Department of Computer Science Technical Reports

Department of Computer Science

1988

Computations with Algebraic Curves

Shreeram S. Abhyankar
Purdue University, ram@cs.purdue.edu

Chandrajit L. Bajaj

Report Number:
88-806

COMPUTATIONS WITH ALGEBRAIC CURVES
SOLID MODELING

Shreeram S. Abhyankar
Chandrajit L. Bajaj

CSD-TR-806
March 1988

Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC 88, Rome, Italy.

Computations with Algebraic Curves

*Shreeram S. Abhyankar**
Department of Mathematics
Purdue University
West Lafayette, IN 47907

Chanderjit L. Bajaj†
Department of Computer Science
Purdue University
West Lafayette, IN 47907

Abstract

We present a variety of computational techniques dealing with algebraic curves both in the plane and in space. Our main results are polynomial time algorithms (1) to compute the genus of plane algebraic curves, (2) to compute the rational parametric equations for implicitly defined rational plane algebraic curves of arbitrary degree, (3) to compute birational mappings between points on irreducible space curves and points on projected plane curves and thereby to compute the genus and rational parametric equations for implicitly defined rational space curves of arbitrary degree, (4) to check for the faithfulness (one to one) of parameterizations.

1 Introduction

Effective computations with algebraic curves and surfaces are increasingly proving useful in the domain of geometric modeling and computer graphics where current research is involved in increasing the geometric coverage of solids to be modeled and displayed, to include algebraic curves and surfaces of arbitrary degree, see [9, 23]. An irreducible algebraic plane curve is implicitly defined by a single prime polynomial equation $f(x,y) = 0$ while irreducible algebraic space curves which are the intersection of two algebraic surfaces are implicitly given by a pair of polynomial equations $f(x,y,z) = 0$ and $g(x,y,z) = 0$ (which generate a prime Ideal). Rational algebraic curves have an alternate representation, namely the parametric equations which are given respectively, as ($x(t)$, $y(t)$) for a plane curve and ($x(t)$, $y(t)$, $z(t)$) for a space curve, where $x(t)$, $y(t)$ and $z(t)$ are rational functions in t, i.e., the quotient of polynomials in t. All the polynomials considered here are assumed to be defined over an algebraically closed field of characteristic zero, such as the field of complex numbers.

*Supported in part by ONR contract N00014-86-0689 under URI, ARO contract DAAG29-85-C-0018 under Cornell MSI and ONR contract N00014-88-K-0402

†Supported in part by NSF Grant MIP 85-21356, ARO Contract DAAG29-85-C0018 under Cornell MSI and ONR contract N00014-88-K-0402

In this paper we consider a variety of computational techniques dealing with algebraic plane and space curves, both in the implicit and rational parametric representations. Though all algebraic curves have an implicit representation only irreducible algebraic curves with *genus* $=$ 0 are rational. Genus, a birational invariant of the curve, measures the deficiency of singularities on the curve from its maximum allowable limit. It is also equal to the topological genus (i.e. the number of handles) when the algebraic curve is viewed as a closed manifold in four dimensional real space. We present algorithms to compute the genus of plane and space algebraic curves, and when the genus is zero, algorithms to compute the rational parametric equations for implicitly defined rational algebraic curves of arbitrary degree. We also present algorithms to check whether a parameterization is faithful (i.e. one to one). Various algorithmic techniques are used, such as the mapping of points to infinity, the "passing" of a pencil of curves through fixed points, the "blowing up" of singularities by affine quadratic transformations, computing "valid" projections, the Taylor resultant, etc.

1.1 Prior Work

Much of the work in algorithmic algebraic geometry dealing with algebraic curves is classical, dating to the pre-1920's, see [16, 19, 22, 24, 25, 29, 31, 32, 36, 38, 44, 48]. However, it was not till the fundamental work of [17, 26, 49] that algebraic geometry found a firm footing, free of the falacies which the earlier classical methods were often troubled with. Modern algebraic geometry nevertheless has its drawbacks in usually being quite abstract and non-constructive. Notable exceptions have been [2, 15, 43] amongst some others. In answering questions arising in geometric modeling and computer graphics, our research efforts here are to recast much of classical and modern algebraic geometry into a constructive framework, using efficient computational techniques from computer algebra and computational geometry. We now consider specific problems dealing with algebraic curves and briefly sketch their computational history.

A variety of (complicated) algorithms have been presented for computing the genus of algebraic curves: by counting the number of linearly independent differentials of the first kind (without poles) [21], the computation of the Hilbert function [30], the computation of ramification indices, [20] and via normalization [45]. The method of this paper uses affine quadratic transformations of [2] and is noteworthy for its simplicity.

Various computational methods have been given for obtaining the parametric equations for special low degree rational algebraic curves: degree two and three plane algebraic curves, [3, 4] the rational space curves arising from the intersection of certain degree two surfaces, [27, 33]. The parameterization algorithms of this paper are applicable for algebraic curves of arbitrary degree and are based on work in [5, 6].

The reverse problem of converting from parametric to implicit equations for algebraic curves, called implicitization is achieved by straightforward elimination methods, i.e., the computation of polynomial resultants, see [8, 37, 42]. Efficient computation of polynomial resultants, also known as the Sylvester resultant, see [25, 39, 46] has been considered by various authors: for univariate polynomials, [14, 40], for multivariate polynomials, [13, 18].

Another fundamental problem has been the resolution of singularities for algebraic curves and surfaces. For curves there have been numerous proofs, by Riemann, Dedekind, Noether and recently Abhyankar [2]. A constructive version of the desingularization theorem has been effectively used in the reliable tracing of algebraic curves, see [10] and in efficient algorithms for generating configuration space obstacles for motion planning, see [11, 12].

1.2 Main Results

We base our upper bound analysis on the RAM model with basic arithmetic operations being of unit time cost, see [7, 41], ignoring for the present the computational costs arising from the growth in size of algebraic numbers. In section 2 we give an algorithm to compute the *genus* of an irreducible algebraic plane curve of degree d in $O(d^6 + d^2T(d^2))$ time. Here $T(d) = O(d^3log^2d + d^2logd\ log(1/\epsilon)$ is the time taken to compute all d real and complex root isolations, with ϵ precision of a degree d univariate polynomial [34]. In section 3 we present an $O(d^4log^3d)$ time algorithm to construct rational parameterizations for a class of algebraic plane curves of degree d having a $d-1$ fold *distinct* singularity. In section 4 we generalize the algorithm of section 3 to provide rational parameterizations for all rational algebraic plane curves of degree d in $O(d^6log^3d + d^2T(d^2))$ time. Crucial here is the distinction between *distinct* and *infinitely near* singularities of an algebraic curve of section 2. In section 5 we consider irreducible algebraic space curves which are the intersection of two algebraic surfaces. We present an $O(d^6log^3d)$ time algorithm to construct a projected plane curve whose points are in birational correspondence with a given space curve. This then generalizes the algorithm of section 2 to compute the *genus* for algebraic space curves as well as generalizes the algorithm of section 3 and section 4 to provide rational parameterizations for rational space curves, in time bound by the plane curve case. In section 6 we present an $O(d^4log^3d)$ time algorithm to check for the faithfulness (one to one) of parameterizations as well as to compute the singularities of parameterically defined algebraic curves.

2 Singularities and Genus

Consider an irreducible plane algebraic curve C_d of degree d. Lines through a point P intersects C_d (outside P) in general at $d - mult_pC_d$ points, where $mult_pC_d = e =$ multiplicity of C_d at $P =$ order at P of the polynomial equation describing C_d . The order of a polynomial equation at a point $P = (a, b)$, is the minimum $(i + j)$, when the polynomial is expressed with terms $(x-a)^i(y-b)^j$. If $e = 0$: P is not on C_d. If $e = 1$ then P is called a simple point. If $e > 1$ we say P is a *singular point* of the curve C_d with multiplicity e or an e-fold point. A 2-fold point is also called a double point and a 3-fold point a triple point.

By Bezout's theorem one may see that the maximum number of double points of C_d is $\leq \frac{(d-1)(d-2)}{2}$. Further, the number of independent conditions needed to specify C_d is $\frac{(d+2)(d+1)}{2} - 1$. One definition of the genus G of a curve C_d is a measure of how much the curve is deficient from its maximum allowable limit of singularities,

$$G = \frac{(d - 1)(d - 2)}{2} - DP \qquad (1)$$

where DP is a 'proper' counting of the number of double points of C_d (summing over all singularities, in the projective complex plane).

Distinct singularities of a plane curve can computationally be obtained by simultaneously solving for the roots of the system of polynomial equations $f = f_x = f_y = 0$ where f_x and f_y are the x and y partial derivatives of f, respectively. One way of obtaining the common solutions is to find those roots of $Res_x(f_x, f_y) = 0$ and $Res_y(f_x, f_y) = 0$ which are also the roots of $f = 0$. Here $Res_x(f_x, f_y)$ (similarly $Res_y(f_x, f_y)$) is the Sylvester resultant of f_x and f_y treating them as polynomials in x (similarly y). For a classical treatment of the Sylvester resultant see [39]. Other methods of computing the roots of a system of polynomial equations, for example via the $U-$resultant may also be used [35]. This method yields an overall time bound of $O(d^6 + T(d^2))$ for computing all the $O(d^2)$ possible singularities of C_d, using the Sylvester resultant which for two j-variate polynomials of maximum degree d can be computed in $O(d^{2j} log^3 d)$ time [13]. Note that singularities at infinity can be obtained in a similar way after replacing the line at infinity with one of the affine coordinate axes. In particular, on homogenizing $f(x, y)$ to $F(X, Y, Z)$ we can set $Y = 1$ to obtain $\tilde{f}(x, z)$ thereby swapping the line at infinity $Z = 0$ with the line $Y = 0$. Now the above computation of roots can be applied to $\tilde{f} = \tilde{f}_x = \tilde{f}_z = 0$ to compute singularities at infinity.

Having computed the singular points one next obtains a proper count of the total number of double points DP of C_d. A proper counting was achieved by Noether using (projective) Cremona quadratic transformations, see [47] Following [2], the same can be achieved using (affine) quadratic transformations.

2.1 Affine Quadratic Transforms

In a general procedure for counting double points, given an e-fold point P of a plane curve C_d, we choose our coordinates to bring P to the origin and then apply the quadratic transformation Q_1 or Q_2.

$$Q_1 \; : \qquad x = x_1 \;, \qquad y = x_1 y_1 \qquad (2)$$

$$Q_2 \; : \qquad x = x_2 y_2 \;, \qquad y = y_2 \qquad (3)$$

Affine quadratic transformations are centered on a singularity and affect the curve locally, allowing one to treat each singularity of C_d in isolation. If now $C_d : \; f(x, \; y) = 0$, then the quadratic transformation Q_1 transforms C_d into the curve $C^1 : \; f_1(x_1, \; y_1) = 0$ given by

$$f(x_1, \; x_1 \, y_1) = {x_1}^e \, f_1(x_1, y_1)$$

C^1 will intersect the exceptional line $E : \; x_1 = 0$ in the points P^1 ,..., P^m, the roots of $f_1(0, \; y) = 0$. If P^i is a e_i-fold point of C^1, then we shall have $e_1 + ... + e_m \leq e$. The P^1 ,..., P^m are termed the points of C_d in the first neighborhood of P. The quadratic transformations can be repeated at each of the P^ipoints of C^1 with $e_i > 1$, yielding points P^{ij} points in the second neighborhood of P and so on. The collection of these neighborhod points are termed the points *infinitely near* P and form in general a *singularity tree* at P. At each node of this tree (including the root) keep a count equal to the multiplicity of the curve (transformed curve) at that point. The desingularization theorem for algebraic plane curves, see [2, 47], states that at every node beyond a certain level, the count equals one; in other words, C has only a finite number of singular points infinitely near P. Next (using Bezout) take $\frac{e(e-1)}{2}$ double points towards DP for a count e and sum over all nodes of a singularity tree and additionally over all singularities of C_d and their corresponding singularity trees, to obtain a precise count for the total number of double points DP of C_d. This proper counting of double points then yields the genus of C_d via the above genus formula, (1).

Theorem 2.1: The Genus G for C_d of degree d can be computed in $O(d^6 + d^2T(d^2))$ time.

Proof : The time taken to compute G is bound by the time $O(d^6 + T(d^2))$ taken to compute the $O(d^2)$ possible singular points of C_d, plus the time taken by the refinement of singularities via quadratic transformations, which we now bound. As many as $O(d^2)$ quadratic transformations may be needed for all *infinitely near* singularities of C_d where a single quadratic transformation takes $O(d^2)$ time. Then there is the $O(d^2\ T(d^2))$ time spent in computing intersections with the exceptional line accounting also for a degree blowup of $O(d^2)$ for the transformed curve in a sequence of quadratic transformations. Additionally, there is the time spent in translating the singularity to the origin which entails an algebraic simplification with an overall cost of $O(d^4)$. This results in the overall time bound of $O(d^6 + d^2\ T(d^2))$. ♠

There is then the concise characterization for curves having rational parametric equations

Theorem [Cayley-Riemann]: C_d has a rational parameterization *iff* $G = 0$.

In other words if the given plane curve has its maximum allowable limit of singularities, then it is rational.

3 Parameterizing with a Pencil of Lines

From Cayley-Riemann Theorem of the earlier section, we know that all degree d curves C_d with one distinct $d-1$ fold point, are rational. One way then of parameterizing these curves C_d is to symbolically intersect them with a pencil of lines $(y - y_0) = t(x - x_0)$ through the $d-1$ fold point (x_0, y_0) on the curve. This pencil intersects C_d in only one additional point, the coordinates of which can be expressed as rational functions of the parameter t. Alternatively, the same can be achieved by mapping the $d-1$ fold point on C_d to infinity along one of the coordinate axis. We illustrate this below.

3.1 Mapping Points to Infinity

Consider $f(x,\ y)$ a polynomial of degree d in x and y representing a plane algebraic curve C_d of degree d with a *distinct* $d-1$ fold singularity. We first determine the $d-1$ fold singularity of the curve C_d and translate it to the origin. Then we can write

$$f(x,\ y)\ =\ f_d(x,\ y)\ +\ f_{d\ -\ 1}(x,\ y)\ \ =\ \ 0$$

where f_i consists of the terms of degree i. Note that f_d and f_{d-1} are the only terms that will exist, since a $d-1$ fold singularity at the origin implies that $\forall (i+j)\ <\ d-1$, $\frac{\partial f^{i+j}}{\partial x^i \partial y^j}\ =\ 0$ at $(0,0)$.

On homogenizing $f(x,y)$ we obtain

$$\begin{aligned} F(X,Y,Z)\ =\ & \qquad a_0Y^d\ +\ a_1Y^{d-1}X\ +\ ...\ +\ a_dX^d \\ & + b_0Y^{d-1}Z\ +\ b_1Y^{d-2}XZ\ +\ ...\ +\ b_dX^{d-1}Z\ =\ 0 \end{aligned} \tag{4}$$

Now by sending the singular point $(0,0,1)$ to infinity along the Y axis we eliminate the Y^d term. Algebraically this is achieved by a homogeneous linear transformation which maps the point $(0,0,1)$ to the point $(0,1,0)$ and is given by $X\ =\ X_1\ ,\ \ Y\ =\ Z_1\ ,\ \ Z\ =\ Y_1$, which yields

$$\begin{aligned} F(X_1,Y_1,Z_1) = a_0Z_1^d\ \ & +\ \ a_1Z_1^{d-1}X_1\ +\ ...\ +\ a_dX_1^d \\ & +\ \ b_0Z_1^{d-1}Y_1\ +\ b_1Z_1^{d-2}X_1Y_1\ +\ ...\ +\ b_dX_1^{d-1}Y_1\ =\ 0 \end{aligned} \tag{5}$$

Then one easily obtains

$$Y_1\ =\ -\frac{a_0Z_1^d\ +\ a_1Z_1^{d-1}X_1\ +\ ...\ +\ a_dX_1^d}{b_0Z_1^{d-1}\ +\ b_1Z_1^{d-2}X_1\ +\ ...\ +\ b_dX_1^{d-1}} \tag{6}$$

Letting $X_1\ =\ t$ and dehomogenizing by setting $Z_1\ =\ 1$ and using the earlier homogeneous linear transformation, we construct the original affine coordinates

$$\begin{aligned} x\ &=\ \frac{X}{Z}\ =\ \frac{X_1}{Y_1} \\ y\ &=\ \frac{Y}{Z}\ =\ \frac{Z_1}{Y_1} \end{aligned} \tag{7}$$

as rational functions of the single parameter t.

Theorem 3.1: An algebraic plane curve of degree d with a *distinct* $d-1$ fold point can be rationally parameterized in $O(d^4 log^3 d)$ time.

Proof: The time taken to determine the $d-1$-fold singularity is bound by $O(d^4 log^3 d)$ the time taken to determine a single mutliple root of a univariate polynomial of degree d is $O(d\ log^2 d$ [34]. This also yields the overall time bound, since the homogeneous linear transformation after a translation of the singularity to the origin, is bound by $O(d^4)$. ♠

4 Parameterizing with a Pencil of Curves

In the general case we consider a curve C_d with the appropriate number of *distinct* and *infinitely near* singularities which make C_d rational (*genus* 0). We pass a pencil of curves $C_{d-2}(t)$ through these singular points and $d-3$ additional simple points of C_d. This pencil intersects C_d in only one additional point, the coordinates of which can be expressed as rational functions of the parameter t.

Let $F(X,Y,Z)=0$ and $G(X,Y,Z)=0$ be the homogeneous equations of the curves C_d and $C_{d-2}(t)$ respectively. For a distinct singular point of multiplicity m of C_d at the point (X_i,Y_i,Z_i) we pass the curve $C_{d-2}(t)$ through it with multiplicity $m-1$. To achieve this we equate

$$\begin{aligned} G(X_i,Y_i,Z_i) &= F(X_i,Y_i,Z_i) \;=\; 0 & (8)\\ G_{X^jY^k}(X_i,Y_i,Z_i) &= F_{X^jY^k}(X_i,Y_i,Z_i) \;=\; 0\;,\;\; 1 \le j\,+\,k \le m-2 & (9)\end{aligned}$$

where $G_{X^jY^k} = \frac{\partial G^{j+k}}{\partial X^j \partial Y^k}$. Similarly for $F_{X^jY^k}$.

For an *infinitely near* singular point of C_d we construct its associated *singularity tree* and pass the curve $C_{d-2}(t)$ with multiplicity $r-1$ through each of the points of multiplicity r in the first, second, third, ..., neighborhoods. To achieve this we apply quadratic transformations T_i to both $F(X,Y,Z)$ and $G(X,Y,Z)$ centered around the *infinitely near* singular points corresponding to the singularity tree. The appropriate multiplicity of passing is achieved by equating the transformed equations F_{T_i} and G_{T_i} and their partial derivatives as above. All the above conditions in totality lead to a square system of homogeneous linear equations where the unknowns are the coefficients of $C_{d-2}(t)$ having one variable parameter t.

A counting argument shows that this method generates the correct number of conditions which specifies $C_{d-2}(t)$ and furthermore the total intersection count between C_d and $C_{d-2}(t)$ satisfies *Bezout*. A curve C_d of *genus* $=0$ has the equivalent of exactly $\frac{(d-1)(d-2)}{2}$ double points. To pass a curve $C_{d-2}(t)$ through these double points and $d-3$ other fixed simple points of C_d, the total number of conditions (= the total number of linear equations) is given by

$$\frac{(d\,-\,1)(d\,-\,2)}{2} + (d\,-\,3) = \frac{d\,(d\,-\,1)}{2} - 2$$

which is exactly the number of independent unknowns to determine a pencil of $C_{d-2}(t)$. Having determined the pencil of $C_{d-2}(t)$ curves we compute the resultant $Res_x(C_d,\ C_{d-2}(t))$ which yields a polynomial of degree $d(d-2)$ in y which on dividing by the common factors corresponding to the $(d-3)$ simple points and $\frac{(d-2)(d-1)}{2}$ double points, yields a polynomial in y and t which is linear in y and thereby gives y as a rational function of t. Similarly repeating with $Res_y(C_d,\ C_{d-2}(t))$ yields x as a rational function of t.

Theorem 4.1: A rational algebraic plane curve of degree d can be rationally parameterized in $O(d^6 log^3 d \,+\, d^2T(d^2))$ time.

Proof: The time taken to compute the $O(d^2)$ point singularities with refinement for infinitely near singularitites is bound as before by the time $O(d^6 \,+\, d^2T(d^2))$. The time taken to determine $d-3$ simple points requires at worst no more than $O(d\ T(d))$ time (most points are simple). Then there is the time taken to solve the homogeneous linear system of size $O(d^2)$. Using a technique similar to Gaussian elimination (which requires $O(d^3)$ for a linear system of size d), the time can be bound by $O(d^6)$. Finally there is the computation of the resultants of the equations for C_d and C_{d-2} involving variables x, y and t and division by univariate polynomials [7], all bound by $O(d^6 log^3 d)$ time. Hence the overall time bound above. ♠

5 Algebraic Space Curves

Consider an irreducible algebraic space curve C_d of degree d, which is implicitly defined as the intersection of two algebraic surfaces $f(x,y,z) = 0$ and $g(x,y,z) = 0$. There always exists a birational correspondence between the points of C_d and the points of an irreducible plane curve P_d of degree d, whose genus is the same as that of C_d [1]. Birational correspondence between C_d and P_d means that the points of C_d can be given by rational functions of points of P_d and vice versa (i.e there exists a 1-1 mapping between points of C_d and P_d, except for a finite number of exceptional points). Consequently, knowing how to compute the genus and rational parameterization of algebraic plane curves from sections 2, 3 and 4, yields an algorithm to compute the genus of the space curve C_d and if genus $= 0$ the rational parametric equations of C_d.

To determine the equation of the plane curve P_d we consider the projection of the space curve C_d along one of the coordinate axis. Projecting C_d along, say the z axis, can be achieved by treating both f and g as polynomials in z with coefficients in x and y and then computing the Sylvester resultant. The resultant yields a polynomial in the coefficients of f and g, viz., a plane curve P_d described by the polynomial in x and y. However this projected plane curve P_d in general, is not in birational correspondence with the space curve C_d. For a chosen projection direction it is quite possible that most points of P_d may correspond to more than one point of C_d (i.e. a multiple covering of P_d by C_d). However this may be rectified by choosing a valid projection direction.

5.1 Valid Projection Direction

To find an appropriate axis of projection, the following general procedure may be adopted. Consider the linear transformation $x = a_1x_1 + b_1y_1 + c_1z_1$, $y = a_2x_1 + b_2y_1 + c_2z_1$ and $z = a_3x_1 + b_3y_1 + c_3z_1$. On substituting into the equations of the two surfaces defining the space curve we obtain the transformed equations $f_1(x_1,y_1,z_1) = 0$ and $g_1(x_1,y_1,z_1) = 0$. Next compute the $Res_{z_1}(f_1,g_1)$ which yields a polynomial $h(x_1,y_1)$ which is the equation of the projected plane curve. Choose the coefficients of the linear transformation, a_i, b_i and c_i such that (i) the determinant of a_i, b_i and c_i is non zero and (ii) the equation of the projected plane curve $h(x_1,y_1)$ is not a power of an irreducible polynomial. The latter can be achieved by making the discriminant $Res_{x_1}(h,h_{x_1})$ to be non zero. Such a choice of coefficients ensures that the projected irreducible plane curve given by $h(x_1,y_1)$ is in birational correspondence with the irreducible space curve and thus of the same genus. As "bad" values for a_i, b_i, c_i, $i = 1 \ldots 3$, satisfy a lower dimension hypersurface, any random choice of values will suffice with probability 1, see [40].

5.2 Constructing the Birational Map

There remains the problem of constructing the birational mapping between points on P_d and C_d. Let the projected plane curve P_d be defined by the polynomial $h(x_1, y_1)$. The map one way is linear and is given trivially by $x_1 = x$ and $y_1 = y$. To construct the reverse rational map one only needs to compute $z = I(x_1, y_1)$ where I is a rational function. We now show how it is always possible to construct this rational function by use of a polynomial remainder sequence along a valid projection direction.

Let the surfaces $f(x, y, z) = 0$ and $g(x, y, z) = 0$ be of degrees m_1 and m_2 respectively. Without loss of generality let this direction be the z axis and that $m_1 \geq m_2$. Both m_1 and m_2 are bound by d, the degree of the space curve C_d. Let $F_1 = f(x, y, z)$ and $F_2 = g(x, y, z)$ be given by

$$\begin{aligned} F_1 &= f_0\, z^{m_1} + f_1\, z^{m_1-1} + \ldots + f_{m_1-1}\, z + f_{m_1} \\ F_2 &= g_0\, z^{m_2} + g_1\, z^{m_2-1} + \ldots + g_{m_2-1}\, z + g_{m_2} \end{aligned} \tag{10}$$

with f_j, $(j = 0 \ldots m_1)$ and g_k, $(k = 0 \ldots m_2)$, denoting polynomials in x, y. Then, there exist polynomials $F_{i+2}(x, y, z)$, for $i = 1 \ldots k$, such that $A_i\, F_i = Q_i\, F_{i+1} + B_i\, F_{i+2}$ where m_{i+2}, the degree of z in F_{i+2}, is less than m_{i+1}, the degree of z in F_{i+1} and certain polynomials $A_i(x, y)$, $Q_i(x, y, z)$ and $B_i(x, y)$. The polynomials F_{i+2}, $i = 1, 2, \ldots$ form, what is known as a polynomial remainder sequence (PRS) and can be computed in various different ways [28]. We choose the subresultant PRS scheme for its computational superiority and also because each $F_i = S_{m_{i-1}-1}$, $1 \geq i \geq r$, where S_k is the k^{th} subresultant of F_1 and F_2. This together with making the z axis a valid projection direction ensures that in the polynomial remainder sequence there exists a polynomial remainder which is linear in z, i.e., $F_{r-1} = z\Phi_1(x,\ y) - \Phi_2(x,\ y) = 0$. This then yields z as a rational function of x and y and the inverse rational map.

Theorem 5.1: For an irreducible algebraic space curve C_d, the equations of the birational map and the projected plane curve P_d can be computed in $O(d^6 log^3 d)$ time.

Proof: The time for computing the valid projection direction via a random choice of values and the above polynomial remainder sequence is bound by the resultant computation for the projection. ♠

This together with Theorems 2.1 and 4.1 yields

Corollary 5.2: The genus of an algebraic space curve of degree d and the parametric equations of a rational space curve of degree d can be computed in $O(d^6 log^3 d + d^2 T(d^2))$ time.

6 Faithful Parmeterizations

Given a polynomial parameterization

$$\begin{aligned} x &= P(t) = a_m t^m + a_{m-1} t^{m-1} + \ldots + a_0 \\ y &= Q(t) = b_n t^n + b_{n-1} t^{n-1} + \ldots + b_0 \end{aligned} \tag{11}$$

of an affine algebraic curve $f(x,y)$ we now give an algorithm to check if the parameterization is faithful, i.e., for all but a finite number of points of the curve there corresponds a single parameter value and vice versa. Both m and n are bound by the degree d of the plane curve. Take the Taylor expansion with a single shift and let

$$C(t) = Res_\tau \begin{pmatrix} \frac{P(t+\tau) - P(t)}{\tau} \\ \frac{Q(t+\tau) - Q(t)}{\tau} \end{pmatrix} \tag{12}$$

$$= Res_\tau \begin{pmatrix} P^{(1)}(t) & +\frac{1}{2}P^{(2)}(t)\tau & +\ldots & +\frac{1}{m!}P^{(m)}(t)\tau^{m-1} \\ Q^{(1)}(t) & +\frac{1}{2}Q^{(2)}(t)\tau & +\ldots & +\frac{1}{n!}Q^{(n)}(t)\tau^{n-1} \end{pmatrix} \tag{13}$$

where P^k is the k^{th} derivative of P. Similarly for Q^k.

Then $C(t) \neq 0$ if and only if the parameterization is faithful. Further, if $C(t)$ is a nonzero polynomial, its roots give the singular points with multiplicities of the affine curve. Finally, if $C(t)$ is a non-zero constant then the affine plane curve is non-singular, or equivalently, since the curve is of genus 0, the curve has a single $d-1$ fold singularity at infinity.

For a rational parameterization

$$\begin{aligned} x &= \frac{P(t)}{R(t)} \\ y &= \frac{Q(t)}{R(t)} \end{aligned} \tag{14}$$

of $f(x,y)$, again take the Taylor expansion with a single shift and let

$$C(t) = Res_\tau \begin{pmatrix} \frac{P(t+\tau)R(t) - R(t+\tau)P(t)}{\tau} \\ \frac{Q(t+\tau)R(t) - R(t+\tau)Q(t)}{\tau} \end{pmatrix} \tag{15}$$

$$= Res_\tau \begin{pmatrix} R(t)P^{(1)}(t) - P(t)R^{(1)}(t) & +\frac{1}{2}(R(t)P^{(2)}(t) - P(t)R^{(2)}(t))\tau + \ldots \\ R(t)Q^{(1)}(t) - Q(t)R^{(1)}(t) & +\frac{1}{2}(R(t)Q^{(2)}(t) - Q(t)R^{(2)}(t))\tau + \ldots \end{pmatrix} \tag{16}$$

Then again $C(t) \neq 0$ if and only if the parameterization is faithful.

Theorem 6.1: The faithfulness of parameterizations as well as the singularities of parameterically defined algebraic curves of degree d can be computed in $O(d^4 log^3 d)$ time.

Proof: The time for the Taylor expansion is at most $O(d^2)$ and is bound by the time taken to compute the resultant. ♠

7 Open Problems

A more detailed bit complexity analysis of the algorithm needs to be achieved taking into account the size of the algebraic numbers involved. Further the corresponding algorithmic questions on rational parameterization for algebraic surfaces and higher dimensional varieties of arbitrary degree, are as yet unresolved.

8 References

1. Abhyankar, S. S., (1971) Algebraic Space Curves, *Les Presses de L'Universite' de Montreal*, Montreal, Canada.

2. Abhyankar, S. S., (1983) Desingularization of Plane Curves, *Proc. of the Symp. in Pure Mathematics*, 40, 1, 1-45.

3. Abhyankar, S. S., and Bajaj, C., (1987a) Automatic Parameterization of Rational Curves and Surfaces I: Conics and Conicoids, *Computer Aided Design*, 19, 1, 11 - 14.

4. Abhyankar, S. S., and Bajaj, C., (1987b) Automatic Parameterization of Rational Curves and Surfaces II: Cubics and Cubicoids, *Computer Aided Design*, 19, 9, 499 - 502.

5. Abhyankar, S. S., and Bajaj, C., (1987c) Automatic Parameterization of Rational Curves and Surfaces III: Algebraic Plane Curves, *Computer Aided Geometric Design*, to appear.

6. Abhyankar, S. S., and Bajaj, C., (1987d) *Automatic Parameterization of Rational Curves and Surfaces IV: Algebraic Space Curves*, Computer Science Technical Report, CSD-TR-703, Purdue University.

7. Aho, A., Hopcroft, J., and Ullman, J., (1974) *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, MA.

8. Bajaj, C., (1987) *Algorithmic Implicitization of Algebraic Curves and Surfaces*, Computer Science Technical Report, CSD-TR-697, Purdue University.

9. Bajaj, C., Dyksen, W., Hoffmann, C., Houstis, E., and Rice, J., (1987) *Computing About Physical Objects*, Computer Science Technical Report, CAPO-87-1, Purdue University.

10. Bajaj, C., Hoffmann, C., Hopcroft, J., and Lynch, R., (1988) Tracing Surface Intersections, *Computer Aided Geometric Design*, to appear.

11. Bajaj, C., and Kim, M., (1987a) Generation of Configuration Space Obstacles III: The case of Moving Algebraic Curves, *Proc. of 1987 IEEE Conference on Robotics and Automation*, Raleigh, North Carolina, 979-984. Updated Version to appear in *Algorithmica.*

12. Bajaj, C., and Kim, M., (1987b) Compliant Motion Planning with Geometric Models, *Proc. of the Third ACM Symposium on Computational Geometry*, Waterloo, Canada, 171-180. Updated Version with title "Generation of Configuration Space Obstacles II: The case of Moving Algebraic Surfaces" to appear in *Intl. J. of Robotics Research.*

13. Bajaj, C., and Royappa, A., (1987) *A Note on an Efficient Implementation of Sylvester's Resultant for Multivariate Polynomials*, Computer Science Technical Report, CSD-TR-718, Purdue University.

14. Brent, R., Gustavson, F. and Yun, D., (1980) Fast Solution of Toeplitz Systems of Equations and Computation of Pade Approximations, *J. of Algorithms*, 1, 259-295.

15. Buchberger, B., (1984) Grobner Bases: An Algorithmic Method in Polynomial Ideal Theory, in *Recent Trends in Multidimensional System Theory*, N. Bose (eds)., Reidel.

16. Cayley, A., (1887) On the Intersection of Curves, *Math. Ann.*, 30, 85-90.

17. Chevalley, C., (1951) *Algebraic Functions of One Variable*, A.M.S. Surveys.

18. Collins, G., (1971) The Calculation of Multivariate Polynomial Resultants, *Journal of the ACM*, 18, 4, 515-532.

19. Dedekind, R., and Weber, H., (1882) Theorie der Algebraischen Funktionen einer Veranderlichen, *Crelle Journal*, 92, 181-290.

20. Dicrescenzo, C., and Duval, D., (1984) Computations on Curves, *Proc. of Intl. Symposium on Symbolic and Algebraic Computation*, EUROSAM'84 Lecture Notes in Computer Science, Springer-Verlag 174, 100-107.

21. Davenport, J., (1979) The Computerization of Algebraic Geometry, *Proc. of Intl. Symposium on Symbolic and Algebraic Computation*, EUROSAM'79 Lecture Notes in Computer Science, Springer-Verlag 72, 119-133.

22. Hensel, K., (1908) *Theorie der Algebraischen Zahlen*, Teubner, Leipzig.

23. Hopcroft, J., and Kraft, D., (1985) The Challenge of Robotics for Computer Science, *Advances in Robotics: Algorithmic and Geometric Aspects of Robotics*, eds, J. Schwartz, and C. Yap, vol 1, 7 - 42.

24. Konig, J., (1903) *Einleitung in die Allgemeine Theorie der Algebriaschen Grossen*, Leipzig.

25. Kronecker, L., (1882) Grundzuge einer Arithmetischen Theorie der Algebraischen Grossen, *Crelle Journal*, 92, 1-122.

26. Krull, W., (1952-1959) *Elementare und Klassische Algebra vom Moderne Standpunkt*, Parts I and II, De Gruyter, Berlin.

27. Levin, J., (1979) Mathematical Models for Determining the Intersections of Quadric Surfaces, *Computer Graphics and Image Processing*, 11, 73 - 87.

28. Loos, R., (1983) "Generalized Polynomial Remainder Sequences", *Computer Algebra, Symbolic and Algebraic Computation*, 115-137, Buchberger, Collins, Loos, Albrecht, eds., Second Edition, Wien, New York.

29. Macaulay, F., (1916) *The Algebraic Theory of Modular Systems*, Cambridge University Press, London.

30. Mora, F., and Moller, H., (1983) Computation of the Hilbert Function, *Proc. of European Computer Algebra Conference*, EUROCAL'83 Lecture Notes in Computer Science, Springer-Verlag 162, 157-167.

31. Newton, I., (1680) *The Mathematical Papers of Issac Newton*, Cambridge University Press, ed., D.T. Whiteside.

32. Noether, M., (1890) Les combinaisons caract'eristiques dans la transformation d'un point singulier, *Rend. Cir. Math.*, Palermo, 1, 89-108.

33. Ocken, Schwartz, J., Sharir, M., (1986) Precise Implementation of CAD Primitives Using Rational Parameterization of Standard Surfaces, *Planning, Geometry, and Complexity of Robot Motion*,ed., Schwartz, Sharir, Hopcroft, Chap 10, 245-266.

34. Pan, V., (1985) Fast and Efficient Algorithms for Sequential and Parallel Evaluation of Polynomial Zeros and of Matrix Polynomials, *Proc. of the 26th Annual Symposium on Foundations of Computer Science*, 522-531.

35. Renegar, J., (1987) *On the Worst Case Arithmetic Complexity of Approximating Zeros of Systems of Polynomials*, Technical Report, Operations Research Dept., Cornell University.

36. Riemann, B., (1857) Theorie der Abelschen Funktionen, *Crelle Journal*, 54, 115-155.

37. Rowe, J., (1916) A New Method of Finding the Equation of a Rational Plane Curve from its Parametric Equations, *Bulletin, A.M.S*, 338-340.

38. Salmon, G., (1852) *A Treatise on the Higher Plane Curves*, Chelsea, N.Y.

39. Salmon, G., (1885) *Lessons Introductory to the Modern Higher Algebra*, Chelsea Publishing Company, NY.

40. Schwartz, J., (1980) Fast Probabilistic Algorithms for Verification of Polynomial Identities, *Journal of the ACM*, 27, 4, 701 - 717.

41. Schwartz, J., and Sharir, M., (1983) On the Piano Movers' Problem: II, General Techniques for Computing Topological Properties of Real Algebraic Manifolds, *Advances in Applied Mathematics*, 4, 298 - 351.

42. Sederberg, T., Anderson, D., and Goldman, R., (1985) Implicit Representation of Parametric Curves and Surfaces, *Computer Vision, Graphics Image processing*, vol 28, 72-84.

43. Seidenberg, A., (1974) Constructions in algebra, *Trans. Amer. Math. Soc.*, 197, 273-313.

44. Sylvester, J., (1840) On a General Method of Determining by Mere Inspection the Derivations From Two Equations of any Degree, *Philosophical Magazine*, 16, 132-135.

45. Trager, B., (1984) *Integration of Algebraic Functions*, Ph.D. Thesis, M.I.T.

46. van der Waerden, B., (1950) *Modern Algebra*, 2 volumes, Frederick Ungar Publishing.

47. Walker, R., (1978) *Algebraic Curves*, Springer-Verlag, New York.

48. Weierstrass, K., (1860) *Vorbereitungssatz*, Berlin University Lecture contained in: Einige auf die Theorie der Analytischen Funktionen mehrerer Veranderlichen sich beziehende, Mathematische Werke II, 135-188.

49. Zariski, O., (1950) The Fundamental Ideas of Abstract Algebraic Geometry, *Proc. International Congress of Mathematics, Cambridge*, 77-89.