Geometric Computations with Algebraic Varieties of Bounded Degree

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

Abstract

The set of solutions to a collection of polynomial equations is referred to as an algebraic set. An algebraic set that cannot be represented as the union of two other distinct algebraic sets, neither containing the other, is said to be *irreducible.* An irreducible algebraic set is also known as an algebraic variety. This paper deals with geometric computations with algebraic varieties. The main results are algorithms to (1) compute the degree of an algebraic variety, (2) compute the rational parametric equations (a rational map from points on a hyperplane) for implicitly defined algebraic varieties of degrees two and three. These results are based on sub-algorithms using multi-polynomial resultants and multi-polynomial remainder sequences for constructing a one-to-one projection map of an algebraic variety to a hypersurface of equal dimension, as well as, an inverse rational map from the hypersurface to the algebraic variety. These geometric computations arise naturally in geometric modeling, computer aided design, computer graphics, and motion planning, and have been used in the past for special cases of algebraic varieties, i.e. algebraic curves and surfaces.

1 Introduction

Background: Current research in geometric modeling is engaged in extending the geometric coverage of solid modelers using polynomial equations of arbitrarily high degree. Effectively manipulating these geometric representations require the ability to manipulate the underlying systems of equations [5, 24].

The set of solutions (or *zero* set $Z(S)$) of a collection S of polynomial equations

$$\begin{aligned} S_1 &: f_1(x_1, ..., x_n) = 0 \\ &\dots \\ S_m &: f_m(x_1, ..., x_n) = 0 \qquad (1) \end{aligned}$$

is referred to as an *algebraic set.* Algorithms for manipulating algebraic sets are crucial components for proof systems deciding existential and universal theories of polynomial equations, see for e.g. [36]. An algebraic set that cannot be represented as the union of two other distinct algebraic sets, neither containing the other, is said to be *irreducible.* An irreducible algebraic set is also known as an algebraic variety.

One computational method for manipulating algebraic sets $Z(S)$ is that of Gröbner basis manipulations [11]. Given the set of polynomials $S = \{S_1, ..., S_m\}$, the Gröbner basis algorithms provide a deterministic iterative method for determining whether a polynomial P lies in the set of all polynomials of the form $\sum A_i S_i$ (the *ideal* of S). It collectively manipulates the combinatorial structure of the entire set S of polynomials and in doing so, indirectly provides answers to questions about the zero set $Z(S)$.

Geometric problems dealing with zero sets $Z(S)$, such as the intersection of surfaces, or the decision whether a surface contains a set of curves, are often first versed in an ideal-theoretic form and then solved using Gröbner basis manipulations. One of the main difficulties involved in using the indirect Gröbner basis technique is that the method may be extremely slow for even small geometric problems. In the worst case, this method requires exponential space and may have running time that is double exponential in the number of variables in problem [33]. Even in special cases where this double exponential behavior is not observed, deriving tight upper bounds on the method's running time is difficult.

In this paper, we present an alternative technique for answering various geometric questions on algebraic varieties of degrees two and three. (We shall define the degree of the algebraic variety in section 3). The technique of constructing rational maps of algebraic varieties with hyperplanes, that we present, deals di-

*Supported in part by NSF Grant DMS 88-16286, and ONR contract N00014-88-K-0402

© 1990 ACM 0-89791-362-0/90/0006/0148 $1.50

rectly with the *zero sets* of polynomial equations (rather than just the combinatorial structure of the polynomials). Such rational maps yield simpler algorithms for computing intersections[9], shading, displaying and texture mapping[7], and in general solving systems of algebraic equations[10]. It is based, though not entirely, on lesser known constructs of algebraic geometry, namely the multi-polynomial resultant[32] and multi-polynomial remainder sequences (a generalization of remainder sequences of two polynomials, see for e.g., [23, 31]). These computations can be done in time single exponential in the number of indeterminates of the equations.

Main Results: In section 3 we present a method of computing the degree of an algebraic variety. This essentially relies on a way of computing a hypersurface birational to the given variety, via a valid projection direction along which the projection map is one-to-one. In section 4 we show how to construct the rational inverse of the one-to-one projection map between the hypersurface and the algebraic variety, using multi-polynomial remainder sequences. In section 5 we build on the earlier result of one-to-one maps and present an algorithm to construct the rational parametric equations (a rational map from points on a hyperplane) for implicitly defined algebraic varieties of degrees two and three. This is based on sub-algorithms for parameterizing arbitrary dimension (≥ 3) hypersurfaces of these degrees.

Prior Work: Much of the work in algorithmic algebraic geometry dealing with algebraic curves, and to a limited extent with algebraic varieties, is classical, dating to the pre-1920's, see[15, 22, 26, 27] However, it was not till the fundamental work of[28, 43] that algebraic geometry found a firm footing, free of the falacies which the earlier classical methods were often troubled with. Modern algebraic geometry, equipped with the preciseness of commutative algebra, has its main drawback in being abstract and non-constructive. Recent interest, stemming largely from geometric modeling, graphics, robotics, and other geometric manipulation applications, has seen a resurgence in constructive algorithm design activity, dealing with algebraic varieties[11, 12, 16, 17, 36, 40].

Various algorithms have been given for constructing the rational parametric equations of implicitly defined algebraic curves and surfaces of low degree[2, 3, 41]. Computational methods have also been given for constructing parametric equations of the intersection space curves of two degree two surfaces by[29] using the fact that the pencil of quadrics contains a ruled surface and by[35], via the computation of eiqenvalues of matrices of quadratic forms. The parameterization algorithms presented in [4] are applicable for irreducible rational plane algebraic curves of arbitrary degree, and irreducible rational space curves arising from the intersection of two algebraic surfaces of arbitrary degree. The parameterization techniques, essentially, reduce to solving systems of homogeneous linear equations and the computation of Sylvester resultants, see for e.g.[37]. For non-rational curves, parameterization algorithms which are valid in local neighborhoods of points, singular or otherwise, are given in[6].

The parametric definition of a curve or surface is a standard example of a rational map. Inverting a parametrization of a surface has applications in areas such as sorting points along a parametric curve[25]. Birational maps have been used in resolving the singular (nonsmooth) points of algebraic curves and surfaces[1]. In particular, [9] uses this idea in the robust tracing of algebraic plane curves. Moreover, [4] use birational maps in determining whether an algebraic space curve has a rational parameterization. From a mathematical point of view, current attempts to classify surfaces and higher dimensional geometric objects usually are restricted to classifications up to birationality [42].

2 Notation and Preliminaries

A point in complex projective space $\mathbf{CP}^n$ is given by a nonzero ***homogeneous coordinate vector*** $(X_0, X_1, \ldots, X_n)$ of $n+1$ complex numbers. A point in complex affine space $\mathbf{CA}^n$ is given by the ***non-homogeneous coordinate vector*** $(x_1, x_2, \ldots, x_n) = (\frac{X_1}{X_0}, \frac{X_2}{X_0}, \ldots, \frac{X_n}{X_0})$ of n complex numbers. The set of points $Z_d^n(f)$ of $\mathbf{CA}^n$ whose coordinates satisfy a single non-homogeneous polynomial equation $f(x_1, x_2, \ldots, x_n) = 0$ of degree d, is called an $n-1$ dimension, affine hypersurface of degree d. The hypersurface $Z_1^n(f)$ is also known as a ***flat*** or a ***hyperplane***, a $Z_2^n(f)$ is known as a ***quadric*** hypersurface, and a $Z_3^n(f)$ is known as a ***cubic*** hypersurface. The hypersurface Z_d^2 is a plane ***curve*** of degree d, a Z_d^3 is known as a ***surface*** of degree d, and Z_d^4 is known as a ***threefold*** of degree d. A hypersurface Z_d^n is ***reducible*** or ***irreducible*** based upon whether $f(x_1, x_2, ..., x_n) = 0$ factors or not, over the field of complex numbers. An algebraic variety $V^n\{f_1, ..., f_n\}$ is then an irreducible common intersection of a collection of hypersurfaces $Z_{d_i}^n(f_i)$.

An irreducible ***rational*** hypersurface $Z_d^n(f)$, can additionally be defined by rational parametric equations which are given as $(x_1 = G_1(u_1, u_2, \ldots, u_{n-1})$, $x_2 = G_2(u_1, u_2, \ldots, u_{n-1})$, $\ldots$, $x_n = G_n(u_1, u_2, \ldots, u_{n-1}))$, where G_1, G_2, $\ldots$, G_n are rational functions of degree d in $\mathbf{u} = (u_1, u_2, \ldots, u_{n-1})$, i.e., each is a quotient of polynomials in $\mathbf{u}$ of maximum degree d.

Multi-polynomial Resultant: If $F_1 = 0, ..., F_n = 0$ are homogeneous polynomial equations in n variables, then the ***resultant*** $R(F_1, ..., F_n)$ is a polynomial in the ***coefficients*** of the F_i that vanishes if and only if the F_i have a common zero in projective space. For this reason, the resultant is also often called the eliminant. Geometrically, the resultant vanishes if and only if the n hypersurfaces $Z_d^n(F_i)$ have a common intersection in projective space.

The resultant of several equations has several different characterizations. Probably the most elegant was discovered by Macaulay [32]. He shows that the multi-polynomial resultant can be expressed as the quotient of the determinant of two matrices whose entries are coefficients of the polynomials. In the case of two equations, the matrix for the denominator always has determinant 1 and the matrix for the numerator is the traditional Sylvester matrix[37].

Multi-polynomial Remainder Sequence: Consider first two polynomial equations $f_1(x_1, \ldots, x_n) = 0$ and $f_2(x_1, \ldots, x_n) = 0$. Treating them as polynomials in x_n, the psuedo-remainder $(f_1/f_2) = g(x_1, \ldots, x_n)$ for degree$(f_2) \leq$ degree(f_1), is the result of one step of psuedo-division in the ring C of coefficient polynomials in $n-1$ variables $(x_1, \ldots, x_{n-1})$, i.e. $\alpha f_1 = \beta f_2 - g$ with $\alpha, \beta \epsilon C$ and degree$(g) <$ degree(f_2). Repeating the psuedo-division with f_2 and g and ensuring that the factors α and β are 'primitve', one can compute a subresultant polynomial remainder sequence (p.r.s):

$$f_1, f_2, g = S_{k-1}, \ldots, S_1, S_0 \tag{2}$$

where S_i is the psuedo-remainder of the two polynomials preceding it in the sequence and is known as the i^{th} subresultant of f_1 and f_2, with respect to x_n, see for e.g [23, 31]. Here S_0 is a polynomial independent of x_n and is the resultant of f_1 and f_2, with respect to x_n.

For the set of polynomial equations 1, treating them as polynomials in x_n, we select the polynomial, say f_k, of minimum degree in x_n. We then compute the subresultant psuedo-remainder for each pair $(f_i/f_k) = g_i$, $1 \leq i \leq m$ and $i \neq k$, yielding a new system of equations g_i and f_k. We repeat the above, first selecting from the new system, a polynomial of minimum degree in x_n, and then computing pairwise subresultant psuedo-remainders. Eventually, we obtain a system of $m-1$ polynomial equations, say S^{m-1}

$$\tilde{f}_1(x_1, \ldots, x_{n-1}) = 0$$
$$\ldots$$
$$\tilde{f}_{m-1}(x_1, \ldots, x_{n-1}) = 0 \tag{3}$$

independent of x_n.

The above is then one (macro) step of the multi-equational polynomial remainder sequence (m.p.r.s). For the new set of polynomial equations (3), treating them as polynomials in x_{n-1}, we repeat the entire process above and obtain yet another reduced system S^{m-2} of $m-2$ polynomial equations, all independent of x_{n-1}, and so on. This sequence of systems of multi-equational polynomial equations

$$S = S^m, S^{m-1}, S^{m-2}, \ldots, S^1, S^0 \tag{4}$$

is what we term the multi-equational polynomial remainder sequence.

3 Birational Hypersurface and Degree Computation

A map of the form

$$y_1 = \psi_1(x_0, x_1, \ldots, x_m) y_0$$
$$\ldots$$
$$y_n = \psi_n(x_0, x_1, \ldots, x_m) y_0,$$

where the $\psi_i = \frac{G_i(x_0, \ldots, x_n)}{H_i(x_0, \ldots, x_n)}$ are ratios of homogeneous polynomials of equal degree in the x_j is referred to as a *rational* map. In general, a rational map may be thought of as a function that transforms some set of points X in $(x_0 \ldots x_m)$ space to set of points Y in $(y_0 \ldots y_n)$ space. Note that the denominators are polynomials and can have zeros. Thus the map may not be defined at all points. We denote this map by $\psi : X \rightarrow Y$.

A rational map $\psi : X \rightarrow Y$ is called *birational* if it admits an inverse. That is, there exists a rational map $\phi : Y \rightarrow X$ such that $\psi(X)$ has the same dimension as Y, $\phi(Y)$ has the same dimension as X, $\psi\phi = 1$ almost everywhere, and $\phi\psi = 1$ almost everywhere. Two sets X and Y are said to be *birational* if there exists a birational map between X and Y.

A classical theorem from algebraic geometry states that *"Any algebraic variety $Z(S)$ is birational with a hypersurface $Z(h)$ of appropriate dimension"* (see [21], Prop.I.4.9).

Definition 1 *The* degree *of the algebraic variety $Z(S)$ is then defined as the corresponding degree of the birationally equivalent hypersurface $Z(h)$.*

The construction of the hypersurface h for a given variety S can be done straightforwardly using multi-polynomial resultants. (Computationally, as we shall show in the next section, under certain assumptions on the variety, this can also be achieved using multi-polynomial remainder sequences). Given m independent equations in n variables (1), let S be the algebraic variety of dimension $n-m$ defined by these equations, i.e. $Z(S)$ is the complete intersection of the m polynomial equations. We may construct a *generic* linear projection onto $n-m+1$ of the variables. The image of this projection is the hypersurface H in these $n-m+1$ variables. Determining, the dimension of an arbitrary variety is a non-trivial problem. However, various solutions have been offered, for e.g., see [20, 34].

To find a generic linear projection, the following general procedure can be adopted. Consider the linear projective coordinate transformation

$$y_0 = a_{10}x_0 \ + \ a_{11}x_1 \ + \ \ldots \ + \ a_{1n}x_n$$

$$\cdots$$

$$y_n = a_{n0}x_0 \; + \; a_{n1}x_1 \; + \; \ldots \; + \; a_{nn}x_n$$

The linear coordinate transformation transforms the original homogenized variety $V\{F_i(x_0, \ldots, x_n)\}$ into, a bilinearly related variety $\breve{S} : \breve{V}\{\breve{F}_i(y_0, \ldots, y_n)\}$, $i = 1, \ldots, m$ (w.l.g.).

Let $R(\breve{F}_1, \ldots, \breve{F}_m)$ be the irreducible resultant polynomial corresponding to the projection hypersurface H of the variety $\breve{S}$. Irreducibility of H follows from the irreducibility of S and the projection mapping[21]. Let k be the multiplicity of polynomial R (i.e. there exists a factor R_1 such that R_1^k divides R but R_1^{k+1} does not). Then by applying ([18],Theorem 8.4.13), we see that the projection map is generically k to one. To make the map one-to-one we choose the coefficients of the linear projective transformation, a_ij, $i, j = 0..n$ such that (i) the determinant of a_ij, is non zero (making the map well defined) and (ii) the discriminant of the polynomial $R(\breve{f}_1, \ldots, \breve{f}_m)$ to be non zero. As "bad" values for a_{ij} which do not satisfy (i) and (ii) above, satisfy a set of hypersurface conditions, any random choice of values will in general suffice with probability 1, see [39].

4 Birational Map Computation

The earlier section gave a way of constructing a hypersurface H is a one-to-one projection of the original algebraic variety S, or a bilinearly related variety $\breve{S}$. We now show how such a one-to-one map can be inverted, yielding a birational map between H and S.

Theorem 1 *Let X and Y be two irreducible n-dimensional varieties and ψ a rational map from X to Y that is generically one-to-one. Then under ψ, X and Y are birational.*

This follows from ([21], Cor. I.4.5). Hence, since the map from S to H is one-to-one, there exists an inverse rational map from H to S. Such an inverse rational map from the irreducible polynomial R to the C_i's may be recovered by using the Theorem of the Primitive Element ([43], section II.9). This construction for $m = 2$ is described in [4, 19]. A more general version for unrestricted m is described in [16]. Using multi-polynomial resultants[14], this algorithm runs in time single exponential in m and n.

We now present an alternate method using the multi-polynomial remainder sequence of section (2) on the original polynomial system (1). We assume that the hypersurfaces $f_i = 0$ $1 \le i \le m$ intersect transversally. First, consider the subresultant polynomial remainder sequence (p.r.s) (2) : $f_1, f_2, g = S_{k-1}, \ldots, S_1, S_0$. If the projection direction x_n is birational, and the hypersurfaces $f_1 = 0$ and $f_2 = 0$ have a transversal intersection, we show in [4] that

$$\begin{aligned} S_1(x_1, \ldots, x_n) &= h_1(x_1, \ldots, x_{n-1})x_n \\ +h_0(x_1, \ldots, x_{n-1}) & \\ S_0(x_1, \ldots, x_{n-1}) &= h(x_1, \ldots, x_{n-1}) \end{aligned}$$

That is, the last polynomial S_0 is independent of x_n, and is the *resultant* of f_1 and f_2 with respect to x_n. More importantly the next-to-last polynomial S_1 is linear in x_n. It is referred to as the *subresultant* of f_1 and f_2 with respect to x_n. The subresultant equation $S_1 = 0$ then provides the rational inverse map $x_n = \frac{h_0(x_1, \ldots, x_{n-1})}{h_1(x_1, \ldots, x_{n-1})}$.

Similarly, computing the multi-polynomial remainder sequence (m.p.r.s) (4), under a birational projection direction x_n, yields after the first macro step, a reduced system (3) independent of x_n as well as the inverse map $x_n = \frac{h_0(x_1, \ldots, x_{n-1})}{h_1(x_1, \ldots, x_{n-1})}$. After the second macro step, under a birational projection direction x_{n-1}, we obtain a reduced system independent of x_{n-1} as well as the inverse map $x_{n-1} = \frac{h_2(x_1, \ldots, x_{n-2})}{h_3(x_1, \ldots, x_{n-2})}$, and so on. Starting with m equations in (1), and after $m - 1$ steps, $n \ge m \ge 2$, with the elimination order of $x_n, x_{n-1}, \ldots, x_{n-m+2}$ one obtains the rational projection as well as the rational inverse map:

$$\tilde{f}(x_1, \ldots, x_{n-m+1}) = 0$$

$$\begin{aligned} x_{n-m+2} &= \frac{h_{2m-4}(x_1, \ldots, x_{n-m+1})}{h_{2m-3}(x_1, \ldots, x_{n-m+1})} \\ &\cdots \\ x_{n-1} &= \frac{h_2(x_1, \ldots, x_{n-2})}{h_3(x_1, \ldots, x_{n-2})} \\ x_n &= \frac{h_0(x_1, \ldots, x_{n-1})}{h_1(x_1, \ldots, x_{n-1})} \end{aligned} \tag{5}$$

5 Parameterizing Varieties

Having an explicit birational mapping (projection and inverse maps) between the variety S and a hypersurface H of equal dimension, the problem of computing the rational parametric equations of algebraic varieties S then reduces to the problem of parameterizing birationally related hypersurfaces H. We now provide such rational parameterization algorithms for degree bounded hypersurfaces of any dimension.

5.1 Parameterizing Hypersurfaces of Bounded Degree

Quadric Hypersurfaces $Z_2^n(f)$, $n \ge 2$

Geometric Idea: A line through a fixed point on $Z_2^n(f)$ intersects $Z_2^n(f)$ in, at most, 1 additional point. The coordinates of this additional point are then rational functions of the parameters of the line.

Algebraic Technique:

1. Pick a point on $Z_2^n(f)$ and translate $Z_2^n(f)$ to the origin via a linear change of coordinates.
2. Map the origin to infinity along the X_n axis via another linear change of coordinates.
3. The transformed equation of the hypersurface, must now be linear in x_n, and hence x_n is expressible as a rational function of the remaining variables.

See also Appendix A.

Cubic Hypersurfaces $Z_3^n(f)$, $n \geq 3$

Geometric Idea: A line intersects $Z_3^n(f)$ in at most three points. If two of these points lie on rational elements of $Z_3^n(f)$ then the parameterized transversal connecting these two points will intersect $Z_3^n(f)$ in at most 1 additional point. The coordinates of this additional point are then rational functions of the parameters of the transversal.

Algebraic Technique:

1. Pick a point on $Z_3^n(f)$ and translate $Z_3^n(f)$ to the origin via a linear change of coordinates
2. Intersect $Z_3^n(f)$ with the tangent plane at the origin to yield a rational hypersurface $Z_3^{n-1}(g)$.
3. Repeat (1) and (2) for a different point on $Z_3^n(f)$ to yield another hypersurface $Z_3^n(h)$.
4. Now consider transversals connecting points on the two rational hypersurfaces $Z_3^{n-1}(g)$ and $Z_3^{n-1}(h)$.
5. The intersection of the transversal with $Z_3^n(f)$ yields three roots. Two of these are the chosen points on $Z_3^{n-1}(g)$ and $Z_3^{n-1}(h)$, which can be factored out, leaving the remaining to be written as a rational function of the parameters of the transversal.

See also Appendix B.

6 Possible Extensions

A natural extension to consider is computations with algebraic varieties of unbounded degree. One possibility for constructing a general parameterization algorithm is perhaps to use an inductive argument on the degree of the variety, with the results of this paper providing the base cases. Another interesting problem is to derive worst case time bounds, using bit complexity analysis to model coefficient growth in all the multivariate polynomial manipulations. Finally, interesting open algorithmic questions (which we did not get to consider in this paper) are to compute the the singularities and the multiple genera of algebraic varieties.

Acknowledgements: I thank Guru Abhyankar for answering numerous questions and providing me references on algebraic geometry. Also, thanks to John Canny, Tom Garrity and Joe Warren for many enlightening conversations.

References

[1] Abhyankar, S. (1988), "Good Points of a Hypersurface," *Advances in Mathematics*, 68, 2, 87 - 256.

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

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

[4] Abhyankar, S., and Bajaj, C., (1989), "Computations with Algebraic Curves", Proc. of Intl. Symposium on Symbolic and Algebraic Computation, (ISSAC88), *Lecture Notes in Computer Science*, No. 358, Springer-Verlag, (1989), 279 - 284.

[5] Bajaj, C. (1989a), "Geometric Modeling with Algebraic Surfaces", *The Mathematics of Surfaces III*, ed. D. Handscomb, Oxford University Press, (1989), 3 - 48.

[6] Bajaj, C., (1989b), "Local Parameterization, Implicitization and Inversion of Real Algebraic Curves", Computer Science Technical Report, Purdue University, CSD-TR-863 and CAPO-89-9. *Proc. of the AAECC-7 Conference*, (1989), Toulouse, France.

[7] Bajaj, C., (1990), "Rational Hypersurface Display", *Proc. of the 1990 Symposium on Interactive 3D Graphics*, Snowbird, Utah, to appear.

[8] Bajaj, C., Canny, J., Garrity, T., and Warren, J. (1989) "Factoring Rational Polynomials over the Complexes", *Proc. of the 1989 Intl. Symposium on Symbolic and Algebraic Computation, ISSAC 1989*, 81-90.

[9] Bajaj, C., Hoffmann, C., Hopcroft, J., and Lynch, R., (1988) "Tracing Surface Intersections", *Computer Aided Geometric Design*, 5, 285 - 307.

[10] Bajaj, C., and Royappa, A.,(1990), "The GANITH Algebraic Geometry Toolkit", Comp. Science Tech. Rept. 914, and CAPO report CER-89-21, Purdue University. Also in *Proc. of the 1st Annual Conference on the Design and Implementation of Symbolic Computation Systems*, (DISCO 90), Capri, Italy, to appear.

[11] Buchberger, B., (1985) "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory," *Multidimensional Systems Theory*, Chapter 6, N. Bose (eds). Reidel Publishing Co.

[12] Canny, J. (1988), "Some Algebraic and Geometric Computations in PSACE," *Proc. of the 28'th Symposium on Theory of Computing*, 460-467.

[13] Canny, J. (1988), "Generalized Characteristic Polynomials," *International Symposium on Symbolic and Algebraic Computation*, ISSAC '88, to appear.

[14] Canny, J. F., Kaltofen, E., and Lakshman, Y. (1989) "Solving Systems of Polynomial Equations Faster", *Technical Report No. 89-14*, Dept. of Computer Science, Rensselaer Polytechnic Institute

[15] Cayley, A. (1848), "On the Theory of Elimination," *Cambridge and Dublin Mathematics Journal*, Vol. III, pp. 116-120.

[16] Chistov, A., and Grigoryev, D. (1983), "Subexponential-Time Solving Systems of Algebraic Equations I", Steklov Institute, LOMI preprint E-9-83.

[17] 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.

[18] Fulton, W. (1984) *Intersection Theory*, Springer-Verlag.

[19] Garrity, T. and Warren, J. (1987), "On Computing the Intersection of a Pair of Algebraic Surfaces", *Computer Aided Geometric Design*, in press.

[20] Guisti, M., (1984) "Some Effectivity Problems in Polynomial Ideal Theory", *Proc. EUROSAM 84*, Springer Verlag, Lecture Notes in Computer Science 174, 159-171.

[21] Hartshorne, R. (1977), *Algebraic Geometry*, Springer-Verlag.

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

[23] Ho, C., and Yap, C. K. (1987) "Polynomial Remainder Sequences and Theory of Subresultants", *Technical Report No. 319, Robotics Report No. 119*, Courant Institute of Mathematical Sciences, New York University.

[24] 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.

[25] Johnstone, J., and Bajaj, C., (1989), "The Sorting of Points Along An Algebraic Curve", *SIAM Journal on Computing*

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

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

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

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

[30] Lazard, D. (1983) "Gröbner-Bases, Gaussian Elimination and Resolution of systems of Algebraic Equations", *Proc. of the Eurocal 83*, 146-156

[31] 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.

[32] Macaulay, F. (1902), "Some Formulae in Elimination," *Proc. London Math. Soc.*, Vol. 35, pp. 3-27.

[33] Mayr, E. and Meyer, A. (1982), "The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals," *Advances in Mathematics*, Vol. 46, pp. 305-329.

[34] 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.

[35] 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.

[36] Renegar, J. (1989) "On the Computational Complexity and Geometry of the First-Order Theory of Reals (Parts I,II, III)", *Technical Report No. 853, 854, 856, School of Operations Research and Industrial Engineering, Cornell University*

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

[38] Semple, J., and Roth, L., (1949) *Introduction to Algebraic Geometry*, Clarendon Press, Oxford.

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

[40] 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.

[41] Sederberg, T., and Snively, J., (1987), "Parameterization of Cubic Algebraic Surfaces", *The Mathematics of Surfaces II*, ed. R. Martin, Oxford University Press,

[42] Wilson, P.M.H. (1987), "Towards Birational Classification of Algebraic Varieties," *Bull. London Math Soc.*, Vol. 19, pp. 1-48.

[43] Zariski, O. and Samuel, P. (1958), *Commutative Algebra (Vol.I, II)*, Springer Verlag.

A Appendix: Quadric Hypersurfaces

Consider the implicit representation of a quadric hypersurfac, (which is neither a cylinder or a cone)

$$Z_2^n(f): \sum_{i_1+i_2+\ldots+i_n\leq 2} a_{i_1,i_2,\ldots,i_n} x_1^{i} \ldots, x_n^{i_n} = 0 \qquad (6)$$

We assume that all quadratic terms of $Z_2^n(f)$ are present, for otherwise there exists a trivial parametricrepresentation.

1. Choose a simple point $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ on $Z_2^n(f)$ and apply a linear coordinate transformation

   $$y_j = x_j - \alpha_j, \qquad j = 1, \ldots, n \qquad (7)$$

   to make the resulting hypersurface pass through the origin. This yields

   $$\begin{aligned} Z_2^n(f_1) \quad : \quad & \sum_{i_1+\ldots+i_n=1} b_{i_1\ldots i_n} y_1^{i_1} \ldots y_n^{i_n} \\ + & \sum_{i_1+\ldots+i_n=2} c_{i_1\ldots i_n} y_1^{i_n} \ldots y_n^{i_n} = 0 \quad (8) \end{aligned}$$

2. Apply the homogenizing transformation

   $$y_j = \frac{Y_j}{Y_0} \qquad j = 1, \ldots, n \qquad (9)$$

   to $Z_2^n(f_1)$ and clear the denominator Y_0^2 to yield

   $$\begin{aligned} Z_2^n(F_1) \quad : \quad Y_0 & \sum_{i_1+i_2+\ldots+i_n=1} b_{i_1 i_2\ldots i_n} Y_1^{i_2} Y_2^{i_2} \ldots Y_n^{i_n} \\ + & \sum_{i_1+i_2+\ldots+i_n=2} c_{i_1 i_2\ldots i_n} Y_1^{i_1} \ldots Y_n^{i_n} =(\!00) \end{aligned}$$

3. Now in (10) there exists some nonzero coefficient of the quadratic terms $Y_1^2, Y_2^2, \ldots, Y_n^2$. Without loss of generality, let that be $b_{200\ldots0} \neq 0$. Then set $Y_1 = 1$, a dehomogenizing transformation to yield

   $$\begin{aligned} Z_2^n(F_2) \quad : \quad Y_0 & \sum_{i_1+\ldots+i_n=1} Y_2^{i_2} \ldots Y_n^{i_n} \\ + & \sum_{i_1+\ldots+i_n=2} Y_2^{i_2} \ldots Y_n^{i_n} = 0 \quad (11) \end{aligned}$$

   from where we obtain

   $$Y_0 = -\frac{\sum_{i_1+\ldots+i_n=2} c_{i_1\ldots i_n} Y_2^{i_2} \ldots Y_n^{in}}{\sum_{i_1+\ldots+i_n=1} b_{i_1\ldots i_n} Y_2^{i_n} \ldots Y_n^{i_n}} \qquad (12)$$

4. Using (12) and (9) with $Y_1 = 1$ we obtain

   $$\begin{aligned} y_1 = \frac{1}{Y_0} \quad &= \quad -\frac{\sum_{i_1+i_2+\ldots+i_n=1} b_{i_1\ldots i_n} Y_2^{i_2} \ldots Y_n^{i_n}}{\sum_{i_1+i_2+\ldots+i_n=2} c_{i_1 i_2\ldots i_n} Y_2^{i_n} \ldots Y_n^{i_n}} \\ y_j = \frac{Y_j}{Y_o} \quad &= \quad -\frac{Y_j \sum_{i_1+i_2+\ldots+i_n=1} b_{i_1\ldots i_n} Y_2^{i_2} \ldots Y_n^{i_n}}{\sum_{i_1+i_2+\ldots+i_n=2} c_{i_1 i_2\ldots i_n} Y_2^{i_2} \ldots Y_n^{i_n}}, \\ j \quad &= \quad 2, \ldots, n \qquad (13) \end{aligned}$$

and finally using (7) we obtain

$$x_j = y_j + \alpha_j \qquad j = 1...n. \tag{14}$$

explicit parametric equations with parameters $Y_2, ..., Y_n$.

B Appendix: Cubic Hypersurfaces

Consider the general implicit equation of a cubic hypersurface

$$Z_3^n(f): \sum_{i_1+i_2+i_n \leq 3} a_{i_1 i_2 ... i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n} = 0 \tag{15}$$

1. Choose a simple point $(\alpha_1, \alpha_2, ..., \alpha_n)$ on $Z_3^n(f)$ and apply the linear coordinate transformation

$$y_j = x_j - \alpha_j, \qquad j = 1, ..., n \tag{16}$$

which translates the hypersurface $Z_3^n(f)$ to pass through the origin. This yields

$$\begin{aligned} Z_3^n(f_1): \quad & \textstyle\sum_{i_1+i_2+...i_n=1} \quad b_{i_1 i_2 ... i_n} y_1^{i_1} y_2^{i_2} ... y_n^{i_n} \\ & + \textstyle\sum_{i_1+i_2+...+i_n=2} \quad b_{i_1 i_2 ... i_n} y_1^{i_1} y_2^{i_2} ... y_n^{i_n} \\ & + \textstyle\sum_{i_1+i_2+...+i_n=3} \quad b_{i_1 i_2 ... i_n} y_1^{i_1} y_2^{i_n} ... y_n^{i_n} \\ = 0 & \end{aligned} \tag{17}$$

2. Apply the linear transformation

$$\begin{aligned} z_1 &= b_{100...0} y_1 + b_{010...0} y_2 + ... + b_{000...1} y_n \\ z_j &= y_j, \qquad j = 1, ..., n \end{aligned} \tag{18}$$

which makes $z_1 = 0$ to be the new tangent hyperplane to the hypersurface at the origin. The hypersurface $Z_3^n(f_1)$ of equation (17) then becomes

$$\begin{aligned} Z_3^n(f_2): z_1 \quad & + \quad z_1 \sum_{0 < i_2+...+i_n \leq 2} c_{i_2 ... i_n} z_2^{i_2} ... z_n^{i_n} \\ & + \quad z_1^2 \sum_{i_1+...+i_n=1} d_{i_1 ... i_n} z_1^{i_1} ... z_n^{i_n} \\ & + \quad \sum_{i_2+...+i_n=2} s_{i_2 ... i_n} z_2^{i_2} ... z_n^{i_n} \\ & + \quad \sum_{i_2+...i_n=3} t_{i_2 ... i_n} z_2^{i_2} ... z_n^{i_n} \end{aligned} \tag{19}$$

3. Intersecting the hypersurface $Z_3^n(f_2)$ with the tangent hyperplane $z_1 = 0$ yields

$$\begin{aligned} Z_3^{n-1}(f_3): \quad & \textstyle\sum_{i_2+...+i_n=2} \quad s_{i_2 ... i_n} z_2^{i_2} ... z_n^{i_n} \\ & + \textstyle\sum_{i_2+...+i_n=3} \quad t_{i_2 ... i_n} z_2^{i_2} ... z_n^{i_n} \\ = 0 & \end{aligned} \tag{20}$$

4. Consider a $\mathbf{u} = (u_1, ..., u_k)$, $k \leq n-2$, parameter family of lines, passing through the origin and lying in the hyperplane $z_1 = 0$. These lines are given by

$$\begin{aligned} z_{i+2} &= u_i z_2, \qquad 1 \leq i \leq k \\ z_j &= z_2, \qquad k < j \leq n-2 \end{aligned} \tag{21}$$

5. Intersect these lines given by equation (21) with $Z_3^{n-1}(f_3)$ of equation (19) to yield

$$z_2 = \frac{-\sum_{i_2+...+i_n=2} s_{i_2 ... i_n} u_1^{i_3} ... u_k^{i_k+2}}{\sum_{i_1+...i_n=3} t_{i_2 ... i_n} u_1^{i_3} ... u_k^{i_k+2}} \tag{22}$$

which together with (21) above yields a parametric representation of $Z_3^{n-1}(f_3)$ in terms of parameters $\mathbf{u} = (u_1, ..., u_k)$.

6. Using the linear transformation (16), (18), the parametric representation of $Z_3^{n-1}(f_3)$ and $Z_1 = 0$ we can straightforwardly construct a $\mathbf{u}$ parameterization of $Z_3^{n-1}(f_3)$ in the original space $(x_1, ..., x_n)$. Namely

$$x_i = M_i(\mathbf{u}) \qquad i \leq i \leq n \tag{23}$$

7. Next choose another simple point $(\beta_1, \beta_2, ..., \beta_n)$ on $Z_3^n(f)$ and repeat steps 1., 2., 3. replacing $(\alpha_1, \alpha_2, ...\alpha_n)$ with $(\beta_1, \beta_2, ..., \beta_n)$. This would yield another $Z_3^{n-1}(\hat{f}_3)$ of similar structure as equation (19), viz.,the intersection of a corresponding hypersurface $Z_3^n(\hat{f}_2)$ with an appropriate tangent hyperplane $\hat{z}_1 = 0$.

8. Analogous to Step 4. above, consider then a $\mathbf{v} = (v_1, ..., v_l)$, $l = n - k - 1$, parameter family of lines, passing through the origin and lying in the hyperplane $\hat{z}_1 = 0$. These lines are again given by

$$\begin{aligned} \hat{z}_{j+2} &= v_j \hat{z}_2, \qquad 1 \leq j \leq l \\ \hat{z}_j &= \hat{z}_2, \qquad l < j \leq n-2 \end{aligned} \tag{24}$$

9. Similar to Steps 5. and 6. above, intersect these lines of equation (24) with $Z_3^{n-1}(\hat{f}_3)$ to derive a $\mathbf{v}$ parametric representation of $Z_3^{n-1}(\hat{f}_3)$ in the original space $(x_1, ..., x_n)$. Namely,

$$x_i = N_i(\mathbf{v}) \qquad 1 \leq i \leq n \tag{25}$$

10. Finally consider the $(\mathbf{u}, \mathbf{v})$ parameter family of lines in $(x_1, ..., x_n)$ space joining points $(M_1(\mathbf{u}), M_2(\mathbf{u}), ..., M_n(\mathbf{u}))$ and $(N_1(\mathbf{v}), N_2(\mathbf{v}), ..., N_n(\mathbf{v}))$. Namely,

$$\begin{aligned} x_i = N_1(\mathbf{v}) \quad & + \quad \frac{(N_i(\mathbf{v}) - M_i(\mathbf{v}))}{N_1(\mathbf{u}) - M_1(\mathbf{u})}(x_1 - N_1(\mathbf{u})) \\ 1 \quad & \leq i \leq n \end{aligned} \tag{26}$$

11. Intersect these lines of equation (26) with the hypersurface $Z_3^n(f)$ to yield

$$f(x_1, \mathbf{u}, \mathbf{v}) = 0 \tag{27}$$

with degree of x_1 to be at most three, i.e., the lines intersect the hypersurface in at most three distinct intersection points.

12. Two of the intersection points lying on the hypersurface $Z_3^n(f)$ have x_1 values $M_1(\mathbf{u})$, and $N_1(\mathbf{v})$, Hence $\frac{f(x_1,\mathbf{u},\mathbf{v})}{(x_1-M_1)(x_1-N_1)}$ yields an expression which is linear in x_1. Thus $x_1 = R(u,v)$ where R is a rational function in the $l+k=(n-1)$ parameters $\mathbf{u} = (u_1, ..., u_k)$, $\mathbf{v} = (v_1, ..., v_l)$. Using this together with equation (26) yields a parametric representation of the hypersurface $Z_3^n(f)$ in terms of the $n-1$ parameters $\mathbf{u}$, $\mathbf{v}$.