On the intersection of a sparse curve and a low-degree curve: A polynomial version of the lost theorem

Pascal Koiran, Natacha Portier, Sébastien Tavenas

On the intersection of a sparse curve and a low-degree curve: A polynomial version of the lost theorem

Pascal Koiran, Natacha Portier, and Sébastien Tavenas

LIP*, École Normale Supérieure de Lyon

October 9, 2013

Abstract

Consider a system of two polynomial equations in two variables:

$$F(X,Y) = G(X,Y) = 0$$

where $F \in \mathbb{R}[X,Y]$ has degree $d \geq 1$ and $G \in \mathbb{R}[X,Y]$ has t monomials. We show that the system has only $O(d^3t + d^2t^3)$ real solutions when it has a finite number of real solutions. This is the first polynomial bound for this problem. In particular, the bounds coming from the theory of fewnomials are exponential in t, and count only nondegenerate solutions. More generally, we show that if the set of solutions is infinite, it still has at most $O(d^3t + d^2t^3)$ connected components.

By contrast, the following question seems to be open: if F and G have at most t monomials, is the number of (nondegenerate) solutions polynomial in t?

The authors' interest for these problems was sparked by connections between lower bounds in algebraic complexity theory and upper bounds on the number of real roots of "sparse like" polynomials.

1 Introduction

Descartes' rule of signs shows that a real univariate polynomial with $t \geq 1$ monomials has at most $t-1$ positive roots. In 1980, A. Khovanskii [10] obtained a far reaching generalization. He showed that a system of n polynomials in n variables involving $l+n+1$ distinct monomials has less than

$$2^{\binom{l+n}{2}}(n+1)^{l+n} \tag{1}$$

*UMR 5668 ENS Lyon - CNRS - UCBL - INRIA, Université de Lyon, {pascal.koiran,natacha.portier,sebastien.tavenas}@ens-lyon.fr

non-degenerate positive solutions. Like Descartes', this bounds depends on the number of monomials of the polynomials but not on their degrees.

In his theory of fewnomials (a term coined by Kushnirenko), Khovanskii [10] gives a number of results of the same flavor; some apply to non-polynomial functions. In the case of polynomials, Khovanskii's result was improved by Bihan and Sottile [3]. Their bound is

$$\frac{e^2+3}{4} 2^{\binom{l}{2}} n^l. \tag{2}$$

In this paper, we bound the number of real solutions of a system

$$F(X,Y) = G(X,Y) = 0 \tag{3}$$

of two polynomial equations in two variables, where F is a polynomial of degree d and G has t monomials. This problem has a peculiar history [4, 13, 16]. Sevostyanov showed in 1978 that the number of nondegenerate solutions can be bounded by a function $N(d,t)$ which depends on d and t only. According to [16], this result was the inspiration for Khovanskii to develop his theory of fewnomials. Sevostyanov suffered an early death, and his result was never published. Today, it seems that Sevostyanov's proof and even the specific form of his bound have been lost.

The results of Khovanskii (1), or of Bihan and Sottile (2), imply a bound on $N(d,t)$ which is exponential in d and t. Khovanskii's bound (1) follows from a general result on mixed polynomial-exponential systems (see Section 1.2 of [10]). One can check that the latter result implies a bound on $N(d,t)$ which is exponential in t only. As we shall see, this is still far from optimal.

Li, Rojas and Wang [14] showed that the number of real roots is upper bounded by $2^t - 2$ when F is a trinomial. When F is linear, this bound was improved to $6t-4$ by Avendaño [1]. The result by Li, Rojas and Wang [14] is in fact more general: they show that the number of non-degenerate positive real solutions of the system

$$F_1(X_1,\ldots,X_n) = F_2(X_1,\ldots,X_n) = \ldots = F_n(X_1,\ldots,X_n) = 0$$

is at most $n + n^2 + \ldots + n^{t-1}$ when each of $F_1,\ldots,F_{n-1}$ is a trinomial and F_n has t terms.

Returning to the case of a system $F(X,Y) = G(X,Y) = 0$ where F is a trinomial and G has t terms, we obtained in [12] a $O(t^3)$ upper bound on the number of real roots. It is also worth pointing out that, contrary to [1], the methods of [12] apply to systems with real exponents.

The present paper deals with the general case of Sevostyanov's system (3). We obtain the first bound which is polynomial in d and t. Indeed, we show that there are only $O(d^3t + d^2t^3)$ real solutions to (3) when their number is finite. Note that we count all roots, including degenerate roots. More generally, we show that when the set of solutions is infinite the same $O(d^3t + d^2t^3)$ upper bound applies to the number of its connected components (but it is actually the finite case which requires most of the work).

Note finally that our bound applies only when F is a polynomial of degree $d \geq 1$. As pointed out in Section 3, the case $d = 0$ is more difficult. The reason is that a system of two sparse equations can be encoded in a system where $F = 0$. We do not know if the number of real roots can be bounded by a polynomial function of t in this case.

The authors' interest for these problems was sparked by connections between lower bounds in algebraic complexity theory and upper bounds on the number of real roots of "sparse like" polynomials: see [11, 8, 12] as well as the earlier work [6, 9, 15].

Overview of the proof

As we build on results from [12], it is helpful to recall how the case $d = 1$ (intersection of a sparse curve with a line) was treated in that paper. For a line of equation $Y = aX + b$, this amounts to bounding the number of real roots of a univariate polynomial of the form

$$\sum_{i=1}^{t} c_i X^{\alpha_i} (aX + b)^{\beta_i}.$$

This polynomial is presented as a sum of t "basis functions" of the form $f_i(X) = c_i X^{\alpha_i}(aX+b)^{\beta_i}$. In order to bound the number of roots of a sum of real analytic functions, it suffices to bound the number of roots of their Wronskians. More precisely, we have the following result [12]:

Theorem 1. *Let I be an open interval of $\mathbb{R}$ and let $f_1, \ldots, f_t : I \to \mathbb{R}$ be a family of analytic functions which are linearly independent on I. For $1 \leq i \leq t$, let us denote by $W_i : I \to \mathbb{R}$ the Wronskian of $f_1, \ldots, f_i$. Then,*

$$Z(f_1 + \ldots + f_t) \leq t - 1 + Z(W_t) + Z(W_{t-1}) + 2 \sum_{j=1}^{t-2} Z(W_j)$$

where $Z(g)$ denotes the number of distinct real roots of a function $g : I \to \mathbb{R}$.

The present paper again relies on Theorem 1. Let us assume that for a system $F(X, Y) = G(X, Y) = 0$, we can use the equation $F(X, Y) = 0$ to express Y as an (algebraic) function of X. Then we just have to bound the number of real roots of a univariate polynomial of the form

$$\sum_{i=1}^{t} c_i X^{\alpha_i} \phi(X)^{\beta_i},$$

and this is a situation where we can apply Theorem 1. Of course, turning this informal idea into an actual proof requires some care. In particular, the algebraic function ϕ needs not be defined on the whole real line, and it needs not be uniquely defined. We deal with those issues using Collin's cylindrical algebraic decomposition (see Section 2.4). We also need some quantitatives estimates on the higher-order derivatives of the algebraic function ϕ because they appear in the Wronskians of Theorem 1. For this reason, we express in Section 2.2 the derivatives of ϕ in terms of ϕ and of the partial derivatives of F. Using Theorem 1, we can ultimately reduce Sevostyanov's problem to the case of a system where both polynomials have bounded degree. The relevant bound for this case are recorded in Section 2.3. We put these ingredients together in Section 3 to obtain the $O(d^3t + d^2t^3)$ bound on the number of connected components.

2 Technical Tools

In this section we collect various results that are required for the main part of this paper (Section 3). On first reading, there is no harm in beginning with Section 3; the present section can be consulted when the need arises.

2.1 The derivatives of a power

In this section, we recall how the derivatives of a power of a univariate function f can be expressed in terms of the derivatives of f. We use ultimately vanishing sequences of integer numbers, i.e., infinite sequences of integers which have only finitely many nonzero elements. We denote the set of such sequences $\mathbb{N}^{(\mathbb{N})}$. For any positive integer p, let $\mathscr{S}_p = \{(s_1, s_2, \ldots) \in \mathbb{N}^{(\mathbb{N})} | \sum_{i=1}^{\infty} i s_i = p\}$ (so in particular for each p, this set is finite). Then if s is in $\mathscr{S}_p$, we observe that for all $i \geq p+1$, we have $s_i = 0$. Moreover for any p and any $s = (s_1, s_2, \ldots) \in \mathbb{N}^{(\mathbb{N})}$, we will denote $|s| = \sum_{i=1}^{\infty} s_i$ (the sum makes sense because it is finite). A proof of the following simple lemma can be found in [12].

Lemma 2. *[Lemma 10 in [12]] Let p be a positive integer and $\alpha \geq p$ be a real number. Then*

$$(f^\alpha)^{(p)} = \sum_{s \in \mathscr{S}_p} \left[\beta_{\alpha,s} f^{\alpha - |s|} \prod_{k=1}^{p} \left(f^{(k)} \right)^{s_k} \right]$$

where $(\beta_{\alpha,s})$ are some constants.

We define the total order of differentiation of a differential polynomial of a function with an example: if f is a function, the total order of differentiation of $f^3 (f')^2 \left(f^{(4)}\right)^3 + 3ff'$ is $\max(3*0+2*1+3*4, 0*1+1*1) = 14$.

Lemma 2 just means that the p-th derivative of a power α of a function f is a linear combination of terms such that each term is a product of derivatives of f of total degree α and of total order of differentiation p.

2.2 The derivatives of an algebraic function

Consider a nonzero bivariate polynomial $F(X,Y) \in \mathbb{R}[X,Y]$ and a point (x_0, y_0) where $F(x_0, y_0) = 0$ and the partial derivative $F_Y = \frac{\partial F}{\partial Y}$ does not vanish. By the implicit function theorem, in a neighborhood of (x_0, y_0) the equation $F(x,y) = 0$ is equivalent to a condition of the form $y = \phi(x)$. The implicit function ϕ is defined on an open interval I containing x_0, and is C^∞ (and even analytic). In this section, we express the derivatives of ϕ in terms of ϕ and of the partial derivates of F. For any integers a, b, we denote $F_{X^aY^b} = \frac{\partial^{a+b}}{\partial X^a \partial Y^b} F(X,Y)$.

Lemma 3. *For all $k \geq 1$, there exists a polynomial S_k of degree at most $2k-1$ in $\binom{k+2}{2} - 1$ variables such that*

$$\phi^{(k)}(x) = \frac{S_k\left(F_X(x,\phi(x)), \ldots, F_{X^aY^b}(x,\phi(x)), \ldots\right)}{(F_Y(x,\phi(x)))^{2k-1}} \tag{4}$$

with $1 \leq a+b \leq k$. Consequently, the numerator is a polynomial of total degree at most $(2k-1)d$ in x and $\phi(x)$. Moreover, S_k depends only on k and F.

Proof. For all k, let $D_k(x) = \frac{\partial^k}{\partial x^k} F(x, \phi(x))$. We will use later the fact that $D_k(x)$ is the identically zero function. We begin by showing by induction that for all $k \geq 1$, $D_k(x) = \phi^{(k)} F_Y + R_k(\phi'(x), \ldots, \phi^{(k-1)}(x), \ldots, F_{X^aY^b}, \ldots)$ where R_k is of total degree at most 1 in $(F_{X^aY^b})_{1 \leq a+b \leq k}$ and of derivation order at most k in the variables $\left(\phi^{(i)}\right)_{1 \leq i < k}$.

For $k = 1$, we get: $D_1 = \phi' F_Y + F_X$. Let us suppose now that the result is true for a particular k, then

$$\begin{aligned} D_{k+1} =& \phi^{(k+1)} F_Y + \phi^{(k)}(F_{XY} + F_{Y^2}\phi') + \frac{\partial}{\partial x} R_k\left(\phi', \ldots, \phi^{(k-1)}, F_{X^aY^b}\right) \\ =& \phi^{(k+1)} F_Y + R_{k+1}\left(\phi', \ldots, \phi^{(k)}, F_{X^aY^b}\right). \end{aligned}$$

Moreover, R_{k+1} is of total degree at most 1 in the variables $(F_{X^aY^b})_{1 \leq a+b \leq k+1}$ and of derivation order at most $k+1$ in $\left(\phi^{(i)}\right)_{1 \leq i \leq k}$ (since R_k is of order of derivation at most k in $\left(\phi^{(i)}\right)_{1 \leq i \leq k-1}$).

As $F(x, \phi(x))$ is zero, then for all $k \geq 1$ we have $D_k(x) = \frac{\partial^k F(x,\phi(x))}{\partial x^k} = 0$. Thus

$$\phi^{(k)} = \frac{-R_k}{F_Y}.$$

Then we show by induction over k that for all $k \geq 1$ there exists a polynomial S_k of degree at most $2k-1$ in $\left(\binom{k+2}{2} - 1\right)$ variables such that Equation (4) is verified.

The result is true for $k = 1$ since $\phi' = \frac{-F_X}{F_Y}$. Let $k \geq 1$ and we suppose that the result is true for all i such that $1 \leq i \leq k$. We know that $D_{k+1}(x) = \phi^{(k+1)} F_Y + R_{k+1}(\phi'(x), \ldots, \phi^{(k)}(x), \ldots, F_{X^aY^b}, \ldots) = 0$. So,

$$\phi^{(k+1)} = \frac{-1}{F_Y} R_{k+1}(\phi'(x), \ldots, \phi^{(k)}(x), \ldots, F_{X^aY^b}, \ldots).$$

So, by induction hypothesis,

$$\phi^{(k+1)} = \frac{-1}{F_Y} R_{k+1} \left(\frac{S_1}{F_Y}, \ldots, \frac{S_k}{F_Y^{2k-1}}, \ldots, F_{X^aY^b}, \ldots \right).$$

As $R_{k+1}(\phi'(x), \ldots, \phi^{(k)}(x), \ldots, F_{X^aY^b}, \ldots)$ is of derivation order $k+1$ on its k first variables and is of total order 1 on its $\left(\binom{k+2}{2} - 1\right)$ last variables, each monomial is of the form:

$$F_{X^aY^b} \frac{S_{i_1}}{F_Y^{2i_1-1}} \cdots \frac{S_{i_p}}{F_Y^{2i_p-1}}$$

with $i_1 + \ldots + i_p \leq k+1$ and $p \geq 0$. Hence, we get:

$$\frac{F_{X^aY^b} S_{i_1} \ldots S_{i_p}}{F_Y^{2i_1-1} \ldots F_Y^{2i_p-1}} = \frac{F_{X^aY^b} S_{i_1} \ldots S_{i_p} F_Y^{2k-2i+p}}{F_Y^{2(k+1)-2}}$$

where $i = i_1 + \ldots + i_p \leq k+1$. Indeed, the exponent $2k - 2i + p$ is a non-negative integer since if $p = 1$, then $2i = 2i_1 \leq 2k$ and otherwise $2i \leq 2(k+1) \leq 2k + p$. The numerator is a polynomial in the variables $F_{X^aY^b}$ of degree

$$\begin{aligned}
&\leq 1 + d^\circ(S_{i_1}) + \ldots + d^\circ(S_{i_p}) + 2k - 2i + p \\
&\leq 1 + 2i_1 - 1 + \ldots + 2i_p - 1 + 2k - 2i + p \\
&\leq 1 + 2i - p + 2k - 2i + p \\
&\leq 2(k+1) - 1.
\end{aligned}$$

So, $\phi^{(k+1)}$ is of the form:

$$\frac{S_{k+1}\left((F_{X^aY^b})_{1 \leq a+b \leq k+1}\right)}{F_Y^{2(k+1)-1}}$$

where S_{k+1} is a polynomial of degree at most $2(k+1) - 1$. $\square$

2.3 Real versions of Bézout's theorem

Bézout's theorem is a fundamental result in algebraic geometry. One version of it is as follows.

Theorem 4. *Consider an algebraically closed field K and n polynomials $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$ of degrees $d_1, \ldots, d_n$. If the polynomial system*

$$f_1 = f_2 = \cdots = f_n = 0$$

has a finite number of solutions in K^n, this number is upper bounded by $\prod_{i=1}^{n} d_i$.

The upper bound $\prod_{i=1}^{n} d_i$ may not apply if K is not algebraically closed. In particular, it fails for the field of real numbers (see e.g. chapter 16 of [5] for a counterexample). Nevertheless, there is a large body of work establishing bounds of a similar flavor for $K = \mathbb{R}$ (see e.g. [2, 5] and the references therein). For instance, we have the following classic result.

Theorem 5 (Oleinik-Petrovski-Thom-Milnor). *Let $V \subseteq \mathbb{R}^n$ be defined by a system $f_1 = 0, \ldots, f_p = 0$, where the f_i are real polynomials of degree at most d. Then the number of connected components of V is at most $d(2d-1)^{n-1}$.*

A proof of Theorem 5 can be found in e.g. Chapter 16 of [5]. In this paper we will use this result as well as a variation for the case $n = p = 2$ (see Lemma 9 at the end of this section). Lemma 6 below will be also useful in Section 3. We now give self-contained proofs of these two lemmas since they are quite short.

Lemma 6. *Let $g \in \mathbb{R}[X,Y]$ be a non-zero polynomial of degree d. The set of real zeros of g is the union of a set of at most $d^2/4$ points and of the zero sets of polynomials $g_1, \ldots, g_k \in \mathbb{R}[X,Y]$ which divide g and are irreducible in $\mathbb{C}[X,Y]$.*

Proof. Let us factor g as a product of irreducible polynomials in $\mathbb{C}[X,Y]$. We have

$$g = \lambda g_1^{\alpha_1} \cdots g_k^{\alpha_k} h_1^{\beta_1} \cdots h_l^{\beta_l} \overline{h_1}^{\beta_1} \cdots \overline{h_l}^{\beta_l}$$

where the g_j are the factors in $\mathbb{R}[X,Y]$, the polynomials $h_j, \overline{h_j}$ are complex conjugate and λ is a real constant. We can assume that none of the h_j is of the form $h_j = \mu_j r_j$ where $\mu_j \in \mathbb{C}$ and $r_j \in \mathbb{R}[X,Y]$: otherwise, we can replace the pair $(h_j, \overline{h_j})$ by r_j^2 and the constant $\mu_j \overline{\mu_j}$ can be absorbed by λ.

The above assumption implies that the h_j (and their conjugates) have finitely many real zeros. Indeed, let p_j, q_j be the real and imaginary parts of h_j. The real solutions of $h_j = 0$ are the same as those of $p_j = q_j = 0$. This system has finitely many complex solutions since p_j and q_j are nonzero and do not share a common factor. Consider indeed a putative factor $f_j \in \mathbb{C}[X,Y]$ dividing p_j and q_j, of degree $\deg(f_j) \geq 1$. Since f_j divides h_j and this polynomial is irreducible, we must have $\deg(f_j) = \deg(h_j)$. As a result, $\deg(p_j) = \deg(q_j) = \deg(f_j)$ and the first two polynomials are constant multiples of the third. We conclude that p_j differs from q_j only by a multiplicative constant, and this contradicts our assumption.

By Bézout's theorem, there are at most $\deg(h_j)^2$ complex solutions to $p_j = q_j = 0$. This is also an upper bound on the number of real roots of the h_j. The $\overline{h_j}$ have the same real roots. Altogether, the h_j and $\overline{h_j}$ have at most $\sum_{j=1}^{l} \deg(h_j)^2 \leq (d/2)^2$ real roots. ∎

The point of this proposition is that since each g_j are irreducible, the set of its singular zeros (i.e., the set of complex solutions of the system $g = \partial g/\partial x = \partial g/\partial y = 0$) is finite and small. We first consider the more general case given by the system $g = \partial g/\partial x = 0$.

Lemma 7. *If $g \in \mathbb{C}[X,Y]$ is an irreducible polynomial of degree $d \geq 1$, then either $g(X,Y)$ is of the form $aY+b$ or the number of zeros in $\mathbb{C}^2$ of $g = \partial g/\partial x = 0$ is at most $d(d-1)$.*

Proof. We consider two cases.

(i) If the system $g = \partial g/\partial x = 0$ has finitely many solutions, it has at most $d(d-1)$ solutions by Bézout's theorem.

(ii) If that system has infinitely many solutions, $\partial g/\partial x$ must vanish everywhere on the zero set of g since g is irreducible. For the same reason, it then follows that g divides $\partial g/\partial x$. This is impossible by degree considerations unless $\partial g/\partial x \equiv 0$ on $\mathbb{C}^2$. Hence g depends only on the variable Y, and must be of the form $g(X,Y) = aY + b$ (by irreducibility again).

□

As the additional condition $\partial g/\partial y = 0$ implies $a = 0$ in the previous lemma, we have:

Corollary 8. *If $g \in \mathbb{C}[X,Y]$ is an irreducible polynomial of degree $d \geq 1$, it has at most $d(d-1)$ singular zeros in $\mathbb{C}^2$.*

We are now going to bound the number of roots of a real system of two dense equations.

Lemma 9. *Let $f, g \in \mathbb{R}[X,Y]$ be two non-zero polynomials of respective degrees δ and d. Let $\mathcal{U}$ be an open subset of $\mathbb{R}^2$. Consider the system of polynomial equations:*

$$\begin{cases} f(X,Y) = 0 \\ g(X,Y) = 0. \end{cases} \tag{5}$$

If the number of solutions in $\mathcal{U}$ is finite, it is upper bounded by $d^2/4 + d\delta$.

Moreover, if f is the zero polynomial, the number of solutions in $\mathcal{U}$ of the same system is infinite or bounded by $\frac{d^2}{4} + d(d-1)$.

Proof. Let us suppose that the system has finitely many solutions in $\mathcal{U}$. By Lemma 6, the set of roots of g is the union of a set of size at most $d^2/4$ and of the sets of roots of the polynomials $g_1, \ldots, g_k$. Hence the number of solutions of System (5) is bounded by $d^2/4$ plus the sum of the numbers of solutions of each system $g_i(X,Y) = f(X,Y) = 0$. Let us define d_i as the degree of g_i. For each i, there are two cases:

(i) if g_i divides f then either the number of real roots of g_i is infinite on $\mathcal{U}$ and then all these roots are solutions of System (5) or the number of its roots is finite and in this case, each one of these roots are singular zeros of g_i. Hence by Corollary 8, the number of real roots is bounded by $d_i(d_i - 1)$, and so, since g_i divides f, by $d_i\delta$ if f is not zero.

(ii) otherwise, g_i does not divide f and thus the system has a finite number of solutions in $\mathbb{C}^2$ and this number is bounded by $d_i\delta$ according to Bézout's theorem.

Thus for each i, the number of solutions of the system $g_i(X,Y) = f(X,Y) = 0$ is at most $d_i\delta$. $\square$

Note that the somewhat worse bound

$$\max(d,\delta).(2\max(d,\delta) - 1)$$

follows directly from Theorem 5.

2.4 Cylindrical algebraic decomposition for one bivariate polynomial

In his paper, Collins [7] introduced the cylindrical algebraic decomposition. The purpose was to get an algorithmic proof of the quantifier elimination for real closed fields. More details on the cylindrical algebraic decomposition can be found in [2]. Here, we will use a similar decomposition of $\mathbb{R}$ for separating the different behaviours of the roots of our system. However, in our case the dimension is just two, and we want to characterize only one polynomial, so we will use an easier decomposition. Let us recall some definitions and properties from [7].

Definition 10. *Let $A(X,Y)$ be a real polynomial, S a subset of $\mathbb{R}$. We will say that $f_1,\ldots,f_m$ with $m \geq 1$ delineate the roots of A on S in case the following conditions are all satisfied:*

1. *$f_1,\ldots,f_m$ are distinct continuous functions from S to $\mathbb{C}$.*
2. *For all $1 \leq i \leq m$, there is a positive integer e_i such that for all a in S, $f_i(a)$ is a root of $A(a,Y)$ of multiplicity e_i.*
3. *If $a \in S$, $b \in \mathbb{C}$ and $A(a,b) = 0$ then for some i with $1 \leq i \leq m$, $b = f_i(a)$.*
4. *For some k with $0 \leq k \leq m$, the functions $f_1,\ldots,f_k$ are real-valued with $f_1 < f_2 < \ldots < f_k$ and the values of $f_{k+1},\ldots,f_m$ are all non-real.*

The value e_i will be called the multiplicity of f_i. If $k \geq 1$, we will say that $f_1,\ldots,f_k$ delineate the real roots of A on S. The roots of A are delineable on S in case there are functions $f_1,\ldots,f_m$ which delineate the roots of A on S.

Collins proved the following theorem.

Theorem 11 (Particular case of Theorem 1 in [7])**.** *Let $A(X,Y)$ be a polynomial in $\mathbb{R}[X][Y]$. Let S be a connected subset of $\mathbb{R}$. If the leading coefficient of A viewed as a polynomial in Y does not vanish on S, and if the number of distinct roots of $A(X)$ on $\mathbb{C}$ is invariant on S then the roots of A are delineable on S.*

Criteria are given in the remainder of Collin's paper for characterizing the invariance of the number of roots. He uses the resultant of two polynomials.

Let A and B be polynomials in $\mathbb{R}[X][Y]$ with $\deg_Y(A) = m$ and $\deg_Y(B) = n$. The Sylvester matrix of A and B is the $m+n$ by $m+n$

matrix M whose successive rows contain the coefficients of the polynomials $Y^{n-1}A(Y), \dots, YA(Y), A(Y), Y^{m-1}B(Y), \dots, B(Y)$, with the coefficient of Y^i occuring in column $m+n-i$. The polynomial $\mathrm{Res(A, B)}$, the resultant of A and B, is $\det(M)$, the determinant of M and if the leading coefficient of A vanishes for a particular x_0, then the resultant $\mathrm{Res(A, A_Y)}$ also vanishes at x_0. We note, for subsequent application, that if $A \in \mathbb{R}[X, Y]$, $\deg_X(A) \leq d$ and $\deg_Y(A) \leq d$, then $\mathrm{Res(A, A_Y)}$ is a polynomial in $\mathbb{R}[X]$ of degree bounded by $2d^2 - d$.

An immediate corollary of Theorem 1, 2 and 3 in [7] is

Corollary 12. *Let $A(X, Y)$ be a polynomial in $\mathbb{R}[X][Y]$. Let S be a connected subset of $\mathbb{R}$. If $\mathrm{Res(A, A_Y)(X)}$ does not have any roots on S, then the roots of A are delineable on S.*

Then, in the following, we will consider some subsets of $\mathbb{R}$ where the polynomial $\mathrm{Res(A, A_Y)}$ does not have roots. In particular, we want this polynomial to be nonzero. We show that this is the case if A is irreducible in $\mathbb{R}[X, Y]$.

Lemma 13. *Let $A(X, Y)$ be an irreducible polynomial in $\mathbb{R}[X][Y]$ with $\deg_Y(A) \geq 1$. Then $\mathrm{Res(A, A_Y)}$ is not the zero polynomial.*

Proof. By a well-known theorem, the irreducibility of A in $\mathbb{R}[X][Y]$ and the condition $\deg_Y(A) \geq 1$ imply that A is irreducible in $\mathbb{R}(X)[Y]$. Let us suppose that $R(X) = \mathrm{Res(A, A_Y)(X)} = 0$. This implies that A and A_Y have a common factor $B \in \mathbb{R}(X)[Y]$ of degree $\deg_Y(B) \geq 1$. Since A is irreducible in $\mathbb{R}(X)[Y]$, there exists C in $\mathbb{R}(X)$ such that $A = CB$. We thus have $\deg_Y(A) = \deg_Y(B) \leq \deg_Y(A_Y)$. This is impossible since $\deg_Y(A) \geq 1$. $\square$

Remark 14. *If (x_0, y_0) is a root of A and of A_Y then $Y - y_0$ divides the polynomials $A(x_0, Y)$ and $A_Y(x_0, Y)$. Hence $\mathrm{Res(A, A_Y)(x_0)} = 0$. Therefore, if $\mathrm{Res(A, A_Y)}$ has no zeros on a subset S of $\mathbb{R}$, the system $A(X, Y) = A_Y(X, Y) = 0$ does not have solutions on $S \times \mathbb{R}$. This remark will be useful for the proof of Lemma 19 in the next section, and for an application of the analytic implicit function theorem before Lemma 18.*

3 Intersecting a sparse curve with a low-degree curve

Recall that a polynomial is said to be t-sparse if it has at most t monomials. In this section we prove our main result.

Theorem 15. *Let $F \in \mathbb{R}[X, Y]$ be a nonzero bivariate polynomial of degree d and let $G \in \mathbb{R}[X, Y]$ be a bivariate t-sparse polynomial. The set of real solutions of the system*

$$\begin{cases} F(X, Y) = 0 \\ G(X, Y) = 0 \end{cases} \tag{6}$$

has a number of connected components which is $O(d^3t + d^2t^3)$.

We will proceed by reduction to the case where F is irreducible and the system has finitely many solutions:

Proposition 16. *Consider again a nonzero bivariate polynomial F of degree d and a bivariate t-sparse polynomial G. Assume moreover that F is irreducible in $\mathbb{C}[X, Y]$ and that (6) has finitely many real solutions. Then this system has $O(d^3t + d^2t^3)$ distinct real solutions.*

We first explain why this proposition implies Theorem 15. Let us begin by removing the hypothesis that the system has a finite number of solutions.

Corollary 17 (Corollary of Proposition 16)**.** *Consider again a nonzero bivariate polynomial F of degree d and a bivariate t-sparse polynomial G. Assume moreover that F is irreducible in $\mathbb{C}[X, Y]$. The set of real solutions of (6) has a number of connected components which is $O(d^3t + d^2t^3)$.*

Proof. There are two cases:

1. The system has a finite set of real solutions. In this case, by Proposition 16 there at most $O(d^3t + d^2t^3)$ solutions.

2. The set of solutions is infinite. This implies that F and G shares a common factor. Since F is irreducible in $\mathbb{C}$, F must be a factor of G. But in this case the set of solutions of (6) is exactly the set of zeros of F. By Theorem 4, this set has at most $2d(d-1)$ connected components.

$\square$

Proof of Theorem 15 from Corollary 17. By Lemma 6, the set of real roots of F is the union of the set of real roots of the real irreducible factors $F_1, \ldots, F_k$ of F and of a set $\mathcal{U}$ of cardinality at most $d^2/4$. Consequently, the number of connected components of the set of solutions of (6) is bounded by the sum of the numbers of connected components of the solutions of the systems $F_i(x, y) = G(x, y) = 0$ for $i \leq k$ and of the system

$$\begin{cases} (X, Y) \in \mathcal{U} \\ G(X, Y) = 0. \end{cases}$$

The latter system has at most $d^2/4$ solutions. By Corollary 17, each system $F_i(x, y) = G(x, y) = 0$ has at most $O((\deg F_i)^3t + (\deg F_i)^2t^3)$ connected components. To conclude, we observe that

$$\begin{aligned} \sum_{i=1}^{k} \left((\deg F_i)^3 t + (\deg F_i)^2 t^3\right) &\leq \left(\sum_{i=1}^{k} \deg F_i\right)^3 t + \left(\sum_{i=1}^{k} \deg F_i\right)^2 t^3 \\ &\leq d^3t + d^2t^3. \end{aligned}$$

$\square$

Note that the non-zero condition on F in Theorems 15 and Proposition 16 is important. Indeed, it is an open problem whether there exists a polynomial $P(t)$ which upper bounds the number of real solutions of any system of two t-sparse polynomials G and H when this bound is finite. However, if we allowed the polynomial F to be 0 in Theorems 15, we would be able to code a system of two sparse equations in the system:

$$\begin{cases} F = 0 \\ G(X,Y)^2 + H(X,Y)^2 = 0. \end{cases} \tag{7}$$

It remains to prove Proposition 16. In the following, we will suppose that the system has a finite number of real solutions. We begin with two basis cases.

1. If $F(X,Y) = cY$, then as $G(X,0) \neq 0$ (otherwise $(x,0)$ is a solution of (6) for all x in $\mathbb{R}$), by Descartes' rule, the number of roots of the form $(x,0)$ is bounded by $2t-1$.
2. If $F_Y(X,Y) = 0$, then F does not depend on Y and there are at most d values $x_1, \ldots, x_p$ of X such that $F(x_l, Y) = 0$. For each of these values, $G(x_l, Y)$ is a univariate t-sparse polynomial so it has at most $2t-1$ distinct real roots. Hence, in this case there are at most $2td - d$ solutions to (6).

We have therefore verified the bound of Proposition 16 in these two particular cases. We will assume in the following we are not in case 1 or 2.

Let us consider the univariate polynomial $\mathrm{Res}(\mathrm{F}, \mathrm{F_Y})$, which is of degree at most $2d^2 - d$ and which is not zero by Lemma 13. Let $x_1 < \ldots < x_q$ with $q \leq 2d^2 - d$ be the real roots of this polynomial and let $\mathcal{I} = \{(x_i, x_{i+1}) | 0 \leq i \leq q\}$ with $x_0 = -\infty$ and $x_{q+1} = +\infty$, be the corresponding set of open intervals. We notice that $|\mathcal{I}| \leq 2d^2 - d + 1$. If I is in $\mathcal{I}$, the roots of F are delineable on I by Corollary 12.

From the definition of delineability, for each interval I in $\mathcal{I}$, there are $m_I \leq d$ continuous real-valued functions $\phi_{I,1} < \ldots < \phi_{I,m_I} : I \to \mathbb{R}$ such that $F(x,y) = 0$ on $I \times \mathbb{R}$ if and only if there exists $i \leq m_I$ such that $y = \phi_{I,i}(x)$. Moreover, $F_Y(x, \phi_{I,i}(x)) \neq 0$ since $\mathrm{Res}(\mathrm{F}, \mathrm{F_Y})$ does not vanish on I (see Remark 14). The analytic version of the implicit function theorem therefore shows that the functions $\phi_{I,i}$ are analytic on I.

Let us denote $\Omega = \bigcup_{I \in \mathcal{I}} I$. We bound separately the number s of solutions of system (6) on $\Omega \times \mathbb{R}$ and the number s' of solutions on $(\mathbb{R} \setminus \Omega) \times \mathbb{R}$.

Lemma 18. *If $F_Y(X,Y)$ is a non-zero polynomial, the number s' of solutions on $(\mathbb{R} \setminus \Omega) \times \mathbb{R}$ of System (6) is at most $2d^3 - d^2$.*

Proof. We recall that $(\mathbb{R} \setminus \Omega) = \{x_1, \ldots, x_q\}$ is a finite set of cardinality at most $2d^2 - d$. For each $i \leq q$, $X - x_i$ does not divide F since F is irreducibleand $F_Y \neq 0$. So the number of roots of F on $\{x_i\} \times \mathbb{R}$ is finite and bounded by d. Consequently, $s' \leq 2d^3 - d^2$. ☐

Now, we want to upperbound the number s of solutions on $\Omega\times\mathbb{R}$. To do so, we will bound the number s_j^I (with $j \le m_I$) of solutions of the following system over $I\times\mathbb{R}$:

$$\begin{cases} Y=\phi_j(X) \\ G(X,Y)=0. \end{cases} \tag{8}$$

Hence, $\sum_I \sum_{0\le j\le m_I} s_j^I = s$ and in particular all the s_j^I are finite.

The polynomial g is t-sparse, so $G(X,Y)=\sum_{j=1}^t a_j X^{\alpha_j} Y^{\beta_j}$. Then, if (x,y) is a root of (8), we have $G(x,\phi_i(x))=\sum_{j=1}^t a_j x^{\alpha_j}(\phi_i(x))^{\beta_j}=0$.

Let us assume that there exist real constants $c_1,\dots,c_t$ (not all zero) such that $H(X,Y)=\sum_{j=1}^t c_j X^{\alpha_j}Y^{\beta_j}$ is a multiple of F. In this case, we can consider the polynomial $\tilde{G}(X,Y)=G-\frac{a_u}{c_u}H$ which is $t-1$ sparse (where c_u is a non-zero coefficient of H). Then, the roots of (6) are exactly the roots of the following system:

$$\begin{cases} F(X,Y)=0 \\ \tilde{G}(X,Y)=0. \end{cases} \tag{9}$$

In this system, the first polynomial has not changed and the number of terms of the second polynomial has decreased. We can therefore assume (by induction on t) that the claimed $O(d^3t+d^2t^3)$ upper bound on the number of real solutions applies to (9). Consequently, we will assume for the remainder of the proof that if $H(X,Y)=\sum_{j=1}^t c_j X^{\alpha_j}Y^{\beta_j}$ is a multiple of F then all the constants c_j are zero.

Before stating the next lemma, we recall that $\mathcal{I}$ is a finite list of open intervals defined before Lemma 18.

Lemma 19. *For $s\le t$, there exists a non-zero polynomial $T_s(X,Y)\in\mathbb{R}[X,Y]$ of degree at most $(1+2d)\binom{s}{2}$ in each variable such that for every interval I in $\mathcal{I}$ and every $0\le i\le m_I$, the Wronskian of the s functions $x^{\alpha_1}(\phi_i(x))^{\beta_1},\dots,x^{\alpha_s}(\phi_i(x))^{\beta_s}$ satisfies:*

$$W(x^{\alpha_1}(\phi_i(x))^{\beta_1},\dots,x^{\alpha_s}(\phi_i(x))^{\beta_s})=\frac{x^{\alpha-\binom{s}{2}}\phi_i^{\beta-\binom{s}{2}}}{F_Y^{s(s-1)}(x,\phi_i)}T_s(x,\phi_i)$$

where $\alpha=\sum_{j=1}^s\alpha_j$ and $\beta=\sum_{j=1}^s\beta_j$. Moreover, this Wronskian is not identically 0 on I.

Proof. Let I be a an interval in $\mathcal{I}$ and i be an integer between 0 and m_I. If $\sum_{j=1}^t c_j x^{\alpha_j}\phi_i^{\beta_j}=H(x,\phi_i(x))$ is the zero polynomial, then F divides H by irreducibility of F. It then follows that $H\equiv 0$ by the assumption preceding the lemma. The family $x\mapsto x^{\alpha_j}(\phi_i(x))^{\beta_j}$ is therefore linearly independent. As the functions are analytic on I, the Wronskian $W(x^{\alpha_1}(\phi_i(x))^{\beta_1},\dots,x^{\alpha_s}(\phi_i(x))^{\beta_s})$

is not identically zero. By Remark 14, $F_Y(x, \phi_i(x))$ has no zeros on I. Then using Lemmas 2 and 3,

$$
\begin{aligned}
\left(x^{\alpha_j}(\phi_i(x))^{\beta_j}\right)^{(p)} &= \sum_{k=0}^{p} \binom{p}{k} (x^{\alpha_j})^{(k)} \left(\phi_i(x)^{\beta_j}\right)^{(p-k)} \\
&= \sum_{k=0}^{p} \binom{p}{k} (x^{\alpha_j})^{(k)} \sum_{s\in\mathcal{S}_{p-k}} \left[c_{\beta_j,s} \phi_i^{\beta_j-|s|} \prod_{l=1}^{p-k} \left(\phi_i^{(l)}\right)^{s_l} \right] \\
&= x^{\alpha_j-p}\phi_i^{\beta_j-p} \sum_{k=0}^{p} \sum_{s\in\mathcal{S}_{p-k}} \left[c'_{\alpha_j,\beta_j,p,s} x^{p-k} \phi_i^{p-|s|} \prod_{l=1}^{p-k} \left(\frac{S_l}{F_Y^{2l-1}}\right)^{s_l} \right] \\
&= \frac{x^{\alpha_j-p}\phi_i^{\beta_j-p}}{F_Y^{2p}} \sum_{k=0}^{p} \sum_{s\in\mathcal{S}_{p-k}} \left[c'_{\alpha_j,\beta_j,p,s} x^{p-k} \phi_i^{p-|s|} F_Y^{2k+|s|} \prod_{l=1}^{p-k} S_l^{s_l} \right] \\
&= \frac{x^{\alpha_j-p}\phi_i^{\beta_j-p}}{F_Y^{2p}} T_{j,p}(x,\phi_i)
\end{aligned}
$$

where $T_{j,p}(X,Y)$ is a polynomial of degree in X bounded by

$$
\begin{aligned}
\deg_X(T_{j,p}) &\le \max_{k,s} \left(p-k+(2k+|s|)d + \sum_{l=1}^{p-k} s_l(2l-1)d \right) \\
&\le \max_{k,s} \left(p-k+2kd+|s|d+2d(p-k)-d|s|\right) \\
&\le 2dp+p
\end{aligned}
$$

and of degree in Y bounded by

$$
\begin{aligned}
\deg_Y(T_{j,p}) &\le \max_{k,s} \left(p-|s|+(2k+|s|)(d-1) + \sum_{l=1}^{p-k} s_l(2l-1)d \right) \\
&\le \max_{k,s} \left(p-|s|+2kd-2k+|s|d-|s|+2dp-2dk-d|s|\right) \\
&\le \max_{k,s} \left(p-2|s|-2k+2dp\right) \\
&\le p+2dp.
\end{aligned}
$$

Moreover $T_{j,p}$ does not depend on ϕ_i by Lemma 3. Hence, the Wronskian is a bivariate rationnal function:

$$
W\left(x^{\alpha_1}(\phi_i(x))^{\beta_1}, \ldots, x^{\alpha_s}(\phi_i(x))^{\beta_s}\right) = \frac{x^{\alpha-\binom{s}{2}}\phi_i^{\beta-\binom{s}{2}}}{F_Y^{s(s-1)}(x,\phi_i)} T_s(x,\phi_i)
$$

where $\alpha = \sum_{j=1}^{s}\alpha_j$, $\beta = \sum_{j=1}^{s}\beta_j$ and $T_s(X,Y)$ is a polynomial of degree bounded by $(1+2d)\binom{s}{2}$ in each variable, which does not depend on I and i. $\square$

Let us count the number $v_{I,i}$ of roots of ϕ_i on I. We assumed that Y does not divide F, so the univariate polynomial $F(X,0)$ is not zero and is of degree at most d. If v_I denotes the number of roots of $F(X,0)$ on I, we have $\left(\sum_{I\in\mathcal{I}} v_I\right) \leq d$. Since each root of ϕ_i is by definition a root of $F(X,0)$, this implies that ϕ_i has at most v_I roots on I.

For any I and i, let us count now the number $r^s_{I,i}$ of roots of $T_s(x,\phi_i(x))$. This number is finite since the Wronskian of Lemma 19 would otherwise be identically 0. Furthermore, let us denote by r^s the number of solutions on $\Omega\times\mathbb{R}$ of the system

$$\begin{cases} T_s\left(X,Y\right)=0 \\ F\left(X,Y\right)=0. \end{cases} \tag{10}$$

Thus, $r^s = \left(\sum_I \sum_i r^s_{I,i}\right)$ is finite.

Finally, by Lemma 9 and as the total degree of T_S is bounded by $2(1+2d)\binom{s}{2}$, the number r^s of roots of (10) is bounded by $d^2/4 + 2d(1+2d)\binom{s}{2}$.

Then, by Lemma 19, for any I and i, $W\left(x^{\alpha_1}(\phi_i(x))^{\beta_1},\ldots,x^{\alpha_s}(\phi_i(x))^{\beta_s}\right)$ has at most $1_I(0)+v_I+r^s_{I,i}$ real roots and Theorem 1 shows that the number $s_{I,i}$ of distinct real roots of $G(x,\phi_i(x))$ is bounded by

$$t-1+2\sum_{s=1}^{t}\left(1_I(0)+v_I+r^s_{I,i}\right) = t-1+2t1_I(0)+2tv_I+2\sum_{s=1}^{t} r^s_{I,i}.$$

Hence,

$$\begin{aligned} s &= \sum_{I\in\mathcal{I}}\sum_{i\leq m_I} s_{I,i} \\ &\leq (2d^2-d+1)d(t-1)+2dt+2td^2+2\sum_{s=1}^{t} r^s \\ &\leq (2d^2-d+1)d(t-1)+2dt+2td^2+2\sum_{s=1}^{t}\left[d^2/4+2(1+2d)\binom{s}{2}d\right] \\ &= (2d^3t+4d^2t^3)(1+o(1)). \end{aligned}$$

This completes the proof of Proposition 16, and of the main theorem.

References

[1] Martín Avendaño. The number of roots of a lacunary bivariate polynomial on a line. *Journal of Symbolic Computation*, 44(9):1280–1284, 2009.

[2] Saugata Basu, Richard D Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10. Springer, 2006.

[3] Frédéric Bihan and Frank Sottile. New fewnomial upper bounds from Gale dual polynomial systems. *Moscow Mathematical Journal*, 7(3):387–407, 2007.

[4] Frédéric Bihan and Frank Sottile. Fewnomial bounds for completely mixed polynomial systems. *Advances in Geometry*, 11(3):541–556, 2011.

[5] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and Real Computation.* Springer-Verlag, 1998.

[6] A. Borodin and S. Cook. On the number additions to compute specific polynomials. *SIAM Journal on Computing*, 5(1):146–157, 1976.

[7] George E Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In *Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20–23, 1975*, pages 134–183. Springer, 1975.

[8] B. Grenet, P. Koiran, N. Portier, and Y. Strozecki. The limited power of powering: polynomial identity testing and a depth-four lower bound for the permanent. In *Proc. FSTTCS*, 2011. arxiv.org/abs/1107.1434.

[9] D. Grigoriev. Notes of the scientific seminars of LOMI. volume 118, pages 25–82, 1982.

[10] A.G. Khovanskiĭ. *Fewnomials.* Translations of mathematical monographs. American Mathematical Society, 1991.

[11] P. Koiran. Shallow circuits with high-powered inputs. In *Proc. Second Symposium on Innovations in Computer Science (ICS 2011)*, 2011. arxiv.org/abs/1004.4960.

[12] Pascal Koiran, Natacha Portier, and Sébastien Tavenas. A Wronskian approach to the real τ-conjecture. *Effective Methods in Algebraic Geometry (MEGA 2013)*, 2013. arxiv.org/abs/1205.1015.

[13] A. Kushnirenko. Letter to Frank Sottile. www.math.tamu.edu/ sottile/research/pdf/Kushnirenko.pdf, 2008.

[14] Tien-Yien Li, J Maurice Rojas, and Xiaoshen Wang. Counting real connected components of trinomial curve intersections and m-nomial hypersurfaces. *Discrete & Computational Geometry*, 30(3):379–414, 2003.

[15] J.-J. Risler. Additive complexity and zeros of real polynomials. *SIAM Journal on Computing*, 14:178–183, 1985.

[16] F. Sottile. *Real Solutions to Equations from Geometry.* University lecture series. American Mathematical Society, 2011.