GROEBNER BASES OF THE IDEAL OF A SPACE CURVE

T.G.BERRY

ABSTRACT. Detailed descriptions of Groebner bases of affine ideals of space curves in general position are given, subject to restrictions on the singularities of the curves. For complete intersections and curves on quadrics Groebner bases for graded reverse Lex are also found, and some specific examples given.

AMS subject classification: 13P10 14Q05

1. INTRODUCTION

In this paper we describe in detail the structure of Groebner bases of the affine ideal of a space curve for elimination orders. The principal results are stated as theorems 5 and 8. Examples are worked out for complete intersections and curves on quadrics and the resulting bases compared with graded reverse Lex. The results are relevant to the general question of the structure of Groebner bases for different types of ideal and different term orders, (c.f. [8, 3, 5]) and more specifically, to the question of the feasibility of using Groebner bases for computations with space curves. This work in fact originated in a study of the applicability of Groebner basis methods to *tracing space curves*, a problem which arises in Computer Aided Geometric Design. This will be reported on elsewhere.

2. NOTATION AND BASIC DEFINITIONS

We first fix some notation. We work over an arbitrary field k, and all geometric objects are assumed defined over k. In particular, $\mathbf{P}^r$ means $\mathbf{P}^r_k$. Homogeneous coordinates in $\mathbf{P}^3$ are (X, Y, Z, W); we think of $W = 0$ as the plane at infinity, and its complement as "the finite space," with corresponding affine coordinates $x = X/W, y = Y/W, z = Z/W$. We identify $\mathbf{P}^2$ with the plane $Z = 0$ in $\mathbf{P}^3$ and use the corresponding coordinates, homogeneous and affine. Both capital and small letters are ordered $Z > X > Y > W$.

Appeared in "Jour. Pure Appl. Alg. 148 (2000), pp17-47."

Let $C \subset \mathbf{P}^3$ be a curve of degree d and arithmetic genus $p > 0$, not lying in a plane (The case $p = 0$ is simpler, and is described in [10]).

Let $I = I(C) \cap \{W \neq 0\})$ be the affine ideal of C in $k[x, y, z]$. Our aim is to describe certain Groebner bases of I .

Let π denote the restriction to C of the projection from $(0, 0, 1, 0)$ to the (X, Y, W)-plane, *i.e.*, of $\mathbf{P}^3 \setminus \{(0, 0, 1, 0)\} \to \mathbf{P}^2$ given by $(X, Y, Z, W) \mapsto (X, Y, W)$, and let $C_* = \pi(C)$. We assume that C satisfies the following, to be referred to as GPH (General Position Hypothesis):

1. C does not pass through $(0, 0, 1, 0)$, the hyperplane at infinity $W = 0$ is transversal to C, and all singularities of C lie in the finite space.
2. $\pi : C \to C_*$ is birational. To avoid trivial cases, we assume that π is *not* an isomorphism.
3. All singularities caused by projection are ordinary double points at finite distance. That is, for almost all points $P \in C, Q \in C_*, \pi(P) = Q$, the natural map $\pi_Q^* : \mathcal{O}_{Q,C_*} \to \mathcal{O}_{P,C}$ is an isomorphism; if it is not an isomorphism then Q is an ordinary double point of C_* in the finite plane, so that $\pi^{-1}(Q)$ consists of two non-singular finite points of C.

If k is infinite, and if C is non-singular then C will satisfy 1, 2, 3 after it is moved by a general projectivity. If C is singular then it will satisfy 1, 2 after a general projectivity, but it will only satisfy 3 if restrictions are made on the nature of its singularities. It is sufficient that C lie on a non-singular surface. The same considerations hold if k is finite and sufficiently large (with respect to $\deg C$). It is worth mentioning this case because most of the experiments which led to the results of this paper were made using Macaulay, Macaulay2, and CoCoA, working over Macaulay's canonical field, $\mathbf{Z}/(31991)$.

We shall in fact need also some further conditions: we shall assume that each of a given finite set of given polynomials is dense, *i.e.*, contains all monomials consistent with its degree with non-zero coefficients (for our purposes it would be enough to assume all monomials of highest degree occur with non-zero coefficients). For example, if $F(x, y) = 0$ is the equation of C_* (a notation to be used throughout), then $\deg F = d$ by GPH(2), and we shall assume that x^d occurs in F. Providing we are dealing with finite sets of polynomials and a field k of characteristic either 0 or sufficiently large, the condition can be achieved by applying a general projectivity.

Let $A = k[x, y, z]/I$ be the affine coordinate ring of C, and $A_* = k[x, y]/(F)$ be the coordinate ring of C_*, so that on these affine rings π corresponds to the map $\pi^* : A_* \to A$ induced by the inclusion

$k[x,y] \to k[x,y,z]$. We shall denote the passage to a quotient in A and A_* by $f \mapsto \bar{f}$. We extend this notation slightly, for example for $f \in k[x,y]$, we write $\bar{f} = \bar{f}(x,y) = f(\bar{x},\bar{y})$.

3. Groebner Bases

Now we turn to the study of Groebner bases for I. By the term "Gbasis" of I we always understand the *reduced* Groebner basis for I, which is uniquely defined by I (the term order being given). Thus if G is a Gbasis then (1) the lead term of any element of I is a multiple of the leading term of some element of G and G is minimal with respect to this property, *i.e.*, contains no redundant elements, and, (2) if $g \in G$ then g is monic and none of its monomials is a multiple of the lead term of any element of $G \setminus \{g\}$. For all this, see [4].

Let us choose an elimination order for z on $k[x,y,z]$. Recall that this means that polynomials in $k[x,y,z]$ are ordered first by their degree in z, and ties are broken by some fixed, but for the moment arbitrary, order on $k[x,y]$. Let G denote the Gbasis for I for this order. We first make some general remarks on the nature of G.

By the fundamental property of elimination orders, $G \cap k[x,y]$ is a Gbasis for $I \cap k[x,y]$, hence consists of the single element $F(x,y)$. All other polynomials in G must contain z explicitly. Since by GPH C does not pass through $(0,0,1,0)$ there are polynomials in I which are monic in z; since polynomials are ordered in the first instance by z-degree, there must be some such polynomial in G, and this polynomial is of minimal degree in z among polynomials in I, monic in z. If this degree is 1, *i.e.*, if there exists in I a polynomial $z - f(x,y)$ then it is easy to see that π is an isomorphism $C \to C_*$, a situation we have excluded. By prop.4 below, there do exist polynomials in I which are monic of degree 2 in z. Then some such polynomial $H \in G$ and no other polynomial of z-degree ≥ 2 can belong to G. We already know that the only polynomial in $k[x,y]$ in G is F, so all other polynomials in G must be linear in z, thus of the form $zg - f$ where $f, g \in k[x,y]$, $g \not\equiv 0 \bmod F$. Following classical terminology we call such polynomials *monoids*. It is clear that we understand G when we understand the monoids.

To understand the monoids we call on the theory of adjoint curves. If $g \in k[x,y]$ annihilates the $k[x,y]$-module A/A_* then we call g an *adjoint polynomial*. A projective plane curve is an *adjoint curve* if its restriction to the finite plane is defined by an adjoint polynomial. (In both these definitions it would be more correct to say adjoint to C_*.

The definitions are only reasonable because C_* is non-singular at infinity.) This terminology is not the classical usage when C is singular. The adjoint curves of C_* in classical terminology are curves coming from the conductor of the integral closure of A_* in its quotient field; when C is singular, so that C_* has more singularities than the double points caused by projection, this integral closure will be strictly larger than A.

Let Δ_C be the divisor on C which is the sum of all the points $P \in C$ at which π is not an isomorphism, and let Δ_{C_*} be the set of points on C_* which lie under points of Δ_C. Classically Δ_C is the "double point divisor" and Δ_{C_*} is the "set of double points of C_* caused by projection." Let u_j denote the dimension of the space of adjoint curves of C_* of degree j. Then $u_j = \dim\{g \in k[x,y], \deg g \leq j$ and g is an adjoint polynomial$\}$. (The "$\leq$" is because we are using affine coordinates.) Then the properties of adjoints that we need are summarised in the following theorem. For C non-singular the proof can be found in [6], or indeed in any classical text on algebraic curves. The results extend to singular Gorenstein curves, as is explained in [9, 2]. One has only to interpret the canonical class as the linear system associated to the dualizing sheaf on C.

Theorem 1.

1. *A polynomial $g \in k[x,y]$ is adjoint to C_* if and only if the plane curve $g = 0$ passes through all points of Δ_{C_*}.*
2. *The set Δ_{C_*} imposes independent conditions on curves of degree $\geq d-3$.*
3. *Adjoints of any degree cut, residual to Δ_C, complete linear systems on C.*
4. *Adjoints of degree $d-3$ cut the canonical class on C, hence $u_{d-3} = p$.*

We have

Lemma 2. *The map $zg - f \mapsto g$ is an isomorphism (of $k[x,y]$-modules) between the monoids in I and the ideal of adjoint polynomials. This isomorphism induces a bijection between monoids in G and the Gbasis of the ideal of adjoint polynomials in $k[x,y]$, the term order being the restriction of the elimination order on $k[x,y,z]$.*

Proof. If $g \in k[x,y]$ is an adjoint then $g\bar{z} = \bar{f}$ for some $f \in k[x,y]$ whence $zg - f \in I$. Conversely if $zg - f \in I$ then it is easy to see that $g = 0$ passes through all points of Δ_{C_*}, hence is an adjoint by theorem 1(1). This establishes the first assertion of the lemma. The second follows easily from considerations of leading terms. □

Lemma 3. *If $zg - f$ is a monoid and either the projective curve defined by $g = 0$ does not have any points at infinity in common with C_*, or $\deg g \leq d-2$, then $f \equiv f_0 \mod F$, where $\deg f_0 = \deg g+1$. In particular if $zg - f \in G$ then $\deg f = \deg g + 1$*

Proof. The rational functions $\bar{z}, \bar{x}, \bar{y}$ have simple poles at all points at infinity, as follows from the representations $\bar{z} = Z/W$ (restricted to C), etc. and the hypothesis that the plane at infinity is transversal to C. The first assertion of the lemma is a straightforward consequence of this observation, and the second then follows because G is a reduced Groebner basis. □

The existence of the polynomial described in the following proposition, without the degree bounds, is also proved in [1] and [10].

Proposition 4. *There exists in I a polynomial of the form*

$$z^2 + a(x,y) + b(x,y) \tag{3.1}$$

of total degree $\leq d-2$. If C is linearly normal, then the total degree is $\leq d-3$.

Proof. Let D_∞ denote the divisor cut out on C by the plane at infinity. As observed in the previous lemma, $\bar{z}, \bar{x}, \bar{y}$ have simple poles at infinity. Thus $\bar{z}^2$ has only double poles at infinity and therefore belongs to $\mathcal{L}(mD_\infty)$, for any $m \geq 2$. Define

$$M(m) = \left\{\bar{x}^i\bar{y}^j, i+j \leq m\right\} \bigcup \left\{\bar{z}\bar{x}^i\bar{y}^j, i+j \leq m-1\right\} ,$$

and let $M^*(m)$ be the k-linear span of $M(m) \subset A$. If, for some $m \geq 2$, $M^*(m) = \mathcal{L}(mD_\infty)$, then $\bar{z}^2$ can be written as a linear combination of elements of $M(m)$; pulling back this relation to $k[x,y]$ gives an equation of the form (3.1) of total degree m. But $M^*(m) \subseteq \mathcal{L}(mD_\infty)$; thus to show the two spaces are equal it is enough to show they have the same dimension. For $m \geq d-3$ the divisor mD_∞ is non-special, so by Riemann-Roch $l(mD_\infty) = md+1-p$. As for $\dim M^*(m)$, an easy count gives $|M(m)| = (m+1)^2$, for any m, but there are in general linear dependencies among the elements of $M(m)$. Assume now $m \leq d-2$. Any relation of linear dependence between elements of $M(m)$ can be written, on collecting terms, in the form $\bar{z}g(\bar{x},\bar{y}) - f(\bar{x},\bar{y}) = 0$, where $\deg g \leq m-1, \deg f \leq m$. Here $\bar{g} \neq 0$, since if $\bar{g} = 0$ we would have $\bar{f} = f(\bar{x},\bar{y}) = 0$, hence the polynomial $f(x,y)$ vanishes on C_*, a contradiction since $\deg f \leq m < d = \deg C_*$. We conclude (using also Lemma 3) that relations of linear dependence in $M(m)$ correspond bijectively to reductions $\mod I$ of monoids $zg-f$, with $\deg g \leq m-1$, and these in their turn (by lemma 2) correspond to adjoints g of C_* of degree $\leq m-1$. Suppose now $m = d-2$. Then adjoints of degree $m-1 = d-3$ cut the canonical class, hence span a p-dimensional space, so $\dim M^*(d-2) = (d-1)^2 - p = l((d-2)D_\infty)$ which establishes the first statement of the proposition. Suppose now C linearly normal. To determine the linear dependencies in $M^*(d-3)$ we need the adjoint polynomials of degree $\leq d-4$ of C_*. Adjoining an appropriate multiple of a line to such an adjoint gives a canonical adjoint, so the space of adjoints of degree $\leq d-4$ is equal to the space of canonical adjoints of C_* containing a line, and this lifting to C is just $\mathcal{L}(K_C - D_\infty)$, which has dimension $i(D_\infty)$. Since we know, by the hypothesis of linear normality, that $l(D_\infty) = 4$, we find by Riemann-Roch that $i(D_\infty) = l(D_\infty) + p - d - 1 = p - (d-3)$, and again we conclude $\dim M^*(d-3) = (d-2)^2 - (p - (d-3)) = d(d-3) + 1 - p = l((d-3)D_\infty)$ and the final assertion of the Proposition follows.

□

There now follows the first of our two main theorems.

Theorem 5. *Let GL denote the reduced Gbasis for I for pure Lex order. Set $D = \frac{(d-1)(d-2)}{2} - p$. Then GL has four elements. The matrix of leading terms is $\left[x^d, z^2, zx, zy^D\right]$ where the first entry is the initial term of the polynomial F, the second term is the leading term of a polynomial $z^2 + a(y)z + b(x,y)$, where $\deg a \leq D-1$, $\deg b \leq D$ the third term is the leading term of a monoid of degree D, and the last term is the leading term of a monoid of degree $D+1$.*

Proof. $F \in G$ for any elimination order and by general position F contains the monomial x^d, which is thus the leading term of F in Lex. We next show that the Gbasis in Lex for the adjoint ideal of C_* consists of polynomials $x + g(y), h(y)$, where $\deg g = D-1, \deg h = D$. By Lemma 2 this gives the monoid terms in the Gbasis of I. (the total degrees of the monoids are given by lemma 3). We establish the adjoint ideal Gbasis by showing that D is the minimum degree of adjoints which are polynomials in y alone, and that there exists an adjoint of the form $x+g(y), \deg g = D-1$, but no adjoints of this form with $\deg g < D-1$. In fact for $h(y) \in k[y]$ to be an adjoint it is necessary and sufficient that the set of horizontal lines $h = 0$ should pass through all points in Δ_{C_*} and there are D of these by the classical formula for the genus of a plane curve. By general position no two double points lie on the same horizontal line, so the minimal number of horizontal lines necessary to form an adjoint, *i.e.*, the minimal degree of g satisfying these conditions, is D. Taking $g = \prod(y - \beta_i)$ where the $(\alpha_i, \beta_i), i = 1 \ldots D$ are the double points, gives an adjoint of the desired type which is, *a priori*, defined only over the algebraic closure of k. However, it is easy to see, using the fact that Δ_{C_*} is an algebraic set defined over k, that in fact g is defined over k. Finally, a polynomial whose lead term in Lex is x has the form $x+g(y)$, $g \in k[y]$. For this to be an adjoint we need $\alpha_i + g(\beta_i) = 0,\ i = 1 \ldots D$ and by Lagrange interpolation such a polynomial exists, of degree $\leq D - 1$. It follows from theorem 1(2) that the degree is precisely $D-1$. Again, it is easy to see that the interpolant is defined over k. Finally, we have already noted the Gbasis must contain a polynomial monic of degree 2 in z; in view of the existence of leading terms zx, y^D in GL, which is reduced, such a polynomial must have the given form. The degree bounds on $a(y), b(x,y)$, are determined as in the proof of prop. 4: the monomials $\bar{z}\bar{y}^i, 0 \leq i \leq D-1, \bar{x}^i\bar{y}^j, 0 \leq i \leq d-1, i+j \leq D$ are linearly independent and therefore span $l(DD_\infty)$, by a dimension count. But $\bar{z}^2 \in l(DD_\infty)$ and the result follows. □

The next theorem will show that the situation is very different if the elimination order is graded when restricted to $k[x,y]$. We may take the restriction as graded Lex. In the following lemma, $|X|$ denotes the cardinality of the set X.

Lemma 6. *Let $J \subset k[x,y]$ be a 0-dimensional ideal, with Gbasis G in graded Lex. For each integer j let $J(j)$ denote the polynomials of degree $\leq j$ in J and let $G(j)$ denote the polynomials of degree exactly j in G, and let $\alpha_k = \dim J(k),\ \beta_k = \alpha_k - \alpha_{k-1}, \gamma_k = \beta_k - \beta_{k-1}$. Let $n = \min\{j | J(j) \neq (0)\}$ and let $m = \min\{j | y^j \in LT(J(j))\}$. Finally, assume that there is a basis for the space $J(m)$ consisting of dense polynomials (c.f. the remarks in § 2). Then $|G| = \beta_m - (m - n - 1)$, $|G_j| = 0$ if $j \notin [n, m]$, $|G(n)| = \gamma_n$, and, for $n + 1 \leq j \leq m$, $|G(j)| = \gamma_j - 1$.*

Proof. First we evaluate the $|G(j)|$. It is clear that $|G(j)| = 0$ for $j \leq n - 1$. Let $\hat{J}(j) = J(j)/J(j-1)$ (we call $\hat{J}$ the space of polynomials of strict degree j in J); then $\dim \hat{J}(j) = \alpha_j - \alpha_{j-1} = \beta_j$. The density hypothesis implies that $\hat{J}(j)$ can be identified with a subspace of $J(j)$ which has a basis of polynomials whose leading terms run through the first β_j monomials of degree j. With this identification it follows easily, by considering initial terms, that the polynomials of $G(j)$ form a vector space basis of $\hat{J}(j)/x\hat{J}(j-1) + y\hat{J}(j-1)$. Suppose first that $j = n$. Then $G(n)$ is a vector space basis of $J(n)$ and $|G(n)| = \alpha_n = \gamma_n$. Suppose now $n + 1 \leq j$. Then, applying the above argument, $LT(\hat{J}(j-1) = [x^{j-1}, x^{j-2}y, \ldots, x^{j-\beta_{j-1}}y^{\beta_{j-1}-1}]$. It follows that $LT(x\hat{J}(j-1)) + y\hat{J}(j-1)) = [x^j, \ldots, x^{j-\beta_{j-1}}y^{\beta_{j-1}}]$ and has cardinality $\beta_{j-1}+1$. We conclude that $|G(j)| = \beta_j - (\beta_{j-1}+1) = \gamma_j - 1$ and $LT(G(j))$ consists of the γ_j monomials of degree j between the β_{j-1}th and the β_jth, as described. Finally, $|G| = \sum_{j=n}^{m} |G(j)| = \beta_m - (m-n+1)$ (the sum telescopes). □

Lemma 7. *For the adjoint ideal of C_*, the integer m defined in lemma 6 is $d-2$.*

Proof. By (4) of theorem 1 the linear system cut by adjoints of degree $\leq d-2$ has dimension $u_{d-2} = d-1+p$. Since $u_{d-3} = p$, the space of adjoints of strict degree $d-2$ has dimension $d-1$, and this is precisely the number of monomials of degree $d-2$ in x, y. By general position, a generic adjoint of degree $d-2$ contains all these monomials with non-zero coefficients and we conclude that there is a basis for the space of adjoints of strict degree $d-2$ which consists of $d-1$ polynomials whose leading terms run through all monomials in x, y of degree $d-2$. In particular there is an adjoint with lead term y^{d-2}, whence $m \leq d-2$. Suppose $m \leq d-3$. Then there is an adjoint of degree $d-3$ with lead term y^{d-3}. Arguing as before this implies that the space of adjoints of strict degree $d-3$ has dimension $d-2$, the number of monomials of degree $d-3$ in x, y, so $u_{d-3} - u_{d-4} = d-2$, which gives, since $u_{d-3} = p$, $u_{d-4} = p-d+2$. But (c.f. the proof of prop. 4) $u_{d-4} = l(K_C - D_\infty) = i(D_\infty)$, and

$$l(D_\infty) - i(D_\infty) = d+1-g\,.$$

But $l(D_\infty) \geq 4$, whence $u_{d-4} = i(D_\infty) \geq p-d+3$, a contradiction. □

Theorem 8. *Let $h_j = h^1(C, \mathcal{O}_C(j))$ for $j \in \mathbf{Z}$. and let $e = \sup\{j | h_j \neq 0\}$. Let GE be the Gbasis of I for the elimination order which restricts to graded Lex on $k[x, y]$.*

1. *GE has cardinality $d-e$. GE contains the polynomial F, a polynomial with lead term z^2 and degree $\leq d-2$, or $\leq d-3$ if C is linearly normal, and $d-e-2$ monoids.*
2. *Set $\beta_i = h_{e-i} - h_{e-i+1}$, $\gamma_i = \beta_i - \beta_{i-1}$. Then the $d-e-2$ monoids in GE fall into blocks of degree $d-2-e+i$, $0 \leq i \leq e+1$. The block of degree $d-2-e$ has cardinality γ_0, and for $i \geq 1$ the block of degree $d-2-e+i$ has cardinality $\gamma_i - 1$, and the leading terms of its monoids are zm_j, where $\beta_{i-1}+1 \leq j \leq \beta_i - 1$ and m_j denotes the j'th monomial of degree $d-2-e+i-1$ in x, y.*

Proof. As in the proof of theorem 5, the key point is to determine the Gbasis of the adjoint ideal of C_*; this is provided by lemmas 6 and 7. In the notation of lemma 6 $\alpha_l = u_l$ for any integer l. Now $h^1(C, \mathcal{O}_C(j)) = h^0(C, \mathcal{O}_C(K_C - jD_\infty)) = u_{d-3-j}$. Thus by the definition of e we have $n = d-3-e$, whence $\alpha_{n+j} = u_{n+j} = h_{e-j}$. Lemma 7 gives $m = d-2$. Thus, applying lemma 6, we obtain a Gbasis for the adjoint ideal which translates, via lemma 2, to the asserted description of the monoids in GE. The rest of the theorem now follows as in the proof of theorem 5. ☐

Finally, we remark that our results for space curves extend trivally to curves in $\mathbf{P}^r$, as follows.

Theorem 9. *Let $C \subset \mathbf{P}^r$ $(r \geq 4)$ be a curve in general position, not lying in any hyperplane, with degree d and genus p. Let $(X_0, \dots, X_r)$ be homogeneous coordinates on $\mathbf{P}^r$ with corresponding affine coordinates $x_i = X_i/X_r$, ordered by $x_i \geq x_j$ if $i \geq j$. Then the Gbasis for the affine ideal of C, for a term order which eliminates successively x_i, $i = r \dots 3$ has the form*

$$[x_r - f_{r-1}, x_{r-1} - f_{r-2}, \dots, x_4 - f_3, G^*]$$

where $f_i \in k[x_0, \dots, x_i]$, $\deg f_i \leq d-i$, G^* is the Gbasis of the affine ideal of the projection of C to $\mathbf{P}^3$ and has the form described in theorems 5 and 8, where the numerical invariants e, α_i of theorem 8 are calculated on C.

Proof. Elimination of variables corresponds to successive projections $C = C_r \to C_{r-1} \dots \to C_3$ where $C_i \subset \mathbf{P}^i$. The projections are biregular, by general position. Then $G^* = G \cap k[x_0, x_1, x_2]$ is a Gbasis for C_3, so is given by theorems 5 and 8, where the numbers e, α_i etc can be calculated on C since they are invariant. For $r-1 \geq i \geq 3$, the projections $C_{i+1} \to C_i$ induce isomorphisms on affine rings; since the affine ring of C_i is a quotient of $k[x_0, \dots x_i]$ it readily follows that $x_{i+1} - f_i \in I(C_{i+1})$ for some $f_i \in k[x_0, \dots x_i]$. Such a polynomial, with LT= x_{i+1}, certainly belongs to G. The degree of f_i can be bounded using the technique of the proof of theorem 4. The coordinates functions x_i, viewed as rational functions on C (or, equivalently on any C_j) have simple poles at infinity, thus lie in $L(jD_\infty)$ for any $j \geq 1$. By the generalized Castelnuovo theorem of Gruson, Lazarsfeld and Peskine (c.f., [7]) hypersurfaces of degree $d-s+1$ cut a complete linear system on any curve C of degree d in $\mathbf{P}^s$, which is equivalent to the statement that monomials of this degree, considered as rational functions on C, span $\mathcal{L}((d-s+1)D_\infty$. The required bound follows. ☐

Theorem 9 applies in particular to give the Gbasis of the ideal generated by a general regular sequence of $r-1$ polynomials in $k[x_0, \dots x_{r-1}]$.

EXAMPLES

Theorems 5 and 8 confirm the inferiority of Lex as an elimination order. Pursuing this theme further, we calculate the Gbases for complete intersections and curves on quadrics, and compare with the corresponding bases in graded reverse Lex (henceforth referred to as DegRevLex), these being cases in which completely explicit calculations are possible.

Example 1. *Complete Intersections.*

If C is a complete intersection of surfaces of degree $m, n, m \leq n$, then C is projectively normal, of degree mn, and the canonical class is cut by surfaces of degree $m+n-4$ (see, *e.g.* [2]). It follows that $2p-2 = mn(m+n-4)$, $e = m+n-4$, and $\gamma_j = j+1 (j \leq m-1), j(m \leq j \leq n-1), m+n-j-1 (n \leq j \leq m+n-1)$, from which the precise form of the Gbasis can be written down. In particular the cardinality of GE is $mn-(m+n-4) = (m-1)(n-1)+3$, the least degree of monoids in GE is $(m-1)(n-1)+1$ and the maximum is $(mn-2)+1$.

Proposition 10. *Let C be a complete intersection of surfaces of degree m and n. Then the Gbasis for Graded Reverse Lex has cardinality $m+1$ and lead term matrix*

$$[z^m, z^{m-1}x^{n-m+1}, z^{m-2}x^{n-m+3}, \dots, zx^{n+m-2}, x^{n+m-1}].$$

The proof is direct, taking into account that the Castelnuovo-Mumford regularity of a complete intersection is $m+n-1$ (so the ideal is generated in degree $\leq m+n-1$).

To point the moral consider the ideal of a complete intersection of curves of degrees 3 and 5. Then the Gbasis in Lex contains 4 polynomials, of degrees 15, 60, 60 and 61; the Gbasis GE of theorem 8 has cardinality 11 and lead term matrix

$$[z^2, zx^8, zx^7y^2, zx^6y^4, zx^5y^5, zx^4y^7, zx^3y^8, zx^2y^{10}, zxy^{11}, zy^{13}, x^{15}]$$

with degrees between 9 and 15, while the Gbasis in DegrevLex has cardinality 4 and lead term matrix

$$[z^3, z^2x^3, zx^5, x^7]$$

with degrees given by the lead terms.

Example 2. *Curves on a quadric.*

Suppose $C \subset Q \subset \mathbf{P}^3$ where Q is a geometrically irreducible non-singular quadric. Recall the standard facts regarding quadrics (see *e.g.* [2]). The Picard group of Q is $\mathbf{Z} \times \mathbf{Z}$, generated by the classes of generators of Q, so any invertible sheaf on Q is $(\mathcal{O}_Q(a,b)$ for some pair of integers a, b. We have

$$
\begin{aligned}
&(3.2) \qquad h^0\left(\mathcal{O}_Q(a,b)\right) &=& \ (a+1)(b+1), a, b \geq -1 \\
&(3.3) \qquad h^1\left(\mathcal{O}_Q(a,b)\right) &=& \ -(a+1)(b+1),\ a \leq -2, b \geq 0 \\
& & & \ \text{or } a \geq 0,\ b \geq -2 \\
&(3.4) \qquad h^2\left(\mathcal{O}_Q(a,b)\right) &=& \ (a+1)(b+1), a, b \leq -2
\end{aligned}
$$

where it is understood that the h^i are zero if a, b fall outside the given ranges.

Let C be of type (a,b) on Q, *i.e.*, $\mathcal{O}_Q(-C) = \mathcal{O}_Q(-a,-b)$, and let J_C be the ideal sheaf of C in $\mathcal{O}_{\mathbf{P}^3}$. Then there are exact sequences

$$0 \to \mathcal{O}_{\mathbf{P}^3}(-2) \to J_C \to \mathcal{O}_Q(-a,-b) \to 0$$

and

$$0 \to J_C \to \mathcal{O}_{\mathbf{P}^3} \to \mathcal{O}_C \to 0$$

Twisting these by $\mathcal{O}_{\mathbf{P}^3}(j)$ and taking cohomology, we get

$$
\begin{aligned}
&(3.5) \qquad h^0\left(\mathbf{P}^3, J_C(j)\right) &=& \ h^0\left(Q, \mathcal{O}_Q(j-a, j-b)\right) \\
& & & \ +h^0\left(\mathcal{O}_{\mathbf{P}^3}(j-2)\right) \\
&(3.6) \qquad h^1\left(\mathbf{P}^3, J_C(j)\right) &=& \ h^1\left(Q, \mathcal{O}(j-a, j-b)\right) \\
&(3.7) \qquad h^2\left(\mathbf{P}^3, J_C(j)\right) &=& \ h^2\left(Q, \mathcal{O}(j-a, j-b)\right) \\
& &=& \ h^1\left(C, \mathcal{O}_C(j)\right)
\end{aligned}
$$

A curve of type $(1,b)$ is rational, while a curve of type (b,b) is a complete intersection. Thus let C be a curve of type (a,b) on Q, where $2 \leq a \leq b-1$. Then one easily calculates, using (3)-(6) above and the fact that a plane section of Q has type $(1,1)$ that $d = a+b,\ p = (a-1)(b-1), e = a-2,\ \gamma_0 = b-a+1, \gamma_j = 2,\ j \geq 1$. Applying theorem 8, we find that the cardinality of GE is $b+2$, and the degree of the members of GE lie between $b-1$ and $b+a$.

Proposition 11. *In DegRevLex, the GBasis of the ideal of a curve of type $(a,b), 1 < a < b$ on a quadric, in general position, has cardinality $b-a+2$, and the lead term matrix is*

$$[z^2, zx^{b-1}, x^b, zx^{b-2}y, x^{b-1}y, \dots,]$$

the final term being $x^{b-k}y^k$ *if* $b-a=2k+1$, *and* $zx^{b-k-1}y$ *if* $b-a=2k$.

Proof. Note that the lead term matrices in DegRevLex are the same for the homogeneous ideal and its dehomogenization with respect to W. By expressions 3.5 and 3.2, one finds easily that the Castelnuovo-Mumford regularity of the ideal is b, and, for $2 \leq r < b$ all members of the ideal of degree r are multiples of Q, the equation of the quadric, while in degree b members of I have the form $QF+G$ where $\deg F = b-2$ and G moves in a $b-a+1$-dimensional space. The proposition follows from these observations and a little calculation. ☐

For example, a curve of type $(9,6)$ has lead term matrix in GE

$$[z^2, x^{15}, zx^5y^3, zx^6y^2, zx^7y, zx^8, zx^4y^5, zx^3y^7, zx^2y^9, zxy^{11}, zy^{13}]$$

while in DegRevLex the lead term matrix is

$$[z^2, x^8y, x^9, zx^7y, zx^8]$$

For GL, the high-order polynomials have degree 36.

ACKNOWLEDGEMENT

This work began when the author was on sabbatical at Indiana University - Purdue University Indianapolis. I would like to thank the Department of Mathematical Sciences, IUPUI for providing an excellent work environment. I thank Richard Patterson for many discussions, and critical readings of several versions of this paper, which resulted in substantial improvements, both in substance and in style. Remaining errors are, of course, my own. On a metamathematical level I give my warmest thanks to Dick and Sarah Patterson for their hospitality during my stay in Indianapolis.

REFERENCES

[1] S.S. Abyankar. *Algebraic Space Curves*. Les presses de l'Université de Montreal, Canada, 1971.

[2] E. Arabello, M. Cornalba, P.A. Griffiths, and J. Harris. *Geometry of Algebraic Curves*, volume 1. Springer Verlag, 1985.

[3] G Carrà Ferro. Groebner bases and Hilbert schemes. *Jour. Symb. Comp.*, 6:219–230, 1988.

[4] D. Cox, J. Little, and D. O'Shea. *Varieties, Ideals and Algorithms*. Undergraduate Texts in Mathematics. Springer Verlag, 1991.

[5] R. Fröhberg and J. Hollman. Hilbert series for ideals generated by generic forms. *Jour. Symb. Comp.*, 17:149–157, 1994.

[6] W. Fulton. *Algebraic Curves*. Addison-Wesley, 1989.

[7] L. Gruson, R. Lazarsfeld, and C. Peskine. On a theorem of Castelnuovo, and the equations defining space curves. *Invent. Math.*, 72:491–506, 1983.

[8] L. Robbiano. Bounds for degrees and number of elements in Groebner bases. In *Applied Algebra, Error-Correcting Codes and Cryptography*, volume 508 of *Lect. Notes in Comp. Sci.* Springer, 1990.

[9] J-P Serre. *Groupes Algébriques et Corps de Classes*. Hermann, Paris, France, 1959.

[10] T.G.Berry. Parameterization of algebraic space curves. *Jour. Pure Appl. Alg.*, 117-118:81–95, 1997.

http://www.ldc.usb.ve/~berry/

DEPARTAMENTO DE MATEMATICAS PURAS Y APLICADAS, UNIVERSIDAD SIMÓN BOLÍVAR, CARACAS, VENEZUELA, MAILTO:BERRY@USB.VE