Polynomial Parametrization of Regular Curves

J. Gutierrez [a,1], R. Rubio [a,1] and J. Schicho [b,2]

[a] *Dep. de Matemáticas, Estadística y Computación, Universidad de Cantabria E–39071 Santander, Spain,*
{jaime, sarito}@matesco.unican.es

[b] *RISC, Johannes Kepler University A–4040 Linz, Austria,*
Schicho@risc.uni-linz.ac.at

Abstract

This paper gives an algorithm to compute a proper polynomial parametrization of non-singular polynomial parametric curves $C = \mathbf{V}(f)$. We use a classical result by Abhyankar and Moh in order to avoid the genus computation of curve C. We present a sequential algorithm that only requires $O(\deg f^3 \log \deg f \log\log \deg f)$ arithmetic operations.

keywords: parametric curves, symbolic computation, algebraic geometry.

1 Introduction

A planar algebraic curve C is any curve which can be described by the implicit polynomial equation $f(x, y) = 0$, that is, C is the zero set of a non–constant polynomial $f(x, y)$,

$$C = \mathbf{V}(f) = \{(x_0, y_0) \mid f(x_0, y_0) = 0\}.$$

A planar parametric curve C (also known as rational curve) is a curve which can be defined parametrically as $x = \frac{p(t)}{r(t)}$ and $y = \frac{q(t)}{r(t)}$ where $p(t), q(t)$ and

[1] Supported by PB97–0346, Spain.
[2] Supported by SFB 1303/ P3, Austria.

$r(t)$ are univariate polynomials, more concrete, C is the smallest algebraic set containing:

$$T = \Big\{ \Big(\frac{p(t_0)}{r(t_0)}, \frac{q(t_0)}{r(t_0)} \Big) \mid r(t_0) \neq 0 \Big\}.$$

In this case, we say that $\left(\frac{p(t)}{r(t)}, \frac{q(t)}{r(t)}\right)$ is a parametrization of the curve C. Both representations have their inherent advantages.

For one hand, the implicit representation is most convenient for determine whether a given point lies on the curve, and determine on which side of the curve it lies. To do this, one merely evaluates the polynomial $f(x, y)$ at a certain point (x_1, y_1). If $f(x_1, y_1) = 0$, the point lies on the curve, if $f(x_1, y_1) > 0$ the point lies on one side of the curve, and if $f(x_1, y_1) < 0$, the point lies on the other side of the curve.

On the other hand, parametric curves (such as Bezier and B–spline curves) have captured the attention of the computer aided geometric design community primarily because they can be pieced together with various degree of derivative continuity, since large numbers of points on such curves can be rapidly generated for display purposes.

This motivates the design of algorithms to convert efficiently from one to the other, whenever possible.

Although all algebraic curves have an implicit representation, only irreducible algebraic curves with *genus* zero have a parametric representation. There exist various methods for computing the genus, a parametrization, in case the genus is zero (see [2,16]); and the implicit representation given a parametrization of the curve (see for instance [4,15,9]).

Polynomial parametrization of an algebraic curve —a parametric curve with has a parametrization given by polynomials $(p(t), q(t))$— if exists, has nicer properties than rational parametrizations. For instance, if the complex curve C has a polynomial parametrization, then $T = \{(p(t_0), q(t_0))\}$ is an algebraic set. A curve has a polynomial parametrization if and only if it has genus zero and exactly one *place at infinity* (see [1]); and can be compute via rational parametrization: given a rational parametrization of a curve satisfying previous properties, it can be reparametrized so that the result is a polynomial parametrization (see [11]). But it is not satisfactory compute polynomial parametrization via rational parametrization, this seems more complicated. In [13], the author gives an approach for a direct method for the computation of polynomial parametrization, but up to now there is no complete algorithm for such a direct algorithm.

In general, the number of arithmetic operations for computing a parametrization of a parametric curve is exponential in the degree of the polynomial equation $f(x, y)$.

The algebraic system MAPLE V has the package *Algebraic Curves* which was designed for performing computation with algebraic sets. The MAPLE V *parametrization* code it is dedicated to compute a parametrization of a planar algebraic curve, if it is exists. In the following example MAPLE V was unable to compute a parametrization —after two days in a SUN machine— of the curve given by the polynomial $f(x, y) =$

$$10-26\,x+5\,y\,x^{12}+10\,y^2\,x^9+5\,y^4\,x^3+10\,y^3\,x^6-6\,x\,y+191\,x^2\,y-y^2-668\,y\,x^3+63\,x\,y^2+1092\,y\,x^4-291\,x^2\,y^2-1302\,x^5\,y+471\,y^2\,x^3+1211\,y\,x^6-601\,x^4+1037\,x^5-1349\,x^6+1359\,x^7-1106\,x^8+7\,y^3+762\,x^9-421\,x^{10}+205\,x^{11}-5\,y^4-75\,x^{12}+25\,x^{13}-5\,x^{14}+y^5+x^{15}-9\,y+15\,x\,y^4+90\,y\,x^{10}+70\,y^3\,x^4+120\,y^2\,x^7-5\,x^2\,y^4-20\,x^{11}\,y-20\,x^5\,y^3-30\,x^8\,y^2+186\,x^3-60\,x\,y^3-480\,y^2\,x^4-840\,y\,x^7+110\,x^2\,y^3+420\,x^5\,y^2+515\,x^8\,y-220\,y\,x^9-80\,y^3\,x^3-220\,y^2\,x^6.$$

The MAPLE package CASA (see `http://www.risc.uni-linz.ac.at/software/-casa/casa.html`) which was also especially designed to perform operations with algebraic sets also could not produce the answer.

However, the planar algebraic curve has a polynomial parametrization given by the polynomial $p(t)$ and $q(t)$, as our algorithm (Section 3) returned in 0.55 seconds:

$$p(t) = -10 + 9\,t + t^2 - 7\,t^3 + 5\,t^4 - t^5.$$

$$q(t) = 1130 - 2906\,t + 2188\,t^2 + 2090\,t^3 - 5733\,t^4 + 4353\,t^5 + 433\,t^6 - 3561\,t^7 + 2991\,t^8 - 807\,t^9 - 551\,t^{10} + 675\,t^{11} - 338\,t^{12} + 96\,t^{13} - 15\,t^{14} + t^{15}.$$

This example illustrates that the complexity of finding the parametrization is concentrated just in the computation of the genus of the curve. Thus it is of outmost interest to be able to find faster methods, when possible, for particular classes of parametric curves.

In this paper we give an algorithm for computing a polynomial parametrization for Abhyakar–Moh curves, that is, the class of the polynomial parametric curves $(p(t), q(t))$ satisfying $K[p(t), q(t)] = K[t]$. In fact, this class of rational curves coincides with the one of polynomial parametric curves without affine singularities. Since the algorithm does not depend on the notion of the genus of a curve, its correctness can be proven in a more elementary way. The complexity of our algorithm is quite low, it uses only $O(\deg f^3 \log \deg f \log\log \deg f)$ arithmetic operations in the sequential model. The algorithm is implemented in the computer algebra system MAPLE and perfoms very well.

The structure of this paper is as follows. In Section 2, we present some results over polynomial parametrized curves. In Section 3, we give an algorithm to find a polynomial parametrization for Abhyankar–Moh curves. In Section 4, we see that our algorithm works over non-singular curves. Finally in Section 5, we show some examples of the efficiency of our implementation in the MAPLE V system.

2 Polynomial parametrized curves

In this section we will review some important results of irreducible algebraic curves with polynomial parametrization. We will also see interesting properties related to our problem.

Let K be an arbitrary field. A plane curve C is given by an irreducible polynomial equation $f(x,y)=0$, where $f(x,y)\in K[x,y]$. The curve $C=\mathbf{V}(f)$ is called a polynomial parametric curve or just a polynomial curve if and only if there exists a parametrization $(p(t),q(t))$, such that $p(t),q(t)\in K[t]$ (not both constants) and verifying $f(p(t),q(t))=0$.

We say that $(p(t),q(t))$ it is a proper parametrization if and only if for every point (x_0,y_0) of the curve C there exists a unique $t_0\in K$ such that $x_0=p(t_0), y_0=q(t_0)$, except a finite number of them (see [14]). The classical Lüroth's Theorem states that any parametric curve has a proper parametrization; in fact, we have that $K(p,q)=K(h)$ where $h(t)$ is a polynomial (see [10]), then $p=p^*(h)$, $q=q^*(h)$ for some polynomials $p^*(t),q^*(t)\in K[t]$ and $(p^*(t),q^*(t))$ is a proper polynomial parametrization of the curve C.

Between the implicitation of an irreducible algebraic curve and, if exists, its parametrization, there is a remarkable relation ([12]).

Theorem 1 *Let K be an arbitrary field. Let $f(x,y)$ be a minimal polynomial of $p(t)$ and $q(t)$, then there exists a non–zero constant c such that*

$$\mathrm{Res}_t(x-p(t),y-q(t))=cf(x,y)^\alpha$$

where

$$\alpha=|K(t):K(p,q)|.$$

Corollary 2 *If $(p(t),q(t))$ is a proper polynomial parametrization of an irreducible algebraic curve $C=V(f)$, then*

(i) $\mathrm{Res}_t(x-p(t),y-q(t))=cf(x,y)$, *where c is a nonzero constant.*

(ii) *If $p = a_n t^n \cdots + a_0$, $q = b_m t^m + \cdots + a_0$ with $\deg p = n$ and $\deg q = m$, then the leading monomial of f with respect to x is $\frac{1}{c}(-1)^{mn+n} b_m^n x^m$ and the leading monomial of f with respect to y is $\frac{1}{c}(-1)^m a_n^m y^n$. In particular, $m = \deg_x f$, $n = deg_y f$.*

PROOF. The first part is immediate since (p, q) is a proper parametrization of C over K, hence $K(p, q) = K(t)$.

For (ii), by the previous part we have $\mathrm{Res}_t(x - p(t), y - q(t)) = cf(x, y)$, we get

$$cf = \begin{vmatrix} -a_n & & & & & \\ 0 & \ddots & & & & \\ 0 & 0 & -a_n & & & \\ & & & y - b_0 & 0 & 0 \\ & & & & \ddots & 0 \\ & & & & & y - b_0 \end{vmatrix}$$

By inspection of the determinant of the Sylvester matrix associated to the polynomials $x - p(t)$ and $y - q(t)$, we observe that the maximum power in the variable y is y^n and its coefficient is $(-1)^m a_n^m \neq 0$. Similarly we get that the leading monomial of cf with respect to x is $(-1)^{mn+n} b_m^n x^m$:

$$cf = \begin{vmatrix} & & & x - a_0 & 0 & 0 \\ & & & & \ddots & 0 \\ & & & & & x - a_0 \\ -b_m & & & & & \\ 0 & \ddots & & & & \\ 0 & 0 & -b_m & & & \end{vmatrix}$$

Using the above corollary we are able to prove our main result in this section.

Theorem 3 *Let $C = \mathbf{V}(f)$ be an irreducible algebraic curve with a proper polynomial parametrization $(p(t), q(t))$ in $K[t]$, and such that deg $p = n$, deg $q = m$ and $d = \gcd(m, n)$. Then*

(i) *If $f = f_k + f_{k-1} + \cdots + f_0$, where f_i is homogeneous polynomial of f with degree i and $f_k \neq 0$. Then $k = \max\{n, m\}$.*

(ii) *If* $f = \sum_{i,j} a_{i,j}x^iy^j$*, then* $ni+mj \leq mn$ *for all* i,j *with* $a_{ij} \neq 0$*. Moreover, the* (n,m)*–weighted homogeneous polynomial* $\sum_{i,j}^{ni+mj=mn} a_{i,j}x^iy^j = a(x^{\frac{m}{d}} + \alpha y^{\frac{n}{d}})^d$ *with* $a, \alpha \in K\backslash\{0\}$ *unique.*

PROOF. **(i)** By the criterion of Abhyankar [1], C has only one point at infinity. Besides, the points at infinity correspond to the zeroes of the polynomial $f_k(x,y) = \sum_{i,j}^{i+j=k} a_{i,j}x^iy^j$, where k is the total degree of f. Hence f_k is a k–th power of a linear form $ux+vy$, where either $u \neq 0$ or $v \neq 0$. By Corollary 2 $m,n \leq k$. So $k = \max\{n,m\}$.

(ii) Suppose $m=n$, by part (i), $\deg f = m$. This implies $i+j \leq m$. Moreover, $\sum_{i,j}^{ni+mj=mn} a_{i,j}x^iy^j = f_m = (ux+vy)^m$ where u,v are in the algebraic closure of K and $uv \neq 0$. Then, $u^{m-i}v^i \in K$ for every $i \in \{0,\cdots,m\}$. So, $a := u^m, \alpha := \dfrac{v}{u} \in K\backslash\{0\}$ and both are unique.

In general, suppose $m \neq n$. Let $g(x,y)$ be the minimal polynomial of the polynomials $(p(t)^{\frac{m}{d}}, q(t)^{\frac{n}{d}})$, that is, $g(x,y)$ is the implicit equation of $(p(t)^{\frac{m}{d}}, q(t)^{\frac{n}{d}})$. Since $\deg(p(t)^{\frac{m}{d}}) = \deg(q(t)^{\frac{n}{d}}) = \frac{mn}{d}$, there exists a proper parametrization $(\hat{p},\hat{q})$ in $K[t]$ of $g(x,y)$ satisfying $s = \deg\hat{p} = \deg\hat{q}$, (see [5]). We have $1 \leq s = \deg g \leq \frac{mn}{d}$. So, the result is true for g. In other words, the homogeneous polynomial g_s is equal to $a'(x+\alpha y)^s$ with $a', \alpha \in K\backslash\{0\}$ and unique.

On the other hand, the two polynomials p,q satisfy the relation $g(x^{\frac{m}{d}}, y^{\frac{n}{d}}) = 0$, hence $f(x,y)$ divides $g(x^{\frac{m}{d}}, y^{\frac{n}{d}})$. Write f as a sum of $\tilde{f}_l = \sum_{i,j}^{ni+mj=l} a_{i,j}x^iy^j$, the (n,m)–weighted homogeneous components of f. Then the largest component $\tilde{f}_r$ divides the largest weighted homogeneous component of $g(x^{\frac{m}{d}}, y^{\frac{n}{d}})$. Note that $g_s(x^{\frac{m}{d}}, y^{\frac{n}{d}}) + \cdots + g_0(x^{\frac{m}{d}}, y^{\frac{n}{d}})$ is the decomposition of $g(x^{\frac{m}{d}}, y^{\frac{n}{d}})$ into (n,m)–weighted homogeneous components; i.e., $\tilde{g}_{\frac{mnt}{d}}(x,y) = g_t(x^{\frac{m}{d}}, y^{\frac{n}{d}})$. This implies that $\tilde{f}_r$ divides $g_s(x^{\frac{m}{d}}, y^{\frac{n}{d}}) = a'(x^{\frac{m}{d}} + \alpha y^{\frac{n}{d}})^s$.

Since $\tilde{f}_r \,|\, a'(x^{\frac{m}{d}} + \alpha y^{\frac{n}{d}})^s$, there exist $1 \leq m' \leq m$ and $1 \leq n' \leq n$ such that $\tilde{f}_r$ has $x^{m'}$ and $y^{n'}$ as monomials. Then $r = m'n = n'm \leq nm$. And, by Corollary 2 $r = mn$. So, $\tilde{f}_r = \sum_{i,j}^{ni+mj=mn} a_{i,j}x^iy^j$.

Moreover, since $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$ and $\alpha \neq 0$ we have that $x^{\frac{m}{d}} + \alpha y^{\frac{n}{d}}$ is irreducible. Therefore $\tilde{f}_{mn} = a(x^{\frac{m}{d}} + \alpha y^{\frac{n}{d}})^d$, where $a, \alpha \in K\backslash\{0\}$ unique.

Following the proof of the above theorem we observe:

Corollary 4 *Let $C = \mathbf{V}(f)$ be an irreducible algebraic curve with a proper polynomial parametrization $(p(t), q(t))$ in $K[t]$. Then it has exactly one point at infinity with K-coordinates.*

Next theorem is a very important result in algebraic geometry, which was given by Abhyankar and Moh around 1975 (see [3]).

Theorem 5 *Let K be an arbitrary field. Let $p(t)$ and $q(t)$ be non–constant polynomials of degree n and m in $K[t]$. Assume either n or m is not divisible by the characteristic of the field K. If $K[t] = K[p, q]$, then either m divides n, or n divides m.*

Now, we are going to see for which kind of curves our algorithm computes its polynomial parametrization.

Definition 6 *We say that a polynomial parametric curve $C = \mathbf{V}(f)$ with a proper parametrization $(p(t), q(t))$ is an Abhyankar–Moh curve if and only if $K[p, q] = K[t]$.*

3 Algorithm

In this section we give an algorithm to find a polynomial parametrization of an irreducible algebraic curve for Abhyankar–Moh curves. The method is presented from a theoretical point of view and considering its implementation on MAPLE.

Algorithm 1 **Input :** *An irreducible polynomial f with coefficients in K with degree k.*

Output: *A polynomial parametrization of $f(x, y)$, if $f(x, y)$ is an Abhyankar–Moh curve.*

A *Let $n_x := \deg_x f$, $n_y := \deg_y f$ and $p_x := x$ and $p_y := y$.*
B *WHILE $n_x > 1$ and $n_y > 1$ do*
- ***B.1*** *If n_x does not divide n_y and n_y does not divide n_x RETURN 'polynomial parametrization not found'.*
- ***B.2*** *Let $M := \max\{n_x, n_y\}$, $m := \min\{n_x, n_y\}$, n:=M/m, X the variable with degree m, Y the variable with degree M. Let $\tilde{f}_M := \sum_{i,j}^{in+j=M} a_{i,j} X^i Y^j$. Compute $a, \alpha \in K \backslash \{0\}$ such that $\tilde{f}_M = a(X + \alpha Y^n)^m$. If such a, α don't exist RETURN 'polynomial parametrization not found'.*

B.3 *Let* $f := f(X - \alpha Y^n, Y)$, $p_X := p_X(X - \alpha Y^n, Y)$, $n_x := \deg_x f$ *and* $n_y := \deg_y f$.

B.4 *If* $n_x > M$ *or* $n_y > M$, *RETURN 'polynomial parametrization not found'.*

C *If* $lc_x(f)$ *or* $lc_y(f)$ *is non–constant RETURN 'polynomial parametrization not found'.*

D *Let* X *be the variable with* $\deg_X f = 1$ *and* $p_z := p_z(X - f(Y = t)/lc_X(f), t)$ *for* $z = x, y$.

E *RETURN* (p_x, p_y).

Analysis It's is important to highlight that the polynomial map

$$\begin{array}{rccc} \phi: & K[X,Y] & \longrightarrow & K[X,Y] \\ & X & \longmapsto & X + \alpha Y^n \\ & Y & \longmapsto & Y \end{array}$$

is an automorphism. In particular transforms an Abhyankar–Moh curve into another one. We will see that the algorithm determines correctly whether $f(x,y)$ has polynomial parametrization with the required conditions, and if so, computes one.

Steps B.1, B.2, B.4 and C are just filters based on the properties of Corollary 2 and Theorem 3.

If the degree of f is equal 1 with respect to one variable we can immediately decide if it is polynomial parametrizable: $f = a(Y)X + b(Y)$, if a is a non–constant polynomial it is not, otherwise $(-b(t)/a, t)$ is a polynomial parametrization.

Suppose that $\deg_Y f \geq \deg_X f > 1$. Then after step B, we get another polynomial parametrizable polynomial $\hat{f}$. If f is polynomial parametrizable, it satisfies $\deg_X f = \deg_X \hat{f}$, $\deg_Y f > \deg_Y \hat{f}$ and $\deg f > \deg \hat{f}$. Moreover, f is polynomial parametrizable if and only if $\hat{f}$ is polynomial parametrizable:

By Theorem 3, we can write $f = a(X + \alpha Y^n)^m + \tilde{f}_{M-1} + \cdots + \tilde{f}_0$. The constants (a, α) are unique and $\hat{f} = f(X - \alpha Y^n, Y) = aX^m + \tilde{f}_{M-1}(X - \alpha Y^n, Y) + \cdots + \tilde{f}_0(X - \alpha Y^n, Y)$. Then $\deg_X f = \deg_X \hat{f}$ and $\deg_Y f > \deg_Y \hat{f}$. Since f is polynomial parametrizable, we also have that $\deg f = M > \deg \hat{f} = \max\{\deg_X \hat{f}, \deg_Y \hat{f}\}$, see proof of Theorem 3.

Suppose f has a polynomial parametrization (p_X, p_Y). Then $(\hat{p}_X, \hat{p}_Y)$, where $\hat{p}_X = p_X + \alpha {p_Y}^n$ and $\hat{p}_Y = p_Y$, is a polynomial parametrization of $\hat{f}$. Conversely, if $(\hat{p}_X, \hat{p}_Y)$ is a polynomial parametrization of $\hat{f}$, we can find a parametrization (p_X, p_Y) for f: $p_X = (X - \alpha Y^n) \circ (\hat{p}_X, \hat{p}_Y)$ and $p_Y = \hat{p}_Y$.

Finally, we will analyze the complexity. We denote by $O(M(r))$ the number of arithmetic operations in the ground field K to compute the product of two univariate polynomials of degree r. We can choose $M(r) = r \log r \log\log r$ ([7,17]), and $M(r) = rlogr$ if K supports a Fast Fourier Transform. Now, the hardest computations are in step B and D. We will analyze them separately.

STEP B.2: The computation of the polynomial $\hat{f}_M$ is just checking if each monomial in $\hat{f}_M$ satisfies the equation $in + j = M$. This costs $O(k^2)$, where k is the total degree of f. Once we have calculated $\hat{f}_M$, we can immediately get the candidate α: In fact, if $\hat{f}_M = a(X+\alpha Y^n)^m$, $\gcd\left(\hat{f}_M, \dfrac{\partial^{m-1}\hat{f}_M}{\partial X^{m-1}}\right) = \dfrac{\partial^{m-1}\hat{f}_M}{\partial X^{m-1}}$. So if $\hat{f}_M = bX^m + cX^{m-1}Y^n + \cdots + dY^M$, $\dfrac{\partial^{m-1}\hat{f}_M}{\partial X^{m-1}} = (m-1)!(bX + cY^n)$ and we get the candidate $\alpha = \dfrac{c}{b}$ if $b \neq 0$. To finish step B.3 we have just to check if $(X + \alpha Y^n)^m \mid \hat{f}_M$. For this last computation we just need to know if $\dfrac{\partial^{m-1}\hat{f}_M}{\partial X^{m-1}}(-\alpha Y^n, Y) = 0$, which equivalent to compute $\dfrac{\partial^{m-1}\hat{f}_M}{\partial X^{m-1}}(-\alpha, 1) = 0$. A bound of this last calculation is $O(m^2)$.

STEP B.3: In this step we require to compose two polynomials over the domain $D[x]$, where $D = K[y]$, it costs $O(k^2)$ operations in D. Each operation in D costs $O(M(k))$ operations in K. The total complexity of this part is $O(k^2 M(k))$.

Step B is repeated at most $k = \deg f$ times. Step D is dominated by step B. Then, the overall cost is $O(k^3 M(k))$ operations in the ground field K.

4 Polynomial Parametrization of Non–singular Curves

In this section we will see that any polynomial regular curve with polynomial parametrization is an Abhyankar–Moh curve. Therefore, we can apply our algorithm to decide if a non–singular curve has a polynomial parametrization, and in the affirmative case to compute such parametrization.

Theorem 7 *Let $f \in K[x, y]$ be an irreducible polynomial. The following are equivalent.*

(i) *The curve $C = V(f)$ has no finite singularities defined over the algebraic closure of K.*
(ii) *The ring $K[C]$ is integral closed.*

PROOF. The property of being integrally closed is independent of the base field, so we may assume without loss of generality that K is algebraically closed.

Integral closed is a local property, so (ii) is equivalent to the statement that $K[C]_{\overline{m}}$ is integral closed for any maximal ideal $\overline{m}$ in $K[C]$. A maximal ideal in $K[x, y]/(f)$ is a maximal ideal in $K[x, y]$ which contains the polynomial f. Thus the maximal ideals in $K[C]$ are in bijective correspondence with the points $p = (x_0, y_0) \in C$, via $\overline{m} = (\overline{x} - x_0, \overline{y} - y_0)$.

By [6,8], statement (i) is equivalent to the statement that all localizations $K[C]_p$ are regular local rings.

We can assert that $K[C]_p$ has dimension 1, since each prime ideal $S^{-1}\overline{p}$ such that

$$S^{-1}(0) \subset S^{-1}\overline{p} \subset S^{-1}\overline{m}$$

satisfies in $K[x, y]$

$$(0) \subset (f) \subset p \subset m.$$

But for local rings of dimension 1, the two properties regular and integrally closed are equivalent (see [6,8]).

Theorem 8 *Let $f \in K[x, y]$ be the irreducible polynomial, such that the its defined curve $C = V(f)$ is polynomial. The following are equivalent.*

(i) *The curve C has no finite singularities defined over the algebraic closure of K.*
(ii) *The curve C is an Abhyankar–Moh curve.*

PROOF. (ii) $\Rightarrow$ (i): the ring $K[C] \cong K[t]$ is integrally closed, hence (i) follows by theorem 7.

(i) $\Rightarrow$ (ii): Let $(p(t), q(t))$ be a proper polynomial parametrization of the curve C. We define $\phi : K[C] \to K[t]$ by $\phi(x) = p$ and $\phi(y) = q$. It is clear that ϕ is injective. The image $K[C] \cong K[p, q]$ is integrally closed by assumption. But $K(p, q) = K(t)$, and t fulfills the monic equation $p(z) - p(t) = 0$. Hence $t \in K[p, q]$ and ϕ is surjective.

Theorem 8 does not tell anything about singularities on the infinite. Indeed, Abhyankar–Moh curves of degree greater than 2 do have a singularity on the infinite, which tends to be quite complicated. This fact is one of the reason why the general parametrization algorithm performs bad for Abhyankar–Moh curves (see the example in the introduction).

5 Examples

In this section, we show examples of the implementation in MAPLE of our algorithm, showing the computation time. The examples have been tested on a Macintosh Centris 650. In each of the following examples we give the input bivariate polynomial over the rational function field, the computing time and the parametrization, if it exists.

Example 9 *Input:* $f = 3\,y-2\,x-2\,y^3+4\,x^2+8\,x\,y^3-8\,x\,y+4\,y^6-8\,y^4+4\,y^2-1.$

Output:
$$x = 3\,t - 4\,t^2 - 40\,t^3 + 96\,t^5 + 64\,t^6.$$
$$y = 1 - 2\,t - 4\,t^2.$$

Time: 0.18 *seconds.*

Example 10 *Input:* $f = -1112\,y^6 + 470\,x - 184\,x\,y + 18\,x^2\,y - 2912\,y^2 + 1122\,x\,y^2 - 108\,x^2\,y^2 + 1110\,y^3 - 3420\,y^4 + 178\,y^5 + 471\,y - 92\,y^{10} + 648\,x\,y^4 + 6\,x^3 - 216\,x\,y^3 + 216\,x\,y^7 - 36\,x\,y^6 + 18\,y^{11} - 92\,x^2 - 18\,x^2\,y^5 - 6\,y^{15} - 108\,y^{12} + 184\,x\,y^5 + 18\,x\,y^{10} - 793 - 648\,y^9 + 216\,y^8 - 1122\,y^7.$

Output: $x = 81316457792\,t^{10} - 7776\,t^{15} - 21327840\,t^{13} + 1283485552722240\,t^2 - 1096009521643600\,t^3 - 929310006754399\,t - 691797388720\,t^9 + 472263120\,t^{12} + 647211965777904\,t^4 + 596160\,t^{14} - 279982756219504\,t^5 + 91671645771456\,t^6 + 4537709831680\,t^8 - 23134999834480\,t^7 + 313592698159494 - 7237819200\,t^{11} + 472263120\,t^{12}.$

$y = -470\,t + 92\,t^2 - 6\,t^3 + 793.$

Time: 0.40 *seconds.*

Example 11 *Input:* $f = 10-26\,x+5\,y\,x^{12}+10\,y^2\,x^9+5\,y^4\,x^3+10\,y^3\,x^6-6\,x\,y+191\,x^2\,y-y^2-668\,y\,x^3+63\,x\,y^2+1092\,y\,x^4-291\,x^2\,y^2-1302\,x^5\,y+471\,y^2\,x^3+1211\,y\,x^6-601\,x^4+1037\,x^5-1349\,x^6+1359\,x^7-1106\,x^8+7\,y^3+762\,x^9-421\,x^{10}+205\,x^{11}-5\,y^4-75\,x^{12}+25\,x^{13}-5\,x^{14}+y^5+x^{15}-9\,y+15\,x\,y^4+90\,y\,x^{10}+70\,y^3\,x^4+120\,y^2\,x^7-5\,x^2\,y^4-20\,x^{11}\,y-20\,x^5\,y^3-30\,x^8\,y^2+186\,x^3-60\,x\,y^3-480\,y^2\,x^4-840\,y\,x^7+110\,x^2\,y^3+420\,x^5\,y^2+515\,x^8\,y-220\,y\,x^9-80\,y^3\,x^3-220\,y^2\,x^6.$

Output: $x = -10 + t^2 - 7\,t^3 + 5\,t^4 - t^5 + 9\,t.$

$y = 1130 - 2906\,t + 4353\,t^5 - 5733\,t^4 + 2090\,t^3 + 2188\,t^2 + 2991\,t^8 - 3561\,t^7 + 433\,t^6 - 551\,t^{10} - 807\,t^9 + 675\,t^{11} - 338\,t^{12} + 96\,t^{13} - 15\,t^{14} + t^{15}$.

Time: 0.58 *seconds.*

Acknowledgements

Most of this work was done when the first two authors visited RISC in Hagenberg (Austria). They are grateful for the kind hospitality and the creative atmosphere during their visits.

References

[1] S.S. Abhyankar, What is the difference between a parabola and a hyperbola, *The Mathematical Intelligencer* **10** no. 4 (1988) 36–43.

[2] S.S. Abhyankar and B. Bajaj, Automatic parametrization of curves and surfaces III, *Computer Aided Geometric Design* **5** (1987) 309–321.

[3] S.S. Abhyankar and T.T. Moh, Embeddings of the line in the plane, *Jnl fur die reineund angewandte mathematik* **276** (1975) 148–166.

[4] C. Alonso, J. Gutierrez and T. Recio, An implicitization algorithm with fewer variables, *Computer Aided Geometric Design* **12** (1995) 1–8..

[5] C. Alonso, J. Gutierrez and T. Recio, Reconsidering Algorithms for Real Parametric Curves, *Applicable Algebra in Engineering, Communication and Computing* **6** (1995) 345–352.

[6] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra* (Addison–Wesley, Reading, Mass., 1969).

[7] D.G. Cantor and E. Kaltofen, On fast multiplication of polynomials over arbitrary algebras, *Acta Inform.* **28** (1987) 693–701.

[8] R. Hartshorne, *Algebraic geometry* (Springer–Verlag, 1977).

[9] C. M. Hoffman, Algebraic and numerical techniques for offsets and blends, in: S. Michelli, M. Gasca, W. Dahmem eds. *Computations of curves and surfaces* (Kluwer Academic, 1990) 499–528.

[10] H. Lausch and W. Nöbauer, *Algebra of polynomials* (North–Holland, 1973).

[11] D. Manocha and J. Canny, Rational curves with polynomial parametrization, *Computer Aided Geometric Design* (1991) 12–19.

[12] J. McKay and S. Wang, An inversion formula for two polynomials in two variables, *J. Pure Appl. Algebra* **40** (1986) 245–257.

[13] J. Schicho, A direct method for polynomial parametrization of curves, Prepint RISC, (1999).

[14] Sederberg, T. Improperly parametrized rational curves. *Computer Aided Geometric Design* **3**(1986) 67–75.

[15] T.W. Sederberg, D.C. Anderson and R.N. Goldman, Implicit representation of parametric curves and surfaces, *Computer Vision, Graphics, and Image Processing* **28** (1984) 72–84.

[16] J.R. Sendra and F. Winkler, Symbolic parametrization of curves. *J. of Symbolic Computation* **12** (1991) 607–631.

[17] A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der chrarakteristik 2. *Acta Informatica* **27** (1977) 641–644.