k'$ an isomorphism of curved fields mapping k to a substructure k' of K'.*

Let $l \subseteq K$ be an extension of k of transcendence degree $n \geq 1$ over k, such that $\delta(l : k) = 0$. Assume further that k and k' are n-sufficient, and that C' satisfies $AE'(n, [k : Q])$. There exists an extension l' of k' and an isomorphism $g : l \to l'$ extending f.

Note that the condition $\delta(l : k) = 0$ implies $\delta(l' : k') = 0$ since g is an isomorphism. This condition implies in turn that l' is $(p - [l' : k'])$-sufficient if k' is p-sufficient for some integer $p > [l : k]$.

Proof of Lemma 4: Since $\delta(l : k) = 0$, there are exactly n points $(a_1, b_1), \ldots, (a_n, b_n)$ on the curve in $l^2 \setminus k^2$. By Lemma 1, there exists a transcendence base of $k(a_1, b_1, \ldots, a_n, b_n)$ over k which is made of n coordinates $c_1 \in \{a_1, b_1\}, \ldots, c_n \in \{a_n, b_n\}$. We can view $(a_1, b_1, \ldots, a_n, b_n)$ as a generic point of an irreducible variety $V_z \subseteq K^{2n}$ defined by a conjunction $\phi(x, y, z)$ of polynomial equations. Here z is a tuple of parameters from k, and we can assume without loss of generality that $k = \overline{Q(z)}$. Since $c_1, \ldots, c_n$ are algebraically independent over k, the projection of V_z on the corresponding variables must be dense in K^n. We conclude that z satisfies formula Ψ from (1). The image z' of z by f must satisfy the same formula since f is an isomorphism. For the same reason, $k' = \overline{Q(z)}$. Since C' satisfies $AE'(n, [k:Q])$, there exist n points $(a'_1, b'_1), \ldots, (a'_n, b'_n)$ on C' such that $K' \models \phi(a'_1, b'_1, \ldots, a'_n, b'_n, z')$ and one can choose n coordinates $c'_1 \in \{a'_1, b'_1\}, \ldots, c'_n \in \{a'_n, b'_n\}$ which are algebraically independent over k'. Let l' be the algebraic closure of $k'(a'_1, b'_1, \ldots, a'_n, b'_n)$. Since V_z is an irreducible variety, there exists a fields isomorphism $g: l \to l'$ which extends f, and maps $a_1, b_1, \ldots, a_n, b_n$ to $a'_1, b'_1, \ldots, a'_n, b'_n$. This implies in particular that $(a'_1, b'_1), \ldots, (a'_n, b'_n)$ are n distinct points, since $(a_1, b_1), \ldots, (a_n, b_n)$ are distinct. We claim that g is in fact an isomorphism of curved fields. To prove this claim we have to show that $(a'_1, b'_1), \ldots, (a'_n, b'_n)$ are the only points on the curve in $l'^2 \setminus k'^2$. This follows from the hypothesis that k' is n-sufficient.

$\triangle$

5 Limit Theorems

Our limit theorems are fairly straightforward consequences of the following fact.

Theorem 1 *Let k_j be a substructure of (K, C_d) of finite transcendence degree Δ_j. Let $\sigma_j : k_j \to k'_j$ be an isomorphism of curved fields mapping k_j to a substructure k'_j of $(K', C_{d'})$. If k_j and k'_j are $(2^j - 1)$-sufficient, σ_j is a j-isomorphism as soon as the following condition is satisfied:*

$$(H_j) \qquad \min(d, d') \geq 2^{j-1}(2^j + \Delta_j + 1) - 1.$$

Proof: by induction on j. There is nothing to prove for $j = 0$, so let us assume that $j \geq 1$. We first observe that (H_j) implies that $k_j^2 \cap C_d$ is a finite set, of cardinality bounded by Δ_j. Indeed, since $d \geq \Delta_j$ we know from section 3 that the coordinates of any set of $\Delta_j + 1$ points on the curve are of transcendence degree at least $\Delta_j + 1$.

By symmetry it suffices to show that for any $a \in K \setminus k_j$ there exists a $(j-1)$-isomorphism which extends σ_j, and is defined in a. By Lemma 2 there exists a $(2^{j-1} - 1)$-sufficient structure k_{j-1} which contains $k_j \cup \{a\}$.

Assume first that we are in case (i) of Lemma 2. We know from hypothesis (H_j) that C_d satisfies $AE'(2^{j-1}, \Delta_j)$. Since k_{j-1} is of transcendence degree at most 2^{j-1} over k_j we can apply Lemma 4: there exists an extension k'_{j-1} of k'_j and an isomorphism $\sigma_{j-1} : k_{j-1} \to k'_{j-1}$ which extends σ_j. Hypothesis (H_j) clearly implies (H_{j-1}): if Δ_{j-1} denotes the transcendence degree of k_{j-1} over the prime field then $\Delta_{j-1} \leq \Delta_j + 2^{j-1}$ so that $\Delta_{j-1} + 2^{j-1} \leq \Delta_j + 2^j$. Moreover, k'_j is $[(2^j - 1) - 2^{j-1}]$-sufficient by the remark after Lemma 4. We can therefore conclude from the induction hypothesis that σ_{j-1} is a $(j-1)$-isomorphism.

Case (ii) of Lemma 2 is similar: we take for k_{j-1} the algebraic closure of $k(a)$, and Lemma 3 yields a $(2^j - 1)$-sufficient substructure k_{j-1} and an isomorphism $\sigma_{j-1} : k_{j-1} \to k'_{j-1}$ which extends σ_j. Since k'_j is of transcendence degree $\Delta'_j \leq \Delta_j + 1$, hypothesis (H_j) also implies (H_{j-1}). We conclude again from the induction hypothesis that σ_{j-1} is a $(j-1)$-isomorphism.

$\triangle$

Theorem 2 *(K, C_d) and $(K', C_{d'})$ satisfy the same (closed) formulas of quantifier rank r as soon as $\min(d, d') \geq 2^{r-1}(2^r + 1) - 1$.*

Proof: K and K' both contain $\overline{Q}$, the algebraic closure of the prime field. Let σ_r be the identity on $\overline{Q}$. By $A(1)$ no point on C_d or in $C_{d'}$ can have both coordinates in $\overline{Q}$, so that σ_r can be viewed as a partial isomorphism of curved fields from K to K'. We also know from section 3 that $\overline{Q}$ is d-sufficient (respectively, d'-sufficient) in K (respectively, in K'). Hence $\overline{Q}$ is $(2^r - 1)$-sufficient in both structures. We conclude from Theorem 1 that σ_r is an r-isomorphism, and both structures therefore satisfy the same formulas of quantifier rank r. △

It turns out that the above bound is fairly tight.

Theorem 3 *If $d > d'$ there is a closed formula ϕ of quantifier rank $1 + \lceil \log_2 d \rceil$ such that $(K, C_d) \models \phi$ but $(K, C_{d'}) \not\models \phi$.*

Proof Sketch: In words, ϕ states that the curve intersects the $\{y = 0\}$ axis in (at least) d distinct points. The obvious formula for this has quantifier rank d:

$$\exists x_1, \ldots, x_d \bigwedge_{i=1}^{d} C(x_i, 0) \wedge \bigwedge_{i<j} x_i \neq x_j.$$

But there is a better way [4]: the fact that $C \cap \{y = 0\}$ has cardinality at least d can be expressed by a formula of quantifier rank $1 + \lceil \log_2 d \rceil$. Here we use the fact that the intersection points of C_d with the horizontal axis are algebraically independent over the prime field (in fact linear independence would be enough, again see [4]). △

Theorem 2 reduces the decision problem for the limit theory to a problem about algebraically closed fields: a closed formula F of the language of curved fields, of quantifier rank r, is true in the limit theory if and only if $(K, C_d) \models F$ where $d = 2^{r-1}(2^r + 1) - 1$. We can therefore construct a formula $F_d(a)$ of the language of fields such that F is true in the limit theory if and only if $K \models F_d(a)$. Here a is a tuple of $(d+1)(d+2)/2$ algebraically independent parameters.

There are several slightly different ways of deciding whether $K \models F_d(a)$. The most straightforward approach is to eliminate quantifiers in F_d to obtain an equivalent quantifier-free formula $G_d(a)$. One may consult [5] on quantifier elimination in algebraically closed fields; more recent algorithms are faster when the input formula in prenex form has few quantifier alternations, see e.g. [3]. An atomic subformula of $G_d(a)$ of the form $P(a) = 0$ is true iff P is identically zero. Alternatively, we may apply directly a decision algorithm for the "extended first order theory of K" (*extended* means that arbitrary parameters from K are allowed). When the decision algorithm performs a test of the form "$P(a) = 0$?" we have to decide whether P is identically zero. Yet another solution would be to replace the algebraically independent parameters by random integers, in the spirit of [9] (bounds on the size of the integers to be used can be obtained by quantifier elimination). As this is not the main point of our paper, we leave it to the reader to work out complexity bounds for these decision algorithms.

We have seen in Theorem 2 that two curves of "high" degree cannot be distinguished by a formula of "small" quantifier rank. One can also show that it is hard to distinguish a curve from a curve minus a point.

Theorem 4 *Let C'_d be the "curve" $C_d \setminus \{(a,b)\}$ where (a,b) is a point on the generic curve $C_d \subseteq K^2$.*

Let $\sigma_j : k_j \to k'_j$ be an isomorphism of curved fields mapping k_j to a substructure k'_j of (K, C'_d). If k_j and k'_j are $(2^j - 1)$-sufficient, σ_j is a j-isomorphism as soon as $d \geq 2^{j-1}(2^j + \Delta_j + 3) - 1$.

The only difference with the proof of Theorem 1 is that C'_d satisfies $AE'(n, \Delta)$ only for $d \geq n(2n + \Delta + 3) - 1$ (see end of section 3). By the same argument as for Theorem 2 we then obtain a quantitative version of another result of [2].

Theorem 5 *Let (a,b) be a point on the generic curve C_d. (K, C_d) and $(K, C_d \setminus \{(a,b)\})$ satisfy the same (closed) formulas of quantifier rank r as soon as $d \geq 2^{r-1}(2^r + 3) - 1$.*

From the fact that a curve cannot be distinguished from a curve minus a point, it was shown in [2] that a curve cannot be distinguished from a curve plus a point. We can give a direct quantitative proof of this result.

Theorem 6 *Let (a,b) be a point of transcendence degree at least one over the coefficients of the generic curve C_d. (K, C_d) and $(K, C_d \cup \{(a,b)\})$ satisfy the same (closed) formulas of quantifier rank r as soon as $d \geq 2^{r-1}(2^r + 1) - 1$.*

The proof is identical to the proof of Theorem 2. First of all, it is clear that if $AE'(n, \Delta)$ is satisfied by C_d this property is also satisfied by any superset of C_d. For universal axioms, there is a little more work to be done:

Lemma 5 *Let (a,b) be a point of transcendence degree at least one over the coefficients of the generic curve C_d. For $n \leq d+1$, n distinct points $(x_1, y_1), \ldots, (x_n, y_n)$ which belong to $C_d \cup \{(a,b)\}$ always have transcendence degree at least n over the prime field.*

Proof: We already know that the result is true if our n points are distinct from (a,b). Let us therefore assume that $(x_n, y_n) = (a,b)$, and let $\overline{c}$ be the tuple of the $N = (d+1)(d+2)/2$ parameters of C_d. It is shown in the proof of Corollaire 6 of [2] that $\overline{c}$ is of transcendence degree at most $N - (n-1)$ over $Q(x_1, y_1, \ldots, x_{n-1}, y_{n-1})$. This implies that the tuple $\overline{c}\hat{\ }a\hat{\ }b$ is of transcendence degree at most $N - (n-1)$ over $Q(x_1, y_1, \ldots, x_{n-1}, y_{n-1}, a, b)$. Since $\overline{c}\hat{\ }a\hat{\ }b$ is of transcendence degree at least $N+1$ over Q, we conclude that the transcendence degree of $Q(x_1, y_1, \ldots, x_{n-1}, y_{n-1}, a, b)$ is at least $(N+1) - (N - (n-1)) = n$. $\triangle$

One can give other results of this kind, for instance:

Theorem 7 *Let (a,b) be a point of transcendence degree two over the coefficients of the generic curve C_d. (K, C_d) and $(K, C_d \cup \{(a,b), (b,a)\})$ satisfy the same (closed) formulas of quantifier rank r as soon as $d \geq 2^{r-1}(2^r + 1) - 1$.*

The proof is similar to the proof of Theorem 6. Lemma 5 is replaced by a lemma with a similar proof, which is left to the reader. This lemma will also be used in the proof of Theorem 9.

Lemma 6 *Let (a,b) be a point of transcendence degree two over the coefficients of the generic curve C_d. For $n \leq d+1$, n distinct points $(x_1,y_1),\dots,(x_n,y_n)$ which belong to $C_d \cup \{(a,b),(b,a)\}$ always have transcendence degree at least n over the prime field.*

6 Elimination of Quantifier Alternations

We need a generalization of Lemma 2.

Lemma 7 *Let k be a p-sufficient substructure of a curved field (K,C) and $a=(a_1,\dots,a_n)$ a tuple of n elements of $K\backslash k$. Set $q=\lfloor\frac{p-n}{n+1}\rfloor$. Let j be the smallest integer such that there exists an extension ℓ of $k(a)$ satisfying $\delta(\ell:k)\leq j$ and $[\ell:k]\leq p-q(j+1)$. Then ℓ is q-sufficient.*

Note that we may assume that $p \geq 2n+1$. Otherwise there is nothing to prove since $q=0$. Note also that repeated applications of Lemma 2 would only yield a $(p/2^n)$-sufficient extension at best.

Proof: Note that j always exists and is upper bounded by n. This follows from the inequalities $\delta(\overline{k(a)}:k)\leq n$ and $[\overline{k(a)}:k]\leq n\leq p-q(n+1)$. Let f be an extension of l such that $[f:\ell]\leq q$. We have to show that $\delta(f:\ell)\geq 0$. Consider first the case $j=0$. Then $\delta(\ell:k)=0$ and $\delta(f:k)\geq 0$ since k is p-sufficient and $[f:k]\leq(p-q)+q=p$. Hence $\delta(f:\ell)=\delta(f:k)-\delta(\ell:k)\geq 0$. Assume now that $j>0$. Since $[f:k]\leq p-qj$ we must have $\delta(\ell:k)>j-1$ by minimality of j. Since $\delta(\ell:k)\leq j$ we conclude again that $\delta(f:\ell)\geq 0$. △

We shall need the following fact about algebraically closed fields.

Fact 1 *Let $c=(c_1,\dots,c_r)$ be a point of K^r. This point satisfies a conjunction $\phi(c)$ of polynomial equations with coefficients in the prime field, such that:*

(i) The transcendence degree over Q of any point c' of K^r which satisfies ϕ is upper bounded by the transcendence degree of c.

(ii) If c' satisfies ϕ and has the same transcendence degree as c, there is an isomorphism of fields $\sigma: Q(c)\to Q(c')$ which sends c to c'.

Proposition 1 *Let $a=(a_1,\dots,a_n)$ and $a'=(a'_1,\dots,a'_n)$ be two tuples of models (K,C) and (K',C') of the limit theory of generic curves. If a and a' satisfy the same existential formulas with at most $2p$ quantifiers, there exists an isomorphism of curved fields $\sigma:\ell\to\ell'$ between a q-sufficient extension ℓ of $Q(a)$ and a q-sufficient extension ℓ' of $Q(a')$, where $q=\lfloor\frac{p-n}{n+1}\rfloor$.*

Proof: We shall see that it suffices to consider existential formulas of the form:

$$\exists x_1,y_1,\dots,x_m,y_m \bigwedge_{i=1}^{m} C(x_i,y_i)\wedge\bigwedge_{i\neq j}(x_i,y_i)\neq(x_j,y_j)\wedge\phi(a,x,y)$$

where ϕ is a conjunction of polynomial equations in $2m+n$ variables, with coefficients in Q.

Let ℓ be the q-sufficient extension of $Q(a)$ obtained from Lemma 7. Let $(\alpha_1, \beta_1), \ldots, (\alpha_m, \beta_m)$ be the points of ℓ^2 on the curve, and ϕ the conjunction of polynomial equations obtained by an application of Fact 1 to the tuple $c = a\hat{\ }\alpha\hat{\ }\beta$. By hypothesis, we can find in K' distinct points $(\alpha'_1, \beta'_1), \ldots, (\alpha'_m, \beta'_m)$ on the curve such that the tuple $c' = a'\hat{\ }\alpha'\hat{\ }\beta'$ satisfies ϕ. We claim that c' has same transcendence degree as c: if it had a smaller transcendence degree, by another application of our hypothesis we could find in K distinct points $(\lambda_1, \mu_1), \ldots, (\lambda_m, \mu_m)$ on the curve such that $a\hat{\ }\lambda\hat{\ }\mu$ has smaller transcendence degree than $a\hat{\ }\alpha\hat{\ }\beta$. This would contradict the minimality of j in Lemma 7. We conclude from Fact 1 that there exists an isomorphism of fields $\tau : \ell \rightarrow \overline{Q(c')}$ which sends c to c'. Again by minimality of j, there are only m points on the curve with both coordinates in $l' = \overline{Q(c')}$, so that τ is in fact an isomorphism of curved fields.

A similar argument shows that there cannot exist an integer $j' < j = \delta(\ell : k)$ and an extension ℓ'' of $Q(a')$ such that $[\ell'' : Q] \leq p - q(j'+1)$ and $\delta(\ell'' : Q) \leq j'$. By Lemma 7, ℓ' is therefore q-sufficient in K'.

$\triangle$

In the proof of the next theorem we use ω-saturated models, which always exist for consistent theories (see [7], Theorem 5.01, or [6], Corollary 10.2.2). Recall that a model M is ω-saturated if for any family $\mathcal{F}$ of formulas in a fixed number of free variables, with parameters from a fixed finite subset of M, if $\mathcal{F}$ is not satisfiable in M then there exists a finite subset of $\mathcal{F}$ which is not satisfiable in M.

Theorem 8 *Let F be a formula of the language of curved fields of quantifier rank r with n free variables. In the limit theory of generic curves, F is equivalent to a boolean combination of existential formulas where each existential formula has at most $2n + 2(n+1)(2^r - 1)$ quantifiers.*

Proof: Let a and a' be two n-tuples of ω-saturated models (K, C) and (K', C') of the limit theory. Assume that a and a' satisfy the same existential formulas with at most $2n + 2(n+1)(2^r - 1)$ quantifiers. By Proposition 1 there exists an isomorphism of curved fields $\sigma : \ell \rightarrow \ell'$ between a $(2^r - 1)$-sufficient extension ℓ of $Q(a)$ and a $(2^r - 1)$-sufficient extension ℓ' of $Q(a')$. We have seen in Theorem 1 that such a σ is an r-isomorphism if C and C' are generic curves of high enough degree. In ω-saturated models of the limit theory this condition on degrees disappears and we conclude that a and a' satisfy the same formulas of quantifiers at most r (see [2] for more details on back-and-forth systems between models of the limit theory). It then follows from a standard argument that F must be equivalent to a boolean combination of existential formulas with at most $2n + 2(n+1)(2^r - 1)$ quantifiers (see Thorme 5.03 of [7]). For the sake of completeness we give a proof below.

Let $\mathcal{F}$ be the family of all formulas of the form

$$(\phi(x) \leftrightarrow \phi(y)) \wedge \neg(F(x) \leftrightarrow F(y))$$

where ϕ is an existential formula with at most $2n + 2(n+1)(2^r - 1)$ quantifiers and n free variables. We have just shown that $\mathcal{F}$ is not satisfiable in K. Since K is ω-saturated there exists a finite subset of $\mathcal{F}$ which is not satisfiable in K. This implies that F is equivalent in K (and in all other models since the limit theory is complete) to a boolean combination of formulas from this finite subset. $\triangle$

In a sense, this theorem is as good as possible since there exist formulas which are not equivalent to existential formulas:

Theorem 9 *In the limit theory of generic curves, the universal formula* $\forall y \neg(C(x,y) \wedge C(y,x))$ *is not equivalent to an existential formula.*

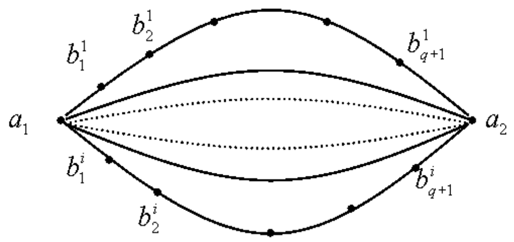
Proof: Assume by contradiction that there exists an existential formula $E(x)$ such that $T \vdash \forall x\ A(x) \leftrightarrow E(x)$, where T is the limit theory and $A(x) \equiv \forall y \neg(C(x,y) \wedge C(y,x))$. By compactness there exists a finite subset Δ of T such that $\Delta \vdash \forall x\ A(x) \leftrightarrow E(x)$. We will now construct two models M and N of Δ with $M \subset N$ such that there exists $a \in M$ such that $M \models A(a)$ but $N \not\models A(a)$. This yields a contradiction because $M \models E(a)$ implies $N \models E(a)$ since E is existential.

The small model M will consist of a generic curve of degree d drawn on an algebraically closed field with transcendence basis $\overline{c}\,\hat{}\,a$, where $\overline{c}$ is the tuple of coefficients of the generic curve. By definition of the limit theory, M is a model of Δ if d is large enough. Let N be the algebraic closure of $M \cup \{b\}$, where b is algebraically independent of M. The curve on M consists of $C_d \cup \{(a,b),(b,a)\}$ where C_d is the algebraic curve with same tuple of coefficients $\overline{c}$ as the curve on M. It follows from section 5 (Lemma 6) that N is also a model of Δ if d is large enough. We can now conclude. Since a is algebraically independent of $\overline{c}$, $M \models \forall y\ \neg(C(a,y) \wedge C(y,a))$, but N is constructed so that $N \models \exists y\ (C(a,y) \wedge C(y,a))$. $\triangle$

6.1 Optimality of Lemma 7

In this subsection we establish the optimality of Lemma 7. This property will not be used in the remainder of the paper.

For the case $n = 1$ the optimality is given by the flower of Lemma 2. Let $n = 2$ and $q = \lfloor \frac{p-2}{3} \rfloor$. Let $\{a_1, a_2\} \cup \{b_1^i, \ldots b_{q+1}^i | i \in \mathbf{N}\}$ be a set of algebraically independent elements. The curve C is a melon made of the lines $\{(a_1, b_1^i), (b_1^i, b_2^i) \ldots, (b_q^i, b_{q+1}^i), (b_{q+1}^i, a_2)\}$.



It is clear that the field $\ell = Q(a_1, a_2)$ is q-sufficient and not $(q+1)$-sufficient, and that there is no finite transcendence degree extension of ℓ that can be $(q+1)$-sufficient. To show the optimality of the lemma we have to prove that the field $k = Q$ is $[3(q+1)+1]$-sufficient and so p-sufficient. Let k be a field such that $[k : Q] = r$ and $r \leq 3(q+1)+1$ and let γ be the curve on k, which is the set of edges of a melon subgraph S. We want to show that $\delta(k : Q) \geq 0$, which means that S has at most r edges. The vertices of the graph belonging to k are exactly r. Consider a connected component of S. If it contents at most one path from a_1 to a_2 then it has one vertex more than edges. If there are two path from a_1 to a_2 then the number of vertices is equal to the number of edges. It is not possible to have three or more paths from a_1 to a_2 because a path has $(q+1)$ vertices except a_1 and a_2 and the total number of vertices is at most $[3(q+1)+1]$. So $\delta(k : Q)$ is between 0 and the number of connected component and thus is positive. $\triangle$

The next proposition takes care of the case $n = 3$.

Proposition 2 *Let p be an integer greater or equal to 7 and let $q = \lfloor \frac{p-3}{4} \rfloor$. There is a curve C on a field K with infinite transcendence degree and some scalar a_1, a_2, a_3 of K satisfying the following conditions:*

(a) *Q is at least p-sufficient;*

(b) *$Q(a_1, a_2, a_3)$ is q-sufficient;*

(c) *$Q(a_1, a_2, a_3)$ has no $(q+1)$-sufficient extension of finite transcendence degree.*

Proof: Let a_1, a_2, a_3 be algebraically independent elements of K. The equilateral triangle T_1 is a cyclic graph with $3(q+1)+3$ edges, and $3(q+1)+3$ vertices which are also elements of K. Let a_1, a_2, a_3 be the three corners of T_1. The first side of T_1 is made of the vertices $a_1, b^1_{1,1}, ..., b^1_{1,q+1}, a_2$, the second side is made of $a_2, b^1_{2,1}, ..., b^1_{2,q+1}, a_3$ and the third of $a_3, b^1_{3,1}, ..., b^1_{3,q+1}, a_1$. All vertices are algebraically independent elements of K. The triangle T_1 represents the curve:

$$(a_1, b^1_{1,1}), ..., (b^1_{1,q+1}, a_2), (a_2, b^1_{2,1}), ..., (b^1_{2,q+1}, a_3), (a_3, b^1_{3,1}), ..., (b^1_{3,q+1}, a_1)$$

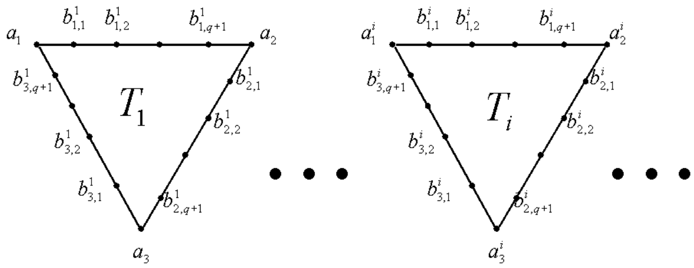
We define now a sequence $(T_i)_{i\geq 1}$ of triangles. Every T_i is isomorphic (in the sense of curved fields) to T_1. The corners a^{i+1}_1, a^{i+1}_2 and a^{i+1}_3 of T_{i+1} are such that:

$$a^{i+1}_1 = a^i_1 + \sum_{k=1,\dots,q+1} b^i_{1,k}$$

$$a^{i+1}_2 = a^i_2 + \sum_{k=1,\dots,q+1} b^i_{2,k}$$

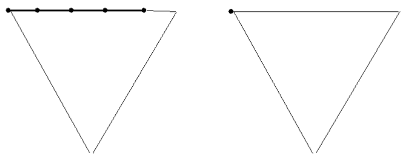
$$a^{i+1}_3 = a^i_3 + \sum_{k=1,\dots,q+1} b^i_{3,k}$$

They are therefore equal to the sum of the vertices of one side minus one extremity of the preceding triangle. The other vertices $b_{j,k}^{i+1} (j = 1, 2, 3; k = 1, ..., q+1)$ of T_{i+1} are algebraically independent over the edges of all preceding triangles. Now let the curve C be the union of all $T_i (i \geq 1)$.



We shall prove that C verifies the three conditions of the proposition. Conditions (b) and (c) are clear. We prove (a). Let k be a field such that $[k : Q] = r$ and $r \leq p$. Then $r \leq 4(q+1)+2$. We want to show that $\delta[k : Q] \geq 0$.

For every $i \geq 1$ let $t_i = T_i \cap k^2$. Let $k_0 = \overline{Q}$. The increasing sequence of algebraically closed fields $(k_i)_{i \in \mathbf{N}}$ is defined by the following: k_{i+1} is the algebraically closed field generated over k_i by the vertices of t_{i+1}. Since the transcendence degree of k is finite there exists an integer u such that $k = k_u$, and the sequence is constant thereafter. The field k_i may contain some corners of T_{i+1}. In fact for $j \in \{1, 2, 3\}$ we have $a_j^{i+1} \in k_i$ if and only if $\{a_j^i, b_{j,1}^i, ..., b_{j,q+1}^i\} \subseteq k_i$. This set is called a quasi-side of T_i. Moreover if $a_j^{i+1} \notin k_i$ and $a_{j'}^{i+1} \notin k_i$ for $j \neq j'$ then they are algebraically independent over k_i. This is easy to prove using $a_j^{i+1} = a_j + \sum_{h=1,...,i} \sum_{k=1,...,q+1} b_{1,k}^h$. Also if $a_1^{i+1} \notin k_i$, $a_2^{i+1} \notin k_i$ and $a_3^{i+1} \notin k_i$ then they are algebraically independent over k_i.



Quasi-side and its associated corner

Let $i \geq 1$. There are zero, one, two or three quasi-sides of T_i in t_i. If t_i has no quasi side then $\delta(k_{i+1} : k_i) \geq 0$. Indeed there is no vertex of t_{i+1} in k_i. Thus the number of vertices of t_{i+1} is equal to $[k_{i+1} : k_i]$ and the number of edges of t_{i+1} is smaller or equal. More precisely $\delta(k_{i+1} : k_i) = 0$ if t_{i+1} is empty or equal to the whole triangle T_{i+1}, and $\delta(k_{i+1} : k_i) > 0$ otherwise.

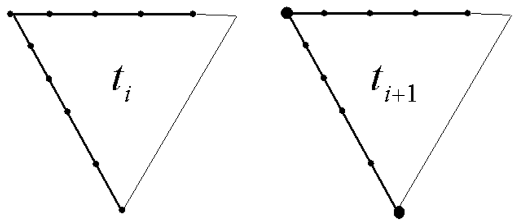
If t_i has exactly one quasi-side then $\delta(k_{i+1} : k_i) \geq 0$. In fact exactly one corner of t_{i+1} is in k_i. The other vertices of t_{i+1} are algebraically independent over k_i. The curve t_{i+1} is not the whole triangle T_{i+1} because of the small transcendence degree of k: $[k_{i+1} : k_i] + [k_i : Q] \leq [k : Q] \leq 4(q+1)+2$ and

$[k_i : Q] \geq (q+1)+1$ and so $[k_{i+1} : k_i] \leq 3(q+1)+1$. Thus t_{i+1} has no cycle and $\delta(k_{i+1} : k_i) \geq 0$.

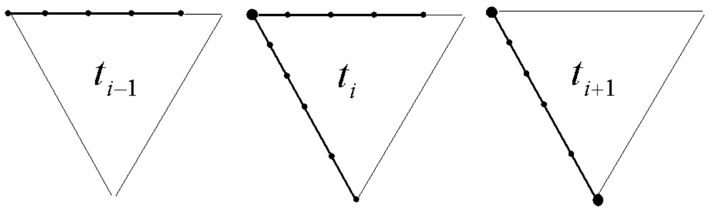
We examine now the case where two distinct t_i's contain two quasi-sides. Suppose $i < i'$ are integers such that t_i and $t_{i'}$ have two quasi-sides. Thus $[k_i : Q] \geq 2(q+1)+2$ and $[k_{i'} : k_i] \geq 2(q+1)$. Also:

$$4(q+1)+2 \leq [k_{i'} : k_i] + [k_i : Q] \leq [k : Q] \leq 4(q+1)+2$$

These inequalities are therefore equalities: $[k_i : Q] = 2(q+1)+2$, $[k_{i'} : k_i] = 2(q+1)$, $i' = i+1$ and the curve on k is the union of t_i and t_{i+1}. We conclude that $\delta(k : Q) = 0$.



In all other cases there is at most one t_i with at least two quasi-sides. In the case where t_i has exactly two quasi-sides we shall see that $\delta(k_{i+1} : k_i) \geq 0$, $\delta(k_{i+1} : k_{i-1}) \geq 0$ or $\delta(k_{i+1} : k_{i-2}) \geq 0$. Suppose $\delta(k_{i+1} : k_i) < 0$ and there is no $t_{i'}$ with two quasi-sides. In particular, t_{i-1} and t_{i+1} have zero or one quasi-side and $\delta(k_{i+1} : k_i) \geq -1$. Suppose first that t_{i-1} has no quasi-side. Then $\delta(k_i : k_{i-1}) \geq 1$ and $\delta(k_{i+1} : k_{i-1}) \geq 0$. Suppose now that t_{i-1} has exactly one quasi-side. Then $[k_{i-1} : Q] \geq (q+1)+1$, $[k_i : k_{i-1}] \geq 2(q+1)+1$, $[k_{i+1} : k_{i-1}] \geq (q+1)$. This implies that $[k : Q] \geq 4(q+1)+2$ and that the inequalities are all equalities. Moreover $k = k_{i+1}$. We have $\delta(k_{i-1} : Q) = 1$, $\delta(k_i : k_{i-1}) = 0$, $\delta(k_i : k_{i-1}) = -1$ and then $\delta(k : Q) = 0$.



If t_i is the whole triangle then $[k_i : Q] \leq 3(q+1)+3$ and $[k_{i+1} : k_i] \leq q$. No two corners of T_{i+1} are in the same connected component of t_{i+1} and $\delta(k_{i+1} : k_i) \geq 0$.

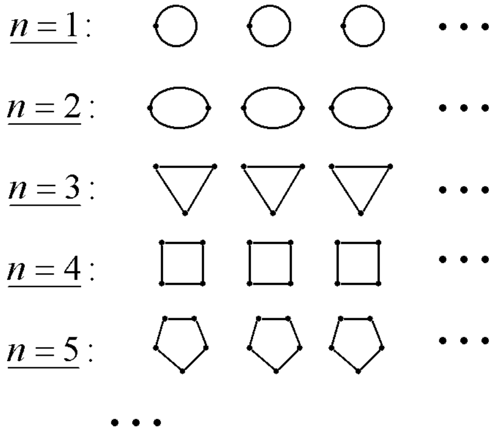
As a conclusion:

$$\delta(k : Q) = \delta(k_u : k_{u-1}) + \ldots + \delta(k_1 : Q) \geq 0$$

$\triangle$

This construction can be generalized to any $n \geq 1$ and $p \geq 2n+1$. The curve C is the union of a sequence of n-gons. The sides of all n-gons have

$q+1 = 1 + \lfloor \frac{p-n}{n+1} \rfloor$ points in addition to their extremities. It can be shown as in Proposition 2 that C is p-sufficient. Moreover, the curved field $Q(a_1, \ldots, a_n)$ is q-sufficient and has no $(q+1)$-sufficient extension of finite transcendence degree.



7 Existential Formulas

In this paper we have used quantifier rank as a measure of the "complexity" of a formula. There are other possibilities. For instance, it is frequently assumed in algorithmic investigations that the input formula is in prenex form. The number and lengths of quantifiers blocks are then used as parameters (see for instance [1, 3, 8]). To illustrate how this could be done for generic curves, we now consider the special case of existential formulas.

Proposition 3 *Let (K, C) and (K', C') be two curved fields. Assume that K' has infinite transcendence degree and that the coordinates of any set of $j \leq n+1$ points on C (respectively, C') have transcendence degree at least j. Assume further that C' is a constructible subset of ${K'}^2$ and satisfies all the inductive axioms $AE'(m, \Delta)$ with $m + \Delta = n$.*

Let l be a substructure of K of transcendence degree n. There exists a substructure l' of K' and an isomorphism of curved fields $g : l \to l'$.

Proof: Let $(a_1, b_1), \ldots, (a_m, b_m)$ be the $m \leq n$ points in $C \cap l^2$. By Lemma 1 there exists a transcendence basis of l of the form $t \,\hat{}\, z$ where $t_i \in \{a_i, b_i\}$ for each component of the m-tuple t. Let k be the algebraic closure of $Q(z)$. Note that there are no points on the curve in k^2, and that k is m-sufficient in l. By $n - m$ applications of Lemma 3 we can find a n-sufficient substructure k' of K' and an isomorphism of curved fields $f : k \to k'$. Now we apply Lemma 4 to obtain an isomorphism of curved fields $g : l \to l'$ which extends f. $\triangle$

It follows that two generic curves C_d and $C_{d'}$ satisfy the same existential formulas with n quantifiers as soon as $\min(d, d') \geq n(2n+1) - 1$. Note that Theorem 2 yields only the much worse bound $\min(d, d') \geq 2^{n-1}(2^n + 1) - 1$.

References

[1] S. Basu, R. Pollack and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of the ACM*, 43(6):1002-1045, 1996.

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

[3] N. Fichtas, A. Galligo, and J. Morgenstern. Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *Journal of Pure and Applied Algebra*, 67:1–14, 1990.

[4] H. Fournier. Exprimer la parit. preprint, 2000.

[5] J. Heintz. Definability and fast quantifier elimination over algebraically closed fields. *Theoretical Computer Science*, 24:239–277, 1983.

[6] W. Hodges. *Model theory.* Cambridge University Press, 1993.

[7] B. Poizat. *Cours de théorie des modèles.* Nur Al-Mantiq Wal-ma'rifah, 1985.

[8] J. Renegar. On the Computational Complexity and Geometry of the First-order Theory of the Reals. Parts I, II, III. *Journal of Symbolic Computation*, 13(3):255-352, 1992.

[9] J. T. Schwarz. Fast probabilistic algorithms for verification of polynomials identities. *Journal of the ACM*, 27:701–717, 1980.