ELSEVIER

Journal of Pure and Applied Algebra 173 (2002) 49–58

JOURNAL OF
PURE AND
APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Effective computation of singularities of parametric affine curves

Hyungju Park

Department of Mathematics and Statistics, Oakland University, Rochester, MI 48309, USA

Received 30 October 2000; received in revised form 1 August 2001
Communicated by M.-F. Roy

Abstract

Let k be a field of characteristic zero and $f(t), g(t)$ be polynomials in $k[t]$. For a plane curve parameterized by $x=f(t), y=g(t)$, Abhyankar developed the notion of Taylor resultant (Mathematical Surveys and Monographs, Vol. 35, American Mathematical Society, Providence, RI, 1990) which enables one to find its singularities without knowing its defining polynomial. This concept was generalized as D-resultant by Yu and Van den Essen (Proc. Amer. Math. Soc. 125(3) (1997) 689), which works over an arbitrary field. In this paper, we extend this to a curve in affine n-space parameterized by $x_1=f_1(t),\dots,x_n=f_n(t)$ over an arbitrary ground field k, where $f_1,\dots,f_n \in k[t]$. This approach compares to the usual approach of computing the ideal of the curve first. It provides an efficient algorithm of computing the singularities of such parametric curves using Gröbner bases. Computational examples worked out by symbolic computation packages are included. © 2002 Elsevier Science B.V. All rights reserved.

MSC: 13P10; 14Q05

1. Introduction

For an arbitrary field k, let $f_1,\dots,f_n \in k[t]$. Consider the curve $C \subset \mathbb{A}^n_k$ given parametrically by

$$x_1 = f_1(t),\dots,x_n = f_n(t).$$

E-mail address: park@oakland.edu (Hyungju Park).

PII: S0022-4049(02)00017-8

This paper is concerned with the following two questions on this parameterization of C:

Q1. Can we effectively determine if the parameterization

$$\psi = (f_1, \ldots, f_n) : \mathbb{A} \to C$$

is a birational equivalence, or equivalently $k(f_1, \ldots, f_n) = k(t)$?

Q2. If $\psi : \mathbb{A} \to C$ is birational, can we compute all the singularities of C? (Without knowing the ideal of C.)

Shannon–Sweedler's algebra membership algorithm [11] effectively answers Problem Q1. It uses a Gröbner bases computation involving $n + 1$ variables with respect to lexicographic order, which can quickly become highly complex for a modestly large n. A new algorithm is developed in this paper, which answers Problem Q1 using a Gröbner bases computation involving two variables regardless of n with respect to an arbitrary fixed term order.

For the special case of two polynomials $f_1, f_2 \in k[t]$ (i.e., when $n = 2$), there are several results available. Abhyankar and Moh [2] have given a necessary condition for $k[f_1, f_2] = k[t]$ in terms of degrees of f_1 and f_2:

Theorem 1 (Abhyankar and Moh [2]). *Let k be an arbitrary field of characteristic p ($p = 0$ or $p > 0$). Suppose that f_1 and f_2 are in $k[t]$ with $m := \deg(f_1) \leqslant n := \deg(f_2)$, and that p does not divide $\gcd(m, n)$. If $k[f_1, f_2] = k[t]$, then m divides n.*

Van den Essen and Yu [1,8] introduced the notion of D-resultant $D(s) \in k[s]$ of two polynomials f_1 and f_2, and gave necessary and sufficient conditions for $k(f_1, f_2) = k(t)$ and $k[f_1, f_2] = k[t]$ in terms of $D(s)$ [7, Theorem 2.1].

Recently, Gutierrez et al. [10] extended the notion of D-resultant to a pair of rational functions in $k(t)$. For two rational functions $f_1, f_2 \in k(t)$, they defined the D-resultant of f_1, f_2, and used it to characterize when $k(f_1, f_2) = k(t)$ or when $k[t] \subset k[f_1, f_2]$, and to find the singularities of the parametric affine curve defined by $x = f_1(t), y = f_2(t)$.

Example 1. Consider $f_1(t) = t^3, f_2(t) = t^2 + t \in k[t]$. The function field $k(t)$ is an algebraic extension of its subfield $k(t^3, t^2 + t)$. To determine if $k(t^3, t^2 + t) = k(t)$, denote the field $k(t^3, t^2 + t)$ by K. Then

$$\begin{aligned} t^2 + t \in K &\Rightarrow (t^2 + t)^2 = t^4 + 2t^3 + t^2 = t^4 - t + (t^2 + t) + 2t^3 \in K \\ &\Rightarrow t^4 - t = t(t^3 - 1) \in K \quad (\text{since } t^2 + t, 2t^3 \in K) \\ &\Rightarrow t \in K \quad (\text{since } t^3 - 1 \in K). \end{aligned}$$

This shows $k(t^3, t^2 + t) = k(t)$. However, since the Abhyankar–Moh necessary condition is not satisfied, $k[f_1, f_2] \subsetneq k[t]$. This means that the parameterization $\psi = (t^3, t^2 + t) : \mathbb{A} \to C$ is a birational equivalence, but not an isomorphism.

Remark 1. It is worth noting that Problem Q1 is closely related to the problem of decomposing polynomials.

For given nonconstant polynomials $f_1,\dots,f_n \in k[t]$, if $k(f_1,\dots,f_n)$ is a proper subfield of $k(t)$, then, by Lüroth's theorem, it is equal to $k(h)$ for some rational function $h \in k(t)$ with $\deg(h) > 1$. In this case, the polynomials $f_1,\dots,f_n$ are decomposable in the following way: for each $i = 1,\dots,n$, $\exists g_i \in k(t)$ such that $f_i(t) = g_i(h(t))$. Therefore, Problem Q1 has affirmative answer if and only if the polynomials $f_1,\dots,f_n$ are not decomposable in this form. See [4,8] for further discussion.

In this paper, we give algorithmic solutions to Problems Q1 and Q2 in the general case of n polynomials using the method of Gröbner bases.

2. Birational parameterization of curves

Throughout this paper, unless there is a possibility of confusion, we will use the shorthand notation $\mathbb{A}^n$ for the affine space $\mathbb{A}^n_k$.

For an arbitrary field k, consider the curve $C \subset \mathbb{A}^n$ given parametrically by

$$x_1 = f_1(t),\dots,x_n = f_n(t),$$

where $f_1,\dots,f_n \in k[t]$. The morphism ψ defined by

$$\psi = (f_1,\dots,f_n) : \mathbb{A} \to \mathbb{A}^n$$

will be simply referred to as the parameterization of C by polynomials $f_1,\dots,f_n$. The curve C is the Zariski closure $\overline{\mathrm{Im}(\psi)}$ of $\mathrm{Im}(\psi)$ in $\mathbb{A}^n$, and we occasionally identify the morphism $\psi : \mathbb{A} \to \mathbb{A}^n$ with the induced morphism $\psi : \mathbb{A} \to C$.

Problem Q1 is equivalent to determining if the induced map of the functions fields

$$\begin{aligned}\psi^* :\ K(\mathbb{A}^n) = k(x_1,\dots,x_n) &\to K(\mathbb{A}) = k(t).\\ x_i &\mapsto f_i\end{aligned}$$

is surjective, i.e.,

$$k(f_1,\dots,f_n) = k(t).$$

So we need to understand what conditions on the polynomials $f_1,\dots,f_n$ will guarantee $k(f_1,\dots,f_n) = k(t)$.

Consider the induced k-algebra homomorphism ψ^* of the coordinate rings

$$\begin{aligned}\psi^* : A(\mathbb{A}^n) = k[x_1,\dots,x_n] &\to A(\mathbb{A}) = k[t],\\ x_i &\mapsto f_i.\end{aligned}$$

Note that the coordinate ring of $C = \overline{\mathrm{Im}(\psi)}$ is

$$A(C) = k[x_1,\dots,x_n]/\mathrm{Ker}(\psi^*) = \mathrm{Im}(\psi^*) \cong k[f_1,\dots,f_n].$$

Proving that ψ is an immersion is equivalent to proving that their coordinate rings are isomorphic:

$$k[t] = k[f_1, \dots, f_n].$$

Now we describe the injectivity and birationality of

$$\psi : \mathbb{A} \to C \subset \mathbb{A}^n$$

in terms of a set of bivariate polynomials derived from f_i's.

Lemma 1. *Suppose that $f_1', \dots, f_n' \in k[t]$ are not identically zero. Then, the morphism*

$$\psi := (f_1, \dots, f_n) : \mathbb{A} \to \mathbb{A}^n$$

is finite.

Proof. We may assume, without loss of generality, that f_1 is not a constant. Consider

$$\begin{aligned} \psi^* : k[x_1, \dots, x_n] &\to k[t], \\ x_i &\mapsto f_i. \end{aligned}$$

Dividing f_1 by its leading coefficient if necessary, we may assume $f_1(t)$ is monic. Then the monic polynomial

$$G(T) := f_1(T) - f_1 \in k[f_1, \dots, f_n](T)$$

gives an integral dependence of $t \in k[t]$ on $k[f_1, \dots, f_n]$. □

For $f_1, \dots, f_n \in k[t]$, we introduce a new variable s and consider

$$f_1(t), \dots, f_n(t), \quad f_1(s), \dots, f_n(s) \in k[s,t].$$

For each $i = 1, \dots, n$, $t - s$ divides $f_i(t) - f_i(s)$ and there exists $g_i(s,t) \in k[s,t]$ such that $f_i(t) - f_i(s) = (t-s)g_i(s,t)$. We will identify the fraction $(f_i(t) - f_i(s))/(t-s)$ with the polynomial $g_i(s,t) \in k[s,t]$. One notes that this fraction is the Bezoutian [5,6] of the polynomials f_i and 1, and it is easy to prove that $g_i(s,s) = f_i'(s)$. The following theorem characterizes the algebraic set $V_{\bar{k}}(g_1, \dots, g_n) \subset \mathbb{A}^2$.

Theorem 2. *For $f_1, \dots, f_n \in k[t]$, let*

$$g_i(s,t) := \frac{f_i(t) - f_i(s)}{t - s} \in k[s,t], \quad i = 1, \dots, n.$$

Consider the induced morphism $\psi = (f_1, \dots, f_n) = \bar{k} \to \bar{k}^n$. Then

$$V_{\bar{k}}(g_1, \dots, g_n) = A_\psi \amalg B_\psi, \tag{1}$$

where

$$A_\psi = \{(a,b) \mid a \neq b \in \bar{k} \text{ and } \psi(a) = \psi(b)\},$$

$$B_\psi = \{(a,a) \mid a \in \bar{k} \text{ and } f_1'(a) = \cdots = f_n'(a) = 0\}.$$

Proof. Suppose $(a,b) \in A_\psi$. Then,

$$\begin{aligned}(a,b) \in A_\psi &\Rightarrow a \neq b \quad \text{and} \quad \psi(a) = \psi(b)\\ &\Rightarrow a \neq b \quad \text{and} \quad f_i(a) = f_i(b) \quad \forall i = 1,\ldots,n\\ &\Rightarrow g_i(a,b) = 0 \quad \forall i = 1,\ldots,n\\ &\Rightarrow (a,b) \in V_{\bar{k}}(g_1,\ldots,g_n).\end{aligned}$$

Hence, $A_\psi \subset V_{\bar{k}}(g_1,\ldots,g_n)$.

Suppose $(a,a) \in B_\psi$. Then,

$$\begin{aligned}(a,a) \in B_\psi &\Rightarrow f_i'(a) = 0 \quad \forall i = 1,\ldots,n\\ &\Rightarrow g_i(a,a) = 0 \quad \forall i = 1,\ldots,n\\ &\Rightarrow (a,a) \in V_{\bar{k}}(g_1,\ldots,g_n).\end{aligned}$$

Hence $B_\psi \subset V(g_1,\ldots,g_n)$. Therefore, $A_\psi \amalg B_\psi \subset V_{\bar{k}}(g_1,\ldots,g_n)$.

In order to show $V_{\bar{k}}(g_1,\ldots,g_n) \subset A_\psi \amalg B_\psi$, let $(a,b) \in V_{\bar{k}}(g_1,\ldots,g_n)$.

If $a \neq b$, then

$$\begin{aligned}&g_i(a,b) = \frac{f_i(b) - f_i(a)}{b-a} = 0 \quad \forall i = 1,\ldots,n\\ &\Rightarrow f_i(b) = f_i(a) \quad \forall i = 1,\ldots,n\\ &\Rightarrow \psi(a) = \psi(b)\\ &\Rightarrow (a,b) \in A_\psi.\end{aligned}$$

If $a = b$, then

$$\begin{aligned}&g_i(a,a) = 0 \quad \forall i = 1,\ldots,n\\ &\Rightarrow a \in V_{\bar{k}}(g_1(s,s),\ldots,g_n(s,s)) = V(f_1'(s),\ldots,f_n'(s))\\ &\Rightarrow (a,a) \in B_\psi. \qquad \Box\end{aligned}$$

Remark 2. The set A_ψ in Theorem 2 describes the multiple points on the curve C, while the set B_ψ describes the ramification points (or branch points) on C. More precisely, if $(a,b) \in A_\psi$, then the point $\psi(a) = \psi(b)$ on C has multiplicity of at least 2. If $(a,a) \in B_\psi$, then $\psi(a)$ is a ramification point on C. Therefore, if $B_\psi = \emptyset$, then the parameterization $\psi : \mathbb{A} \to C$ is an étale morphism.

Theorem 3. *For $f_1,\dots,f_n \in k[t]$, let*

$$g_i(s,t) := \frac{f_i(t)-f_i(s)}{t-s} \in k[s,t], \quad i=1,\dots,n.$$

Suppose that $f_1',\dots,f_n' \in k[t]$ are not identically zero and C is the curve in $\mathbb{A}^n$ given parametrically by $x_1 = f_1(t),\dots,x_n = f_n(t)$. Then the parameterization

$$\psi = (f_1,\dots,f_n) = \mathbb{A} \to C$$

is a birational equivalence if and only if $V_{\bar{k}}(g_1,\dots,g_n)$ is a finite set.

Proof. We may assume that k is algebraically closed. By Lemma 1, the morphism $\psi : \mathbb{A} \to \mathbb{A}^n$ is finite, and thus proper. Hence $\mathrm{Im}(\psi)$ is a Zariski closed set of dimension 1 in $\mathbb{A}^n$, and is equal to C.

($\Longleftarrow$) Let $V(g_1,\dots,g_n) = \{(a_1,b_1),\dots,(a_l,b_l)\}$. Define open sets $U \subset \mathbb{A}$ and $V \subset \mathbb{A}^n$ by

$$U = \mathbb{A} - \{a_1,\dots,a_l\}, \quad V = C - \{\psi(a_1),\dots,\psi(a_l)\}.$$

Then ψ induces a finite injective morphism $\psi|_U : U \to V$. Since each fiber of $\psi|_U$ has one point, its degree $[K(U):K(V)]$ is 1. Therefore, $\psi = \mathbb{A} \to C$ is birational.

($\Rightarrow$) Since $\psi : \mathbb{A} \to C = \mathrm{Im}(\psi)$ is birational, there exist open sets $U \subset \mathbb{A}$ and $V \subset C$ such that ψ induces an isomorphism between them. Since $\mathbb{A} - U$ is a proper closed subset of $\mathbb{A}$, the irreducibility of $\mathbb{A}$ forces $\dim(\mathbb{A} - U) < 1$, i.e. $\mathbb{A} - U$ is a finite set. Therefore, the injectivity of ψ fails only at finitely many points of $\mathbb{A}$, and A_ψ is a finite set. Since at least one of f_i''s is nonzero, $f_1',\dots,f_n' \in k[t]$ have at most finitely many zeros. This means that B_ψ is a finite set. Hence, by Theorem 2 $V(g_1,\dots,g_n) = A_\psi \amalg B_\psi$ is a finite set. □

Corollary 4. *For $f_1,\dots,f_n \in k[t]$, let*

$$g_i(s,t) := \frac{f_i(t)-f_i(s)}{t-s} \in k[s,t], \quad i=1,\dots,n.$$

Suppose that $f_1',\dots,f_n' \in k[t]$ are not identically zero. Then,

$$k(f_1,\dots,f_n) = k(t)$$

if and only if $|V(g_1,\dots,g_n)| < \infty$.

Let $\pi_1 : \mathbb{A}^2_{\bar{k}} \to \mathbb{A}_{\bar{k}}$ be the projection onto the first component. C is the curve in $\mathbb{A}^n$ given parametrically by $x_1 = f_1(t),\dots,x_n = f_n(t)$. If the parameterization $\psi = (f_1,\dots,f_n) = \mathbb{A}_{\bar{k}} \to C_{\bar{k}}$ is a birational equivalence, then $\psi(\pi_1(V_{\bar{k}}(g_1,\dots,g_n))) \subset C_{\bar{k}}$ is a finite set. The following theorem says that this set describes all the singularities of $C_{\bar{k}}$.

Theorem 5. *For $f_1,\dots,f_n \in k[t]$, let*

$$g_i(s,t) := \frac{f_i(t)-f_i(s)}{t-s} \in k[s,t], \quad i=1,\dots,n.$$

If the parameterization $\psi=(f_1,\dots,f_n)=\mathbb{A}_{\bar{k}}\to C_{\bar{k}}$ *is a birational equivalence, then* $\psi(\pi_1(V_{\bar{k}}(g_1,\dots,g_n)))\subset C_{\bar{k}}$ *is the set of all the singularities of* $C_{\bar{k}}$.

Proof. The map ψ is the normalization of $C_{\bar{k}}$, which can be seen as a cascade of blow-ups. Noting that the resolution of each singularity produces a point in A_ψ or B_ψ, one deduces a theorem from Theorem 2. □

Theorem 6. *For* $f_1,\dots,f_n\in k[t]$, *let*

$$g_i(s,t):=\frac{f_i(t)-f_i(s)}{t-s}\in k[s,t],\quad i=1,\dots,n.$$

Suppose that $f_1',\dots,f_n'\in k[t]$ *are not identically zero. Then, the morphism*

$$\psi:=(f_1,\dots,f_n):\mathbb{A}\to\mathbb{A}^n$$

is a closed immersion if and only if $V_{\bar{k}}(g_1,\dots,g_n)=\emptyset$.

Proof. By Theorem 5, the condition $V_{\bar{k}}(g_1,\dots,g_n)=\emptyset$ is equivalent to the nonsingularity of the curve $C_{\bar{k}}:=\overline{\mathrm{Im}(\psi)}$. This immediately implies the theorem. □

Corollary 7. *For* $f_1,\dots,f_n\in k[t]$, *let*

$$g_i(s,t):=\frac{f_i(t)-f_i(s)}{t-s}\in k[s,t],\quad i=1,\dots,n.$$

Suppose that $f_1',\dots,f_n'\in k[t]$ *are not identically zero. Then,*

$$k[f_1,\dots,f_n]=k[t]$$

if and only if $V_{\bar{k}}(g_1,\dots,g_n)=\emptyset$.

3. Examples and applications

The results of the previous section provide a simple new proof of the following well-known result.

Theorem 8 (A special case of the Abhyankar–Moh epimorphism theorem). *Suppose that* $f_1,f_2\in k[t]$ *and* $\gcd(\deg(f_1),\deg(f_2))=1$. *Then* $k(f_1,f_2)=k(t)$ *while* $k[f_1,f_2]\neq k[t]$.

Proof. Let $m=\deg(f_1)$ and $n=\deg(f_2)$. From the chains of field extensions

$$k(f_i)\hookrightarrow k(f_1,f_2)\hookrightarrow k(t),\quad i=1,2,$$

one easily deduces that $[k(t):k(f_1,f_2)]$ is a common divisor of $m=[k(t):k(f_1)]$ and $n=[k(t):k(f_2)]$. Hence, the condition $\gcd(m,n)=1$ implies $[k(t):k(f_1,f_2)]=1$, i.e., $k(f_1,f_2)=k(t)$.

It remains to show that the set $V_{\bar{k}}(g_1,g_2)\subset\mathbb{A}^2$ is nonempty where $g_1(s,t):=(f_1(t)-f_1(s))/(t-s)$ and $g_2(s,t):=(f_2(t)-f_2(s))/(t-s)$. Consider the projective embedding of $\mathbb{A}^2$ into $\mathbb{P}^2$, and let $g_1^h,g_2^h\in k[s,t,u]$ be the homogenizations of $g_1,g_2\in k[s,t]$. Then, the points at infinity of $V_{\bar{k}}(g_1^h,g_2^h)$ is described by

$$V_{\bar{k}}\left(\frac{t^m-s^m}{t-s},\frac{t^n-s^n}{t-s}\right),$$

which is empty due to the condition $\gcd(m,n)=1$. By Bezout, this means $V_{\bar{k}}(g_1^h,g_2^h)$ has $(m-1)(n-1)$ points in $\mathbb{A}^2$ (counting multiplicity). Since $V_{\bar{k}}(g_1,g_2)$ is nonempty, Corollary 7 implies $k[f,g]\neq k[t]$. □

Example 2. Consider $f_1(t)=t^3$ and $f_2(t)=t^2+t\in k[t]$ of Example 1. Let us compute

$$V\left(\frac{f_1(t)-f_1(s)}{t-s},\frac{f_2(t)-f_2(s)}{t-s}\right).$$

We have to solve

$$\frac{f_1(t)-f_1(s)}{t-s}=\frac{t^3-s^3}{t-s}=t^2+ts+s^2=0,$$

$$\frac{f_2(t)-f_2(s)}{t-s}=\frac{(t^2-s^2)+(t-s)}{t-s}=t+s+1=0.$$

From the second equation, $t=-s-1$. By putting it into the first equation,

$$(-s-1)^2+(-s-1)s+s^2=s^2+s+1=0.$$

Let ζ be a primitive cubic root of unity in $\bar{k}$. Then,

$$V_{\bar{k}}\left(\frac{f_1(t)-f_1(s)}{t-s},\frac{f_2(t)-f_2(s)}{t-s}\right)=\{(\zeta,\zeta^2),(\zeta^2,\zeta)\}.$$

Since this set is finite, Theorem 3 confirms our earlier finding $k(t^3,t^2+t)=k(t)$. But since this set is nonempty, by Theorem 6, $k[t^3,t^2+t]\subsetneq k[t]$ as predicted by the Abhyankar–Moh result [2]. By Theorem 5, the plane curve parametrized by $x=f_1(t),y=f_2(t)$ has precisely one singular point $(f_1(\zeta),f_2(\zeta))=(f_1(\zeta^2),f_2(\zeta^2))=(1,-1)$.

For $f_1,\dots,f_n\in k[t]$, define $g_1,\dots,g_n$ by $g_i(s,t):=(f_i(t)-f_i(s))/(t-s)$, $i=1,\dots,n$. The finiteness condition on $V(g_1,\dots,g_n)$ described in Theorem 3 is equivalent to the zero dimensionality of the ideal $I:=\langle g_1,\dots,g_n\rangle\subset k[s,t]$. Fix a term order $\prec$ on the set of monomials in $k[s,t]$, and let $h_1,\dots,h_l\in k[s,t]$ be the reduced Gröbner basis of the ideal I w.r.t. $\prec$. For an arbitrary polynomial $f\in k[s,t]$, denote the initial (or leading) term of f w.r.t. $\prec$ by $\mathrm{in}(f)$. Then I is zero dimensional if and only if there exist

$i, j \in \{1, \ldots, l\}$ such that $\mathrm{in}(h_i) = s^p$ and $\mathrm{in}(h_j) = t^q$ for some $p, q \in \mathbb{N}$ (see [3, Theorem 2.2.7] for a proof). This produces the following algorithmic solution to Problem Q1:

Algorithm 1.

```
Input:  $f_1, \ldots, f_n \in k[t]$.
Output: *yes* if $k(f_1, \ldots, f_n) = k(t)$, *no* otherwise.
    Step 1: For each $i = 1, \ldots, n$, compute $g_i := (f_i(t) - f_i(s))/(t - s) \in k[s, t]$.
    Step 2: Compute the reduced Gröbner basis $G = \{h_1, \ldots, h_l\}$ of the ideal
            $I := \langle g_1, \ldots, g_n \rangle \subset k[s, t]$.
    Step 3: Output *yes* if there exist $i, j \in \{1, \ldots, l\}$ such that $\mathrm{in}(h_i) = s^p$ and $\mathrm{in}(h_j) = t^q$
            for some $p, q \in \mathbb{N}$. Output *no* otherwise.
```

As mentioned in the Introduction, Shannon–Sweedler's algebra membership algorithm [11] effectively answers Problem Q1. It uses a Gröbner bases computation involving $n + 1$ variables with respect to lexicographic order, which can quickly become highly complex for even a modest n. The algorithm described above answers Problem Q1 using a Gröbner bases computation involving two variables regardless of n with respect to an arbitrary fixed term order.

The following examples are worked out with the computer algebra system *Singular* [9].

Example 3. Consider the curve $C \subset \mathbb{A}^2_{\mathbb{C}}$ given parametrically by

$$x = f_1(t) := 2t^8 + t^4 + 3t + 1, \quad y = f_2(t) := t^4 - 2t^2 + 2.$$

Then,

$$\begin{aligned} g_1(s,t) &:= \frac{f_1(t) - f_1(s)}{t - s} \\ &= 2(t^7 + t^6 s + t^5 s^2 + t^4 s^3 + t^3 s^4 + t^2 s^5 + t s^6 + s^7) \\ &\quad + (t^3 + t^2 s + t s^2 + s^3) + 3, \\ g_2(s,t) &:= \frac{f_2(t) - f_2(s)}{t - s} \\ &= (t^3 + t^2 s + t s^2 + s^3) - 2(t + s). \end{aligned}$$

Fix the lex order $\prec$ on $\mathbb{C}[s, t]$ with $s \prec t$. Then a computation shows that the reduced Gröbner basis of $\{g_1, g_2\}$ w.r.t. $\prec$ is $\{h_1, h_2\}$ where

$$\begin{aligned} h_1 &= 128s^{10} - 640s^8 + 1600s^6 + 48s^5 - 2240s^4 - 96s^3 + 1800s^2 + 108s - 639, \\ h_2 &= 3t - 16s^6 + 48s^4 - 68s^2 - 3s + 36. \end{aligned}$$

Therefore, the parameterization $\psi = (f_1, f_2) : \mathbb{A}_{\mathbb{C}} \to C$ is a birational equivalence, but not an isomorphism. Note that h_1 is a univariate polynomial of s, which can be numerically solved. A numerical computation shows that $h_1(s)$ has two real roots and eight complex roots. Let $s_1,\dots,s_{10}$ be the ten roots of h_1. Then $S := \{(f_1(s_i), f_2(s_i)) \mid i = 1,\dots,10\}$ is the set of singularities of C, which consists of five points.

Although $\mathbb{C}[f_1, f_2] \neq \mathbb{C}[t]$, the Abhyankar–Moh necessary condition [2] for $\mathbb{C}[f_1, f_2] = \mathbb{C}[t]$ is satisfied since $\deg(f_1)$ divides $\deg(f_2)$. Hence, this example confirms that the Abhyankar–Moh condition is a necessary but not a sufficient condition for $\mathbb{C}[f_1, f_2] = \mathbb{C}[t]$.

Example 4. Consider the curve $C \subset \mathbb{A}^3$ given parametrically by

$$x = f_1(t) := t^{10} + t^4, \qquad y = f_2(t) := t^8 + 2t^2, \qquad z = f_3(t) := t^6 - t^4 + 1.$$

Then, for $g_i(s,t) := (f_i(t) - f_i(s))/(t-s)$, $i = 1,2,3$, the reduced Gröbner basis G of $\{g_1, g_2, g_3\}$ w.r.t. the degree reverse lex order is

$$G = \{t + s\}.$$

Hence, according to Algorithm 1, the parameterization

$$\psi = (f_1, f_2, f_3) : \mathbb{A} \to C$$

is not a birational equivalence.

References

[1] A. Abhyankar, Algebraic Geometry for Scientists and Engineers, Mathematical Surveys and Monographs, Vol. 35, American Mathematical Society, Providence, RI, 1990.

[2] A. Abhyankar, T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math. 276 (1975) 148–166.

[3] W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Graduate Studies in Mathematics, Vol. 3, American Mathematical Society, Providence, RI, 1994.

[4] C. Alonso, J. Gutierrez, T. Recio, A rational function decomposition algorithm, J. Symbol. Comput. 19 (1995) 527–544.

[5] A. Cayley, On the theory of elimination, Cambridge Dublin Math J. III (1865) 210–270.

[6] A.L. Dixon, The elimination of three quantics in two independent variables, Proc. London Math. Soc. 6 (1908) 468–478.

[7] A. van den Essen, J. Yu, The *D*-resultant, singularities and the degree of unfaithfulness, Proc. Amer. Math. Soc. 125 (3) (1997) 689–695.

[8] J. von zur Gathen, J. Gutierrez, R. Rubio, On multivariate polynomial decomposition, in: V. Ganzha, E. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing-CASC'99, Springer, Berlin, 1999, pp. 463–478.

[9] G.-M. Greuel, G. Pfister, H. Schönemann, SINGULAR 2.0. A computer algebra system for polynomial computations, Centre for Computer Algebra, University of Kaiserslautern, 2001, http://www.singular.uni-kl.de.

[10] J. Gutierrez, R. Rubio, J. Yu, D-resultant for rational functions, Proc. Amer. Math. Soc. 2002, to appear.

[11] D. Shannon, M. Sweedler, Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms determine birational equivalence, J. Symbol. Comput. 6 (2–3) (1988) 267–273.